+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

READING SAMPLE

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

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

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.

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.

CYBERSECURITY AWARENESS

1

1.3.2 Challenges and pressures faced by OEMs and Tier-N suppliers

The need to integrate cybersecurity into organizations is driven by more than just internal factors, such as the goal of preventing and mitigating cyber risks. As the automotive ecosystem becomes increasingly complex, additional challenges and pressures exerted by external factors must also be taken into account by the industry.

OEMs and Tier-N suppliers face organizational, technical, methodological, and supply chain challenges associated with cybersecurity. In particular, cooperation with external or non-automotive companies can be challenging, because end-to-end cybersecurity requires effort from several parties along the value chain and therefore calls for additional cybersecurity measures that address the activities distributed between OEMs, suppliers and other stakeholders. Furthermore, cybersecurity is a relatively new topic for some companies in the automotive domain, which leads to companies being faced with upfront costs for the implementation of new security measures and systems. The amount of effort required to address cybersecurity holistically is widely unknown, and it is often not yet possible to reference best-practice approaches, because cybersecurity is a new additional discipline to a large extent.

Securing software and hardware in modern vehicles will require new skills. But automotive companies are still building up the cybersecurity competence that is needed to fill the cybersecurity skills gap. On the one hand, a lack of knowledge and competence often leads to longer development time and inefficient solutions, as poor cybersecurity decisions are made, e.g. when selecting appropriate cybersecurity controls to address specific threats. On the other hand, a lack of organizational management of cybersecurity can lead to unstructured, solitary and isolated solutions within companies. The lack of a common approach to tackling cybersecurity risks that is incorporated into organization-wide policies forces different departments or project teams to solve cybersecurity issues themselves.

Besides that, the growing need for cybersecurity is also driven by external stakeholders, such as government bodies and authorities. New, upcoming regulations and standards increase the pressure on organizations to ensure that vehicles meet appropriate industry requirements for cybersecurity. Growing public awareness of cybersecurity is another factor. On the one hand, this is caused by hacks and data leaks that attract media attention. On the other hand, it is also triggered both by the growing demand for privacy protection and by higher expectations in the digital world as regards cybersecurity throughout the product lifecycle. As consumers are becoming more concerned about security and privacy risks, consumer trust is becoming crucial and cybersecurity is regarded as a fundamental part of corporate responsibility. Rather than seeing cybersecurity as a special feature added to modern vehicles, consumers see it as a proactive discipline that is taken for granted and is necessary in order to earn the trust of consumers.

1.3.3 Inhibitors of cybersecurity

We have seen in the previous sections that inadequate cybersecurity is posing a real threat. But many companies are still reluctant to take action. They point to differences of opinion among stakeholders and the costs of investment. There are several recurring lines of argument that may be used to negate the importance of cybersecurity outlined earlier. These include:

Costs arising from the implementation of cybersecurity technologies/requirements
Establishing and maintaining cybersecurity increases the overall costs of a product. For instance, the Bill of Materials (BOM) cost could increase as a consequence of ensuring cybersecurity. And the need for message encryption leads to a need for hardware security modules (HSMs) which leads to an increase in the cost of an ECU. Furthermore, additional development activities are required, such as risk assessments, the definition of cybersecurity concepts, and penetration testing. In addition, regulations such as the China GB for automotive cybersecurity (see Chapter 2 for more information) require specific consideration of test cases. This creates a need for cybersecurity controls to ensure that tests are carried out in accordance with the regulations. Such regulations are a particularly significant cost driver because controls are often needed for the entire fleet, which includes vehicles which were already in the field before the regulation came into effect. This means that measures have to be implemented after development and during the operation and maintenance phase, which is even more costly.

According to the VDA's position on automotive security, cybersecurity requirements will increase costs and inhibit innovation. However, as mentioned above, these costs are insignificant in comparison with the costs that may be incurred as a result of cyberattacks.

The margin of automotive products is already under pressure, so it is important to recognize that investments in cybersecurity right now can further reduce overall cost.

Reduced product performance
Cybersecurity is seen as a disturbing element for user experience (e.g. degradation of features because higher computing power is needed for encryption, delayed system availability, reduced data exchange with third-party devices, 2-FA etc.). However, cybersecurity must be seen as an integral part of functionality, not as an add-on which impacts product performance but rather as an essential aspect that secures it.

Complex cooperation and processes (external and internal)
Cybersecurity can cause additional disruption within established product development processes within an organization. There may be a conflict of interest, for example, between, on the one hand, technical engineers at software and hardware level who do not see the necessity for cybersecurity itself or see it as an add-on which can be included later in the process and, on the other hand, cybersecurity managers who need to ensure compliance with standards and regulations. Besides the cybersecurity managers, cybersecurity engineers are also often seen as an additional threat to the timely release of a new product. So new cooperation strategies are required in order to provide transparent, pre-defined processes and escalation paths.

But complex cooperation is not only limited to the organization itself. There is often a lack of cooperation and even a misalignment between Tiers and OEMs. This is usually the result of a lack of pre-defined communication strategies and a failure to define key stakeholders, especially at the technical level. Such conflicts between two parties, either internal (e.g. between projects) or external (e.g. between two organizations), can be mitigated by a distributed development cybersecurity strategy. This is discussed further and in more detail in Chapter 4.

In the automotive domain, a Development Interface Agreement (DIA) is the core document in the collaboration between the vehicle manufacturer and several suppliers for a system that is to meet specific requirements. Therefore, a corresponding Cybersecurity Development Interface Agreement that specifies distributed cybersecurity activities and documented responsibilities, information exchange, and work share between the parties involved in development is required by ISO/SAE 21434.

Lack of state-of-the-art references
For many years, cybersecurity had remained unregulated in the automotive sector. Organizations were willing to invest in cybersecurity had no references for state-of-the-art techniques and best practices for implementing automotive cybersecurity. In addition, existing cybersecurity standards and regulations were fragmented and focused mainly on Information Technology (IT) and data privacy. This changed with the UN R155 on automotive cybersecurity and the ISO/SAE 21434 on road-vehicle cybersecurity engineering back in 2021.

Lack of company vision
Cybersecurity has become a new dimension of quality for automobiles. However, organizations are not yet aware of this paradigm shift, so they do not consider cybersecurity to be a fundamental and essential part of their overall company vision which often leads to wrong prioritization. To have an influential cybersecurity culture not only the commitment of management is needed, but also cybersecurity awareness among all employees. The lack of cybersecurity awareness among employees leads to a lack of focus in the overall company vision.

Lack of resources and disruption of daily routines
Additional resources (e.g. manpower, new licenses, tools, etc.) are required and this could be rather demanding for quite a few companies on the financial front. Synergies are therefore essential to the creation of a suitable organizational structure. Furthermore, human habits represent an additional inhibitor because humans, who are creatures of habit, would have to change their daily routine and their ways of working.

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.

1.3.4 Cybersecurity as business enabler

Many companies underestimate the benefits of cybersecurity and highlight the inhibitors outlined in the previous chapter. However, implementing cybersecurity would not only prevent cyberattacks but could also be the key business enabler that opens up new revenue opportunities. By giving attention to the enablers described below, business leaders can target their funds and resources in such a way that they not only reduce the costs of cybercrime but also benefit from new opportunities for generating economic value.

- **Cybersecurity enables safety**
  Safety hazards and cybersecurity threats converge in cyber-physical systems such as automated vehicles. For instance, a malicious party can exploit cyber vulnerabilities to create extremely hazardous situations and can even manipulate driving behavior and endanger human life. Without strong cybersecurity measures, safety cannot be ensured, and the intended vehicle functionality cannot be guaranteed under defined operational conditions. SAE J3061 states that every safety-related system is always cybersecurity related. Safety can be supported by cybersecurity if cyberattacks are discovered at a very early stage of the vehicle lifecycle. This means that cybersecurity can also help to protect human life.

- **Cybersecurity facilitates business profitability and operations**
  The integration of cybersecurity activities during the initial stage of product development would benefit an organization financially because the cybersecurity framework would then be established during an earlier phase of product development. This would enable the business to react swiftly to cyberattacks by implementing countermeasures in good time to prevent blackouts of the system, e.g. a complete breakdown of the vehicle. This can be ensured through an established framework of incident handling within the organization. With the ever-increasing time and cost pressures in automotive development, this could be a criterion which determines whether or not a new project is selected.

- **Cybersecurity provides an advantage over competitors**
  Today, cybersecurity is already a criterion in decision making. In the case of end customers, for example, awareness has increased greatly in recent years. End customers will no longer buy a car if they feel that it might not be secure, especially where autonomous driving (as described above) is concerned. And OEMs have started to include cybersecurity in the supplier selection process. As regulations force car manufacturers to mitigate supplier-related risks, cybersecurity capability has become part of the supplier evaluation criteria and is therefore a reason for selecting a particular supplier for collaboration.

- **Cybersecurity ensures customer loyalty and builds trust**
  Consumer trust plays a key role with regard to long-term product adoption and business growth. Brand loyalty can be improved by developing a reputation for safeguarding sensitive information from the hacks discussed earlier in this chapter and by providing transparency, thereby building trust with customers. The impact of the Jeep hack described above on the stock value of Fiat Chrysler is an example of the negative impact of a lack of attention to cybersecurity.

- **Cybersecurity supports process driven work**
  The establishment of cybersecurity in accordance with new standards and regulations (more in Chapter 2) forces companies not only to establish new cybersecurity processes, but also to examine their existing quality management system as the basis for it. This creates an awareness of the need for, and benefits of, a proper process framework and working in an aligned and systematic way on a day-to-day basis. As a result, development errors can be reduced, efficiency increased, and misunderstandings avoided. This topic is a major concern especially (but not only) as regards smaller start-ups, previously mechanic-based suppliers, and manufacturers of special-purpose vehicles, who are not yet used to the high expectations of the automotive industry. But cybersecurity can be a business enabler for established companies as well. Cybersecurity and its processes can be seen as a role model because activities are established throughout the overall V-model, providing a holistic view of the engineering process. More and more companies use this approach as a blueprint when establishing other mandatory management systems, such as the functional safety management system required by UN Regulation No. 157.

– **Cybersecurity supports business agility**
Cutting-edge technologies play a key role in agile organizations, enabling them to gain a competitive edge, supporting the development of new products and services, providing better customer experiences, and more. The digital transformation of the automotive industry requires a strong cybersecurity posture which enables the use of cutting-edge technologies in sensitive areas. Building up a proper cybersecurity infrastructure helps organizations recover quickly and efficiently in the event of security breaches, using predefined approaches and strategies to address cyber threats and risks.

1.4 Key trends impacting automotive cybersecurity

Driven by the digital transformation of the automotive sector, cars are turning into computers on wheels, which makes them tempting targets for cyberattacks. Digitalization is only one of the four key trends that are driving the transformation of the automotive industry. While these trends bring new challenges, create new attack potential, and increase the attack surface and threat landscape, organizations can leverage them for their future growth when automotive cybersecurity is addressed throughout the lifecycle from cradle to grave.

1.4.1 Autonomous driving

Autonomous driving is redefining the role of the automobile. Instead of us driving them, fully automated cars and trucks that drive us will become reality. Capable of sensing their environment and operating without human involvement, autonomous cars will enhance comfort and safety by providing more free time which was previously spent driving. Vehicles that are currently released for sale only reach SAE Level 2 or, at most, SAE Level 3 of autonomous driving as defined by SAE J3016. SAE Level 5 is the highest level that can be achieved. Commercial vehicles with SAE Level 4 functionality are still in an early stage of development. In addition to the technical challenges, there is also a need to comply with a variety of country-specific regulations.

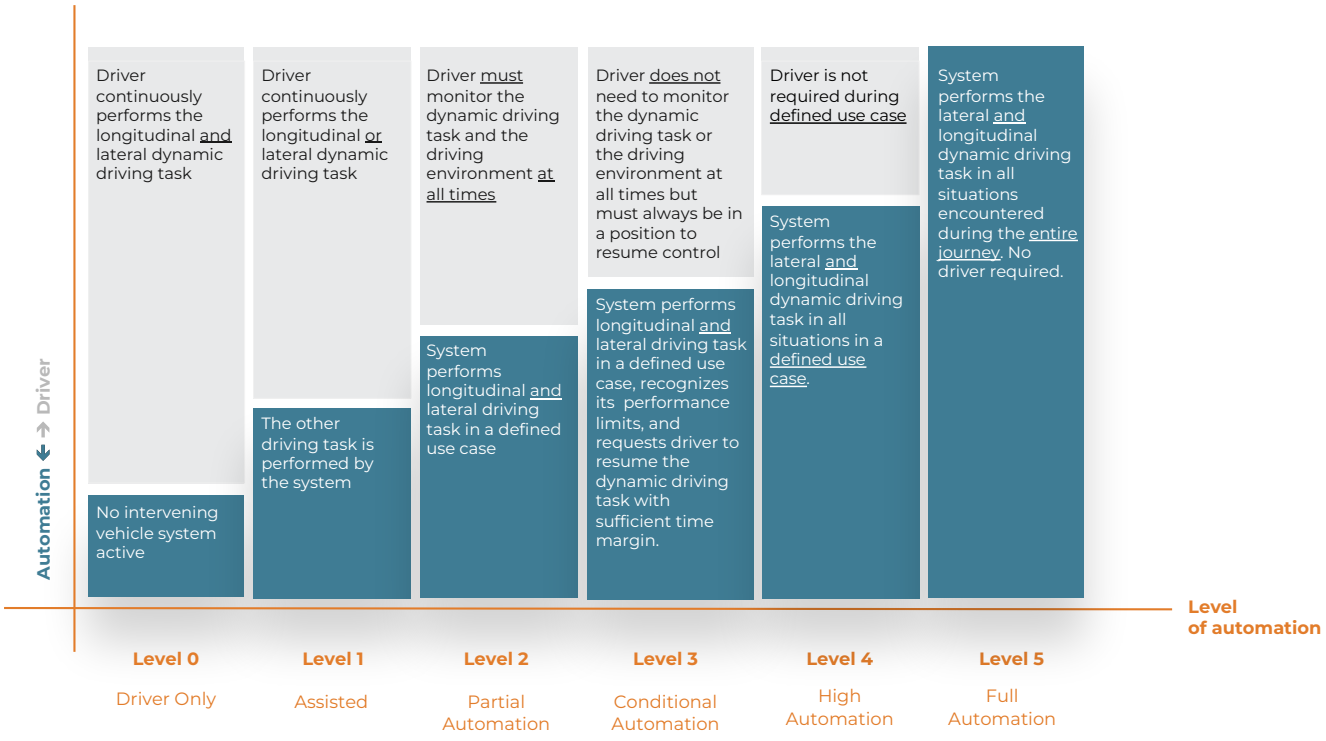


Figure 1.9 SAE J3016 levels of driving automation

As automated driving systems (ADS) take on greater responsibility, the potential impact of errors and attacks increases due to the broader range of functions required [284]. In contrast with conventional IT systems, a simple shut-down is not feasible in the case of attacks on the cyber-physical vehicle system, as this could lead to hazardous situations. One need only think of the consequences of a shut-down during an overtaking maneuver or when driving on hairpin bends in the mountains. Additional fallback systems and redundancy are required to ensure that all safety-critical functions continue even in the case of a failure of the system. Autonomous driving also has a greater impact on privacy due to the increased need for data collection and processing (inside the vehicle as well as within the infrastructure), from basic navigation to deep knowledge about driving circumstances. Functional safety (FuSa) is a discipline with a long history in the automotive sector, but it needs to converge with cybersecurity to ensure the high quality of products and device reliability. Organizations need to address both disciplines in such a way that vehicles are protected against attacks and disturbance from the environment or humans, and humans are protected against threats arising from technical system failures.

1.4.2 Electric vehicles

A glance at the figures confirms that this is not a temporary phenomenon. In 2022, 58% of newly registered cars in Sweden were electric and 89% in Norway. A look at the overall figures confirms this: In 2023, more than 800,000 new EVs will be registered in Germany, and more than one million in California (U.S.). By 2023, 4% of all vehicles on the road in Europe were electric [331], [332]. According to the VDA, this trend will continue, and the importance of EVs will increase due to ambitious climate targets and the pressure from (non-)governmental organizations on the automotive industry to rethink the mobility of tomorrow [307]. A good example of this is the ban on combustion engines that is currently under discussion in Germany and other countries.

EVs will have an impact on the automotive ecosystem because they contain not only a larger number of electronic components but also many new ones in comparison with conventional cars with an internal combustion engine (ICE). This increases the attack surface and therefore the impact on cybersecurity. It is necessary to ensure that infrastructures are protected from the influence of electric vehicles and that the integrity of data required for EVs is guaranteed [284].

- **Data integrity**
  With advancements in EVs, new risks are emerging in the form of attacks based on the loss of data integrity. These attacks can be divided into two categories. On the one hand, attacks on the performance of EVs must be prevented by ensuring the integrity of data from different data sources used to extend the range of the automobile. The manipulation of such data can lead to unexpected negative performance of EVs. For example, a scenario could arise such as miscalculation of the remaining driving distance using battery power due to insufficient data, which could cause the car to stop in the middle of nowhere. On the other hand, new components like the battery itself and the battery management systems are often purchased from third parties who have no connection with the automotive industry and are therefore often not subject to the same cybersecurity rules and regulations [300]. This can enable hackers to attack specific hardware or software components or their sub-components, e.g. by manipulating the temperature sensor to trigger overheating of the battery.

- **Critical infrastructures**
  The charging infrastructure required for powering EVs connects the automotive domain with the critical infrastructure of electricity generation and distribution. As electromobility is highly dependent on the availability of charging infrastructure, interfaces need to be protected appropriately. In addition, it is possible for attackers to leverage electronic charging stations to cause damage or financial loss [300]. This is often accomplished by manipulating the Near Field Communication (NFC) card that is used to handle billing when drivers charge their EVs [300]. Researchers have shown that they are able to copy these cards and use them to charge their vehicles, with the bill going to the associated account [300]. To avoid financial harm, charging infrastructures and related payment technology need to be protected. Along with payment data, personal data also needs to be protected. This includes any data linked to the user's account with the charging station provider, such as address and date of birth. Typically, charging stations communicate with electric vehicles to manage the charging process. Securing this communication is crucial to the prevention of interruptions or other forms of tampering. There is also a vast network behind the charging stations. To protect the infrastructure, it is necessary to prevent unauthorized access from a charging station to the backend.

Note: Pages missing in this reading sample

This reading sample is only an excerpt from the publication “1000 Things Worth Knowing in Automotive Cybersecurity” and contains only selected pages as a preview. The full reading experience is available in the complete publication.

2. REGULATIONS, STANDARDS, AND INITIATIVES

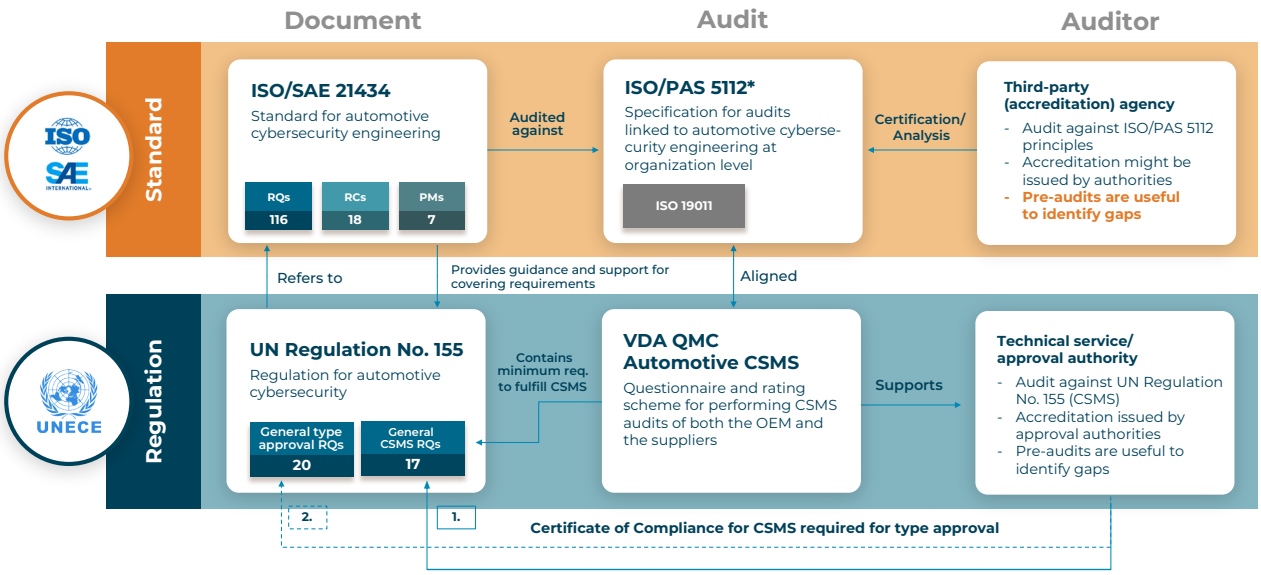


Figure 2.7 Summary of Cysec regulation and standardization

ISO/SAE 21434 will allow an audit of adherence to common cybersecurity practices and attestation by third parties. Legal experts see this as the basis for resolving legal disputes and liability issues in the case of cybersecurity-related vehicle incidents, so automotive players can use this standard to demonstrate adherence to the UN Regulation, e.g. in contracts between OEMs and Tier-N suppliers [49].

In order to support inspection, auditing, and certification bodies in the independent attestation of security practices and to support organizations in conducting internal audits, ISO Publicly Available Specification (PAS) 5112, "Road vehicles – Guidelines for auditing cybersecurity engineering" was published in March 2022. The objective of this specification is to provide guidance on the following:

- Management of a CSMS audit program along the value chain
- Conducting audits
- Competence of CSMS auditors
- Provision of documentation to serve as evidence

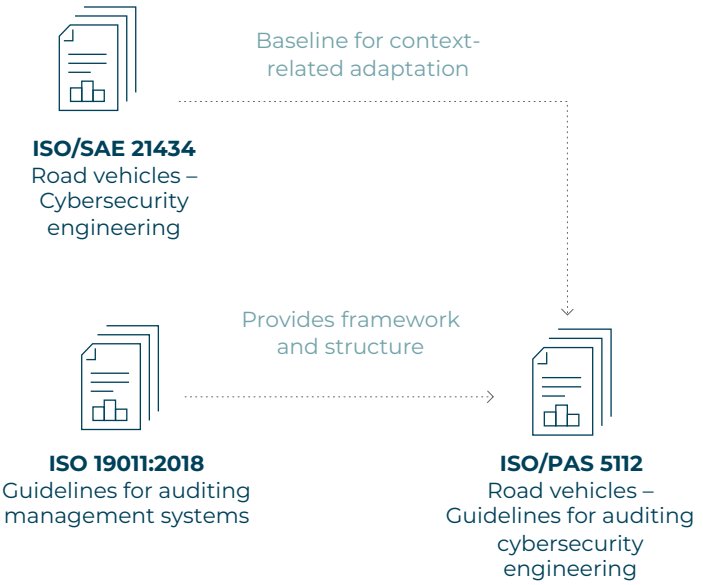


Figure 2.8 Input for the structure of ISO/PAS 5112

ISO/PAS 5112 is useful for those who need to understand or conduct internal/external audits of a CSMS or to manage a CSMS audit program. As shown in figure above, the structure is based on ISO 19011 (“Guidelines for auditing management systems”), which provides a framework both for companies to use when planning, implementing, and improving their audit programs and for auditors to use when auditing the implementation of management systems. ISO 19011 focuses on internal audits (first-party audits) and audits of external suppliers or other external interested parties (second/third-party audits). ISO/SAE 21434, in turn, provides the actual context for adapting the audit methodology of ISO 19011 to automotive cybersecurity engineering. This provides the basis for the contextual adaptation of ISO/PAS 5112.

2.2.4.2 Differences between auditing ISO/SAE 21434 and UN R155

Both ISO/SAE 21434 and UN R155 require an audit of the cybersecurity organization and its processes. The UN R155 audit, based mainly on its requirements in Chapter 7.2, is required in order to obtain a CoC and is therefore a prerequisite for type approval. The audit is carried out by a technical service (e.g. TÜV Süd, TÜV Nord, DEKRA or some other technical testing organization in Germany, VCA in the UK, and IDIADA in Spain) and is valid for three years only. A re-audit must then be carried out to confirm that the CSMS is still adequate. For the preparation and execution of the UN R155 audit, several support materials are available, such as ISO/PAS 5112, the KBA checklist, and the UN R155 interpretation document. Further information can be found in the following chapters.

An ISO/SAE 21434 audit can be carried out by anyone, as long as a sufficient number of independent auditors can be found. There are also no specific requirements as regards how long a passed audit is valid. But it appears that certificates are valid for three years as in the case of R155. As mentioned above, ISO/PAS 5112 provides guidance on the conduct of ISO/SAE 21434 audits.

Neither of these audits focuses on project-specific solutions. They focus rather on the cybersecurity management system and its processes. However, the two documents each have a different scope, so the scope of the audits may also be different.

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

It is not recommended for suppliers to go for UN R155 as the regulation is written for OEMs and not all requirements can be met by the supplier.

2.2.4.3 KBA questionnaire

The KBA (Kraftfahrtbundesamt), which is the Federal Motor Transport Authority in Germany, has also published a catalogue of requirements derived from UN R155 and UN R156. The purpose of this document is to standardize audit expectations and help companies as well as technical services to prepare for audits. In Germany, technical services are also faced with dedicated requirements in the context of the KBA procedure according to UN R155 and UN R156 [356] and use this as a starting point for conducting audits.

Part A of the document provides general requirements for management systems that are independent of cybersecurity or software updates. Part B lists specific requirements for CSMS/SUMS. Requirements from both regulations are combined and structured into 5 sections:

1. General requirements for CSMS/SUMS and planning CSMS/SUMS
2. Risk Management
3. Requirements for processes
4. Other requirements according to UN-R 156
5. Monitoring and measuring

Unlike the VDA ACSMS, the KBA catalogue is publicly available and free of charge [343].

For companies that have to start from scratch in establishing a CSMS or SUMS, the requirements in part A of the catalogue can be quite helpful in assessing the status of the overall quality management system and whether the basis for a CSMS and SUMS is in place.

2.2.4.4. ENX Vehicle Cybersecurity Audit Scheme

The ENX Association (formerly the European Network Exchange Association) has also provided a questionnaire for vehicle cybersecurity audits. This is called the Vehicle Cybersecurity Audit (VCSA) and is designed to provide a basis for self-audits, audits by internal departments, and audits within the ENX 3rd party framework.

It is much more comprehensive than the VDA and KBA publications. It contains not only mandatory requirements, but also recommendations, further related information, and the names of possible references. The requirements and recommendations are not only based on UN R155 and ISO/SAE 21434, but also consider additional contributions from ISO 19011 (Guidelines for Auditing Management Systems), ISA (VDA Information Security Assessment), ISO/PAS 5112 (discussed in more detail later in this section), a VDA position paper on Cybersecurity Interface Agreement, and the VDA ACSMS document mentioned above.

As of now, the questionnaire is structured as follows:

1. Organizational Cybersecurity
2. Human Resources – Cybersecurity Culture
3. Risk Management
4. Internal Assessments
5. Concept and Product Development Phase
6. Post-Development (excluding Operations and Maintenance)
7. Operations Security
8. Incident Management
9. Supply Chain Relationships

This questionnaire is the most comprehensive. And it is a good tool especially for companies and audits that aim for a holistic approach that is fully integrated into a company's management system. Like the KBA catalogue, this document is publicly available free of charge [342].

2.2.5 Further automotive cybersecurity standards

Now that the ISO standards that were developed in the working groups have been in use throughout the industry for several years and are being applied in daily practice, the first feedback, experiences, and needs for improvement from the industry's point of view are available. These relate on the one hand to specific fields of action from a cybersecurity perspective and on the other hand to practical application in the automotive environment. Further specifications in the form of separate standards for specific topics have been identified.

2.2.5.1 ISO/SAE PAS 8475 Cybersecurity Assurance Level

According to experts, publication of the second edition of ISO/SAE 21434 cannot be expected until 2028 at the earliest. Solutions must therefore be found for precisely those areas that are not adequately covered in the first edition. A joint effort between ISO and the SAE committee is therefore already focusing on improving and clarifying the most pressing issues that are missing in the current edition of ISO/SAE 21434.

One such topic is clarification of the use of Cybersecurity Assurance Levels (CAL) which appear as a proposal (not a requirement) in Annex E of the current edition of ISO/SAE 21434. Several companies and experts in the industry have found the purpose of the CAL beneficial, but the lack of clear guidance and a standardized approach has led to it not being widely adopted. The main goal of CAL is to specify and communicate a set of activities not only internally, but also between supplier and customer relating to the level of rigor that is required in order to provide sufficient assurance that the cybersecurity engineering of an item is fit for purpose.

As one can imagine, some components are more cybersecurity-relevant than others. They may be more likely to be compromised, and/or the impact of any compromise may be greater. One goal of ISO/SAE PAS 8475 is therefore to provide guidance on how to select the appropriate CAL level for an item or component and on the activities that should be carried out, given the level that has been selected.

To help with the CAL concept, another attribute has been introduced that was not mentioned in the 1st edition of ISO/SAE 21434, i.e. targeted attack feasibility (TAF). TAF describes the expected level of attack feasibility for an item or component and rates the expected attack feasibility of an item or component after cybersecurity controls have been assigned to it. When performing the TARA, it is possible to end up with different evaluations of the same attack path. TAF can help with the comparison of TARA results and the derivation of the appropriate technical requirements, especially in the coordination between customer and supplier

When we consider the roles of both attributes, CAL and TAF, it becomes clear that a pressing issue in automotive cybersecurity is communication between customers and suppliers, especially when it comes to how cybersecurity is to be implemented and verified. The ISO/SAE PAS will serve as optional guidance for customers and suppliers when they are communicating about the attributes of the products concerned. This will simplify the process of selecting the appropriate cybersecurity controls for each product and determining how much verification and validation needs to be done.

Please note that this standard is still under development towards the end of 2024. At this point in time, official announcements and information are still pending. All details given here are based on discussions with experts involved in the creation of the document. The standard may be subject to further changes or adjustments.

2.2.5.2 ISO/SAE TR 8477 Cybersecurity Verification & Validation

Another pressing issue that has already been mentioned is the cybersecurity verification and validation process. Although the first edition of ISO/SAE 21434 contains several requirements and examples of verification and validation (V&V) activities, there is still an ongoing discussion about the methods that will be required and the division of responsibilities between customer and supplier. This technical reference aims to clarify open issues and provide a consistent and unified definition of V&V in the context of cybersecurity, together with examples for each of the activities. Like ISO/SAE AWI PAS 8475, this standard is at an early stage of development but is eagerly awaited by many companies.

2.2.5.3 Automotive SPICE for Cybersecurity

Introduction to Automotive SPICE

Automotive Software Performance Improvement and Capability Determination (ASPICE) is the domain-specific variant of the international standard ISO/IEC 15504 Software Process Improvement and Capability determination (SPICE). Market demand is pushing for increasingly complex innovations that are environmentally friendly, safe, economic, and user-friendly, all within ever shorter timeframes. This, combined with growing reliability requirements, makes it essential to monitor and improve the development processes in software-based system development. Process models for development can help to tackle the challenges in these situations. ASPICE is one such model that consists of two dimensions:

- The process dimension describes (in the newest version 4.0) 32 processes and how each with its specific requirements should be conducted in a project
- The capability dimension describes the Capability Level (CL) for rating the capability of a process

Cybersecurity Extension

New processes specifically related to cybersecurity were added to the existing ASPICE model. These new additional processes mostly relate to three different areas. The first area is supplier management, especially the evaluation and selection of suppliers. Secondly, new processes for development activities have been defined which apply to both sides of the V-model, i.e. the specification and implementation of cybersecurity on the one hand and, on the other hand, the integration, verification, and validation of cybersecurity. Last but not least, cybersecurity has its own risk management process.

Note: Pages missing in this reading sample

This reading sample is only an excerpt from the publication “1000 Things Worth Knowing in Automotive Cybersecurity” and contains only selected pages as a preview. The full reading experience is available in the complete publication.

CYBERSECURITY MANAGEMENT

4.

4. CYBERSECURITY MANAGEMENT

The management of cyber risks throughout the product lifecycle has become crucially important for organizations in the automotive industry. This means that there is a strong need to establish cybersecurity processes in the form of new work practices. This entails creating a cybersecurity management system which includes rules and processes, roles and responsibilities for the assessment and management of cybersecurity risk to vehicles, its functions and components [49]. The development of cybersecurity management entails various activities that focus on the integration of cybersecurity throughout the organization and the supply chain. Cybersecurity management is required at two different levels [145]:

a. At the organizational level, cybersecurity management includes activities throughout the realm of corporate governance. The aim of these activities is to develop and implement operational strategies and continuous management procedures for overall cybersecurity.

b. At the project level, cybersecurity management includes activities that are carried out during the development and post-development phases of the product.

On the one hand, cybersecurity management at the organizational level is independent of, and provides a framework for, product development. On the other hand, project-level cybersecurity management must be applied to each new development project. The timelines for carrying out cybersecurity activities during different projects can be independent of each other, depending on the project objectives.

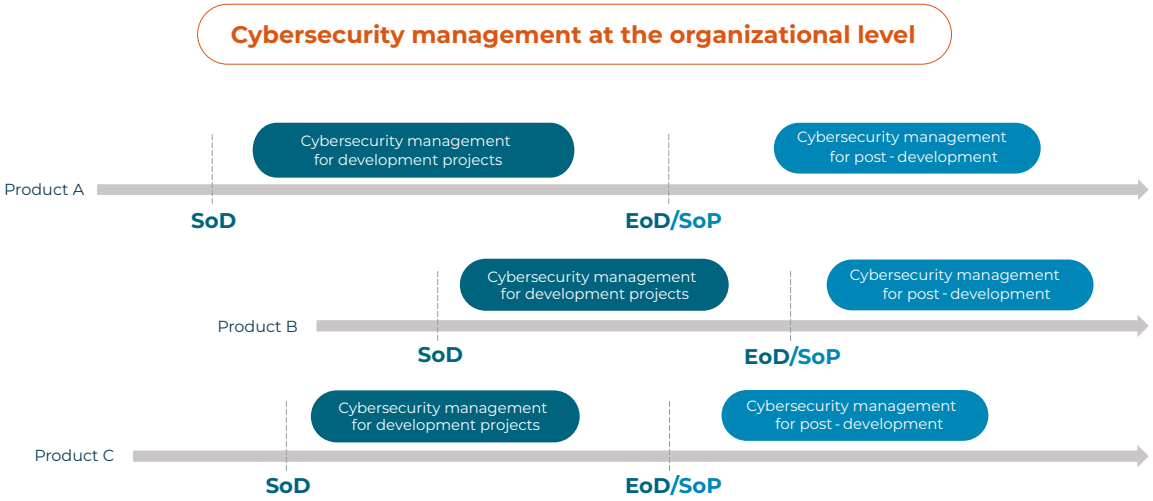


Figure 4.1 Aspects of cybersecurity management

4.1 Cybersecurity management at the organizational level

Cybersecurity management at the organizational level can be divided into creating the preconditions for organizational cybersecurity, ongoing cybersecurity activities, and supporting processes. According to NIST, the need for trusted and secure frameworks has never been more vital to an organization's long-term economic interests and also to national security interests, due to the continuing frequency, intensity, and negative consequences of cyberattacks, disruptions, threats, and other hazards [234]. This section describes and interprets the cybersecurity management requirements that must be met by the organization.

All the activities described in this chapter are required or at least helpful in the process of obtaining a certificate of compliance in accordance with UN R155 and ensuring compliance with GB 44495.

4.1.1 Pre-conditions for organizational cybersecurity

The pre-conditions for organizational cybersecurity encompass activities that need to be performed by the organization to enable projects to integrate cybersecurity into the phases of product development. If companies do not fulfill the pre-conditions, the projects lack orientation or guidance on how to handle cybersecurity. As a result, project teams are forced to try to solve problems on their own using unplanned effort and resources. This has a major impact on time and cost planning, due to the failure to meet pre-conditions.

4.1.1.1 Cybersecurity policy

A cybersecurity policy is the starting point for every company when establishing cybersecurity. And it is the very first requirement of ISO/SAE 21434: **RQ-05-01**. It can be regarded as an intellectual strategic plan for defining and achieving cybersecurity in an organization [74] [234].

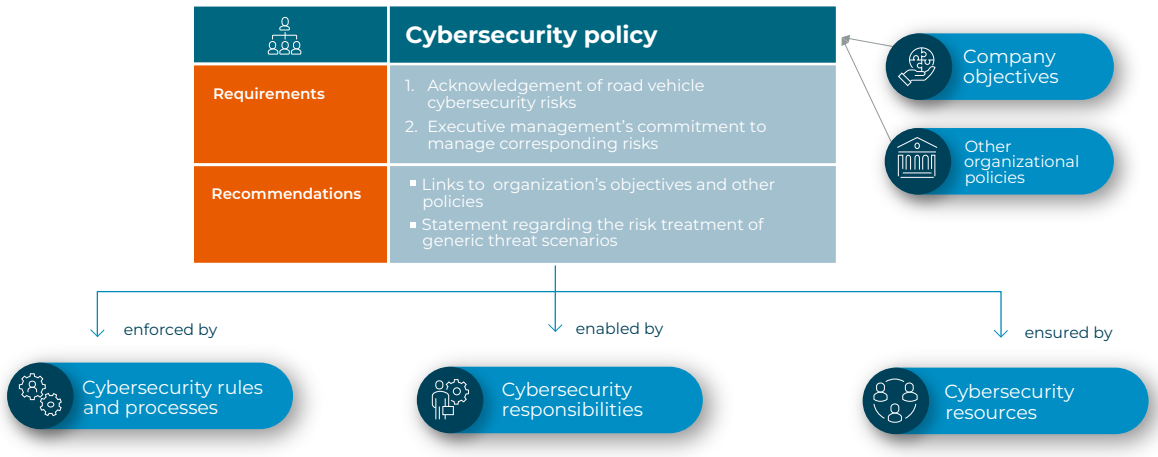


Figure 4.2 Cybersecurity governance according to ISO/SAE 21434

The cybersecurity policy incorporates the identification of road vehicle cybersecurity risks and an expression of executive management's commitment to mitigating those risks, as shown above. Executive management needs: to act as a role model; to ensure that cybersecurity mitigations are implemented throughout the organization; and to mitigate the concerns of employees when necessary. The cybersecurity policy is considered mandatory, because it enables executives to monitor cybersecurity in an organization. The cybersecurity policy needs to be linked to the organization's goals in order to ensure consistency with other company objectives. The policy should also define a strategy for reaching goals dedicated to addressing cybersecurity as part of the organizational goals. This enables the organization to understand the need for cybersecurity, and to assess risks, set targets, plan employee training, and seek expert advice [254]. The finalized cybersecurity policy then needs to be used as a basis for framing other internal policies and the policies of associated organizations, e.g. partners, sub-contractors, suppliers, vendors, and consultants. The organizational cybersecurity policy is then [145] [234]:

- enforced by establishing cybersecurity rules and processes which are to be followed as part of day-to-day work
- enabled by the assignment of cybersecurity responsibilities which are defined, e.g. in a responsibility matrix which includes all the stakeholders involved
- ensured by the provision of cybersecurity resources which need to be identified, assessed, aligned, and assigned to build up the required skills of the workforce, e.g. talents, tools for cybersecurity

The cybersecurity policy has a huge impact on the implementation of organizational goals and also on employees because it is made visible to everyone and reflects the approach of the organization to the handling of cybersecurity. It builds the trust of employees, raises their awareness, and serves as a source of orientation.

Every company should have a clearly defined cybersecurity strategy, which is communicated to all its stakeholders as part of the organizational cybersecurity policy.

> A real, hand-written signature from senior management (e.g. CEO, CTO) and making the policy visible to everyone (e.g. printing and posting around the office) will help to emphasize the importance of the policy and the seriousness of the issue

4.1.1.2 Cybersecurity rules and processes

RQ-05-02 requires every organization to establish its own specific rules and processes for implementing the cybersecurity policy. This serves to facilitate the implementation of the requirements of ISO/SAE 21434 and also to support the execution of the corresponding activities.

Let us start with a brief general overview of a process. A process can be defined as a series of steps that are taken in order to reach a certain goal. Processes are a fundamental element in any organization, as they ensure a systematic and consistent approach to work and a common understanding, regardless of the teams, products, or time frames involved. As a result, processes support the effectiveness of teams by clearly defining the tasks that need to be completed and helping to prevent mistakes. They also support onboarding activities by providing guidance on how to perform specific tasks.

A process is more than just the combination of a few activities into a workflow, however. It consists of inputs and outputs that are usually interdependent and also have an impact on other processes (cybersecurity and non-cybersecurity). It is always essential to look at the big picture because cybersecurity processes cannot be created in isolation from the overall context.

Processes can be classified according to different levels: purpose, goals, and strategy ("why"); procedure ("what"); method ("how"); and means (“whereby”) (see figure below). The classification of processes is often part of automotive standards, but not all standards cover all the levels listed above.

For instance, ISO 26262 covers “why”, “what” and, to some extent, “how”, whereas ISO/SAE 21434 and UN R155 stop at “what” and do not prescribe any requirements as regards the “how”. This limitation as regards "how" to apply the requirements is covered in other automotive standards such as ASPICE. Hence there is a need for synergy between ISO/SAE 21434 and ASPICE in order to ensure that cybersecurity is integrated into the overall process landscape of a company.

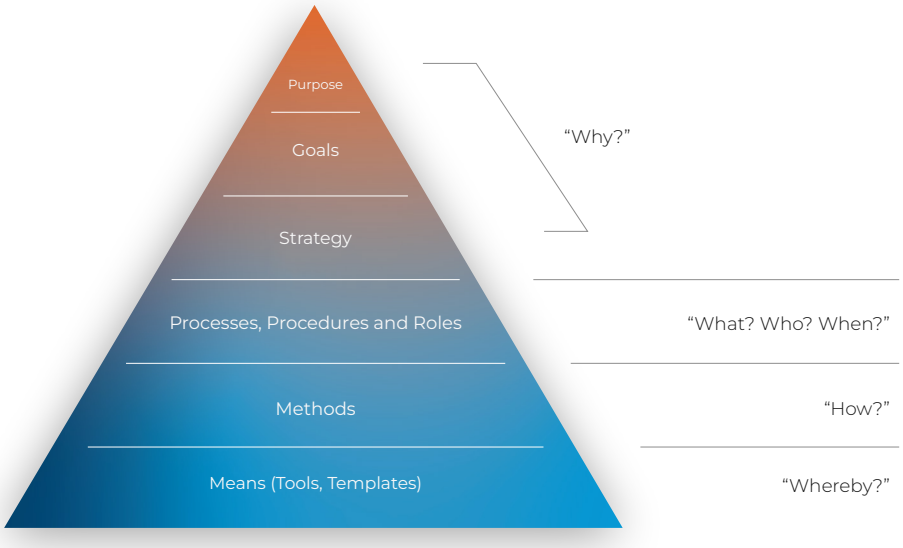


Figure 4.3 Process pyramid

Experiences and developments are evolving rapidly in the field of automotive cybersecurity, so defining roles and processes is not a one-off task. It requires an iterative methodological approach, which involves defining, establishing, assessing, and improving processes as outlined here:

- **Defining the process** starts with the definition of process goals in accordance with various standards and the needs of stakeholders. The definition of a process addresses the existing ways of working that need to be considered in order to obtain the acceptance of users involved in the process.
- **Establishing the process** includes piloting and requires staff training.
- **Assessing the process** involves measuring the feasibility of reaching the goals, checking for compliance with relevant standards (in this case ISO/SAE 21434), and assessing the efficiency and practicality of the process.
- **Improving the process** involves correcting any weaknesses that may be identified and taking steps to increase efficiency.

The cybersecurity process needs to be aligned with all the other relevant management systems (e.g. QMS) and their processes, such as requirements management, project management, testing processes, and supporting processes. For the purposes of this alignment, the identification and coordination of interfaces with other processes are crucial. The cybersecurity process is connected with other relevant processes, so it cannot be created independently. To create a process that is secure and can be trusted, it is necessary to follow an iterative approach in order to identify the constraints imposed by different interfaces, interconnections, and interactions [234]. If cybersecurity processes are not defined and followed, both the project and the organization will be exposed to serious risks.

Compared to other industries, the automotive industry has a high demand for processes and many standards. This is due to the complexity of the products (e.g. a passenger car has more lines of software codes than a jet), the high number of units per product (e.g. more than a million cars of one model), and the fatal consequences (in case of malfunctions, people could die).

The following are examples of risks which might arise if cybersecurity processes are lacking in a project:

- Risk of misalignment between engineers and projects due to different ways of working
- Risk of isolated and parallel intermediate processes due to project-specific solutions
- Risk of mismanagement due to a lack of integration of cybersecurity in project planning
- Risk of incomplete satisfaction of cybersecurity requirements and regulations due to a failure to identify interfaces between cybersecurity engineering and requirements management
- Risk of introducing technical weaknesses and vulnerabilities due to a lack of processes for gaining the acceptance of requirements and implementation
- Risk of delivering an insecure product to clients due to a lack of consideration of cybersecurity in testing processes and procedures
- Risk of failing to comply with agreements/contracts due to a lack of incident management processes during the life of the product

4.1.1.3 Resources

In requirement **RQ-05-04**, ISO/SAE 21434 requires organizations to provide the resources to address cybersecurity. Resources usually refers to both people (human resources) and infrastructure. Human resources include all the people who are responsible for performing activities, e.g. during cybersecurity development and during risk and incident management [145]. Infrastructure includes quality management, purchasing and service, tools, information and knowledge management systems, guidelines, budget, and other infrastructure that is required in order to carry out the cybersecurity project activities [145][224].

One might argue that only one role is needed, i.e. that of cybersecurity manager. However, this is not enough. Additional cybersecurity resources are needed for setting up the cybersecurity organization. This includes building a cybersecurity core team, which establishes and coordinates cybersecurity throughout the company, assigns responsible persons to act as experts on particular subjects, and defines new technical cybersecurity teams (testing, incident handling). In addition to this, resources are required in order to build competence and know-how by training and coaching team members and through participation in conferences and joint working groups. Cybersecurity resources are also required

Note: Pages missing in this reading sample

This reading sample is only an excerpt from the publication “1000 Things Worth Knowing in Automotive Cybersecurity” and contains only selected pages as a preview. The full reading experience is available in the complete publication.

CYBERSECURITY RISK ASSESSMENT

6.

6.1 Asset Identification

TARA is a method for the optimal direction of efforts to ensure cybersecurity. Asset identification assists this direction of efforts by systematically identifying which elements of the cybersecurity item need to be protected.

A cybersecurity asset is an entity of the system for which a loss of cybersecurity properties may lead to non-negligible damage to the interests of a stakeholder. Such an asset may be a component, data, an input, software, or any other informational entity with at least one cybersecurity attribute (e.g. confidentiality, integrity, or availability) which enables it to fulfill its mission. Conversely, an asset is not a cybersecurity asset, if its compromise does not lead to significant harm to the interests of stakeholders – e.g. a debug log file on an automotive ECU may be compromised by a cyberattack, but its loss of function does not lead to any harm to a stakeholder's interests that would warrant further attention.

In the general risk assessment according to ISO/SAE 21434, only the road-vehicle user is considered as a stakeholder, but it is recommended to extend the scope to include additional stakeholders, such as organizations, like the OEM, supplier and other parties who might be impacted.

Whether a physical or informational entity is cybersecurity relevant may not be immediately obvious, so the adoption of a formal, structured approach to asset identification is recommended. The approach that is adopted needs to have the following properties:

- Completeness: Use of the approach must provide reasonable assurance that no potential assets have been overlooked.
- Repeatability: Multiple persons using the approach on the same cybersecurity item should obtain the same results.

The next section will focus on an asset identification approach which we recommend on the basis of practical experience gained over many years of automotive consulting.

The overall process of asset identification is shown in the figure below and discussed in the following section.

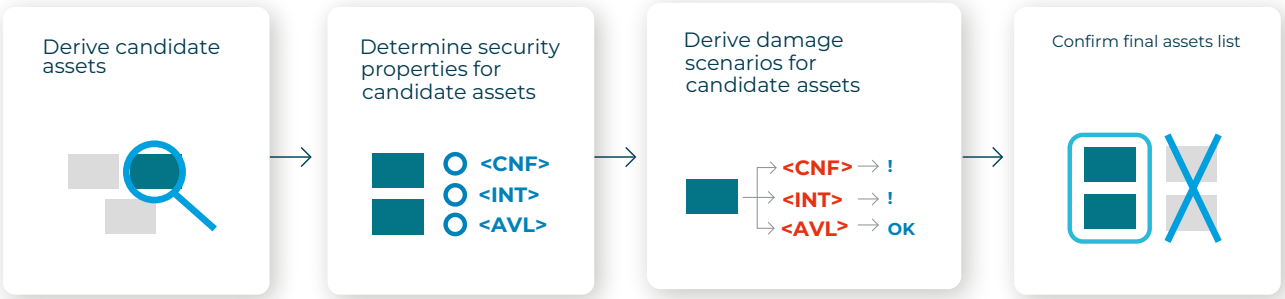


Figure 6.2 Recommended process for asset identification

6.1.1 Derive candidate assets

When the essential properties of an asset derivation process have been identified, the next step is to formally define a method for deriving assets from a cybersecurity item. Bearing in mind that "security-by-design" is a recommended design practice, the asset derivation approach should ideally be applied before significant systems design decisions are made. To accommodate possible variations in project maturity when performing asset identification, two distinct approaches are recommended for determining candidate cybersecurity assets: a functional approach and a technical approach.

The functional approach is recommended for early product development stages when no clear technical solutions have been agreed, but an overall functional architecture covering the whole cybersecurity item is available as a minimum. Using the functional approach entails performance of the following actions on the overall functional systems architecture (i.e. a diagram or description which outlines the system's functions and interactions, focusing on meeting requirements and guiding the selection of the components that are needed):

- identification of each instance of information transfer within the cybersecurity item scope, as a candidate asset,
- identification of each instance of information transfer across the in/out boundary of the cybersecurity item scope, i.e. the inputs and outputs, as a candidate asset,
- identification of each instance of information generation within the cybersecurity item scope, including the functionality of providing outputs based on the inputs, as a candidate asset,
- identification of each instance of information transformation within the cybersecurity item scope, as a candidate asset.

To get an idea of the functional approach in action, consider the example of the system architecture for an airbag control unit, as illustrated below:

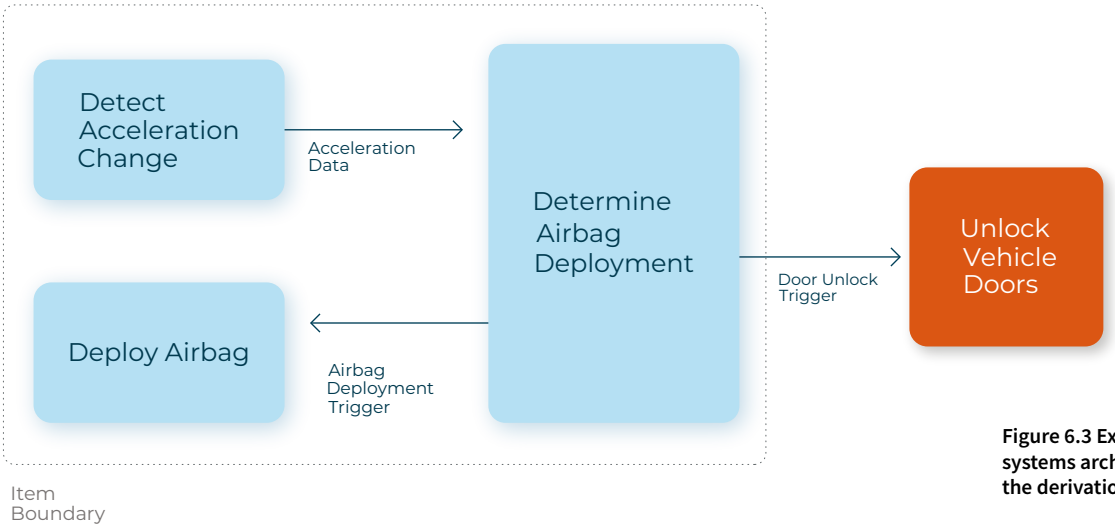


Figure 6.3 Example of functional systems architecture to be used for the derivation of candidate assets

When observing the architecture, two instances of information transfer within the item scope can be seen: transfer of acceleration data and transfer of the airbag deployment trigger. Both architectural elements are listed as candidate assets. One instance of information transfer across the item boundary can be seen in the form of the transfer of the door unlock trigger, which is then also listed as a candidate asset. Information generation in the sample architecture happens in the detect acceleration change function (creation of acceleration data), while information transformation happens in the determine airbag deployment function (transformation of acceleration data into airbag deployment and door unlock triggers) and the deploy airbag function (transformation of airbag deployment trigger into airbag activation). All three of these functions are listed as candidate assets. Note that the unlock vehicle doors function also performs information transformation but is outside the cybersecurity item scope, and is therefore not a candidate asset.

Furthermore, since all the candidate assets that are listed are interconnected, it can be beneficial to combine them into a single asset, in this case, "Airbag Deployment Function". This makes the assessment less detailed but saves time and resources without losing the fundamental advantage of the functional approach. It is important to remember that TARA has a so-called "tree structure", which means that an increase in the number of assets will cause an exponential increase in the size of the TARA as a whole. It is therefore necessary to find a good compromise between the degree of detail and sufficiently broad coverage.

The technical approach is better suited to the analysis of relatively mature systems, in which some software and hardware design decisions have already been made. A prerequisite for use of the technical approach is that software and hardware block diagrams should be available for analysis using the following steps:

- Identification of each software block within the cybersecurity item scope, as a candidate asset
- Identification of each instance of data transfer between software blocks, where at least one block is part of the cybersecurity item scope, as a candidate asset
- Identification of each hardware block within the cybersecurity item scope, as a candidate asset

To get an idea of the technical approach, consider the example of a technical architecture illustrated below:

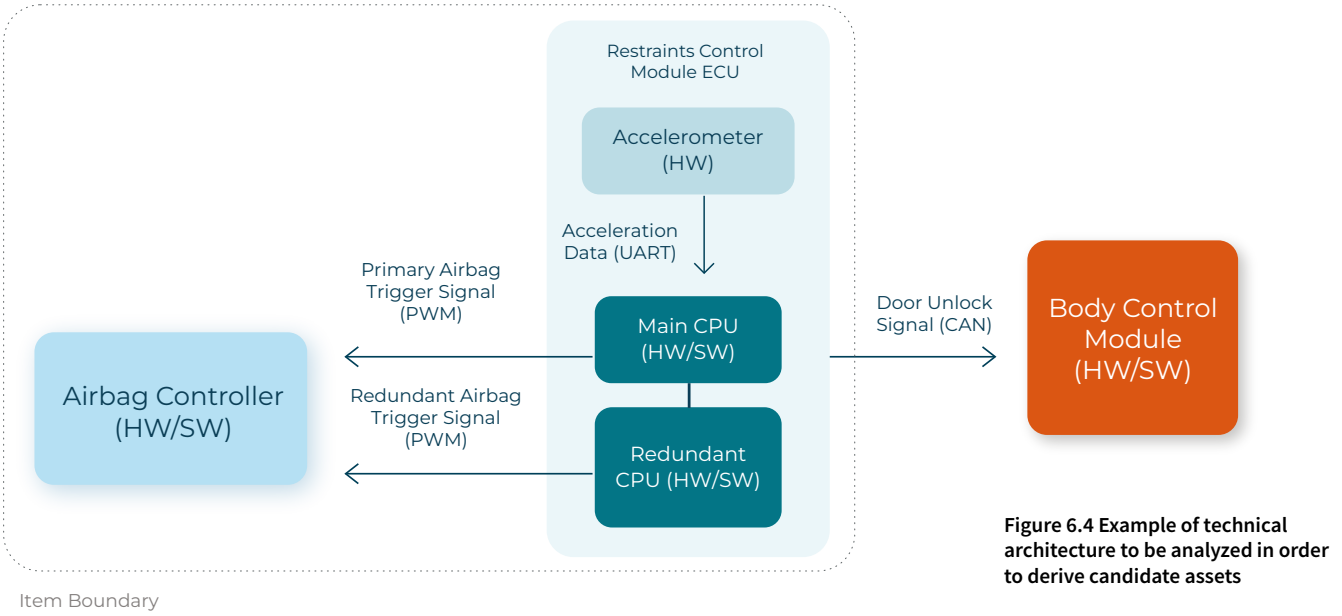


Figure 6.4 Example of technical architecture to be analyzed in order to derive candidate assets

Looking at the architecture illustrated above, three components can be identified as software blocks: the airbag controller, the main central processing unit (CPU), and the redundant CPU. While none of the listed blocks is a software-only block, they all contain notable software parts that need to be listed as candidate assets. The body control module also contains notable software parts but is not part of the cybersecurity item and is therefore not a candidate asset. Four instances of data transfer can be seen in the sample architecture: the acceleration data signal, the primary and redundant airbag trigger signals, and the door unlock signal. All of these are listed as candidate assets. Finally, the four hardware blocks within the cybersecurity item boundary — the accelerometer, the airbag controller, the main CPU, and the redundant CPU — are listed as hardware candidate assets.

Using either of the two approaches outlined above should result in the identification of a list of candidate assets. The next step in the asset identification method provides an answer as to whether an identified candidate asset has enough cybersecurity relevance to warrant its inclusion in risk assessment.

There is no one way to identify assets. This activity depends on the company, the product, and also the experience of the cybersecurity engineer performing this analysis. Therefore, it is common for a first draft of asset candidates to be refined as the TARA progresses and also as the understanding of the system grows.

6.1.2 Determination of security properties

As explained in the introduction to asset identification, a candidate asset is judged to be cybersecurity relevant, if it possesses cybersecurity properties, the loss of which would lead to harm to the interests of stakeholders. Before assessing whether the loss of cybersecurity properties leads to harm, it is necessary to choose which cybersecurity properties belong to the cybersecurity element. Once a general choice of cybersecurity properties has been made, each candidate asset can then be assessed as to whether it possesses at least one of the chosen cybersecurity properties.

Note: Pages missing in this reading sample

This reading sample is only an excerpt from the publication “1000 Things Worth Knowing in Automotive Cybersecurity” and contains only selected pages as a preview. The full reading experience is available in the complete publication.

CYBERSECURITY CONTROLS

8. CYBERSECURITY CONTROLS

At the most fundamental level, cybersecurity is about protecting things that are of value to an organization - in other words, the organization's assets [312]. That generally includes tangible assets such as products, raw material, property, money or people and intangible assets, also known as organizational capabilities, such as business processes or client relationships. Cybersecurity controls can help organizations protect these assets. They can take any form of policy, procedure, technique, method, solution, plan, action, or device design [312]. However, when it comes to deploying cybersecurity controls, organizations face several questions. How does one select the right cybersecurity controls for the organization and its products? How can organizations determine whether the selected controls provide an appropriate level of protection for an item or component? To answer these questions, automotive players must first understand what cybersecurity controls are, before they can begin selecting controls using the risk management approach and lifecycle-based cybersecurity engineering process proposed by ISO/SAE 21434. This chapter presents the fundamental concepts associated with cybersecurity controls, including their definition, their relationship to cybersecurity risks, approaches to their selection, and special derivatives of controls for the automotive industry.

8.1 What are cybersecurity controls?

Automotive organizations can generally distinguish between two categories of controls: conventional IT security controls and automotive cybersecurity controls designed specifically for automotive products. NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, provides a definition of security controls that is commonly accepted in the traditional IT security world [102]. According to this publication, IT security controls can be viewed as descriptions of the safeguards and protection capabilities that are appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of the organization's stakeholders. IT security controls, such as user authentication and antivirus software on workstations, serve as the foundation for the secure development, production, and operation of automotive products. They are outside the scope of ISO/SAE 21434 because they are not related specifically to automotive products (e.g. vehicles, ECUs, and embedded software). They are addressed in other standards and recommended references. Some of the most common ones are described later in this chapter.

SAE J3061 has been largely superseded by ISO/SAE 21434, but it is still a relevant source in the automotive cybersecurity landscape. It provides a definition of automotive-specific cybersecurity and defines cybersecurity controls as management, operational, and technical controls (e.g. safeguards or countermeasures) that are prescribed for an item to eliminate potential vulnerabilities or to reduce the likelihood that a vulnerability will be exploited [237]. This definition focuses on the application of cybersecurity controls that are specifically tailored to the unique products of the industry, such as ECUs or the entire connected vehicle. The main objective of these controls is to safeguard the product's assets from potential threats, and thereby to protect the organization and its assets against the potential negative consequences that could result from a cyberattack.

ISO/SAE 21434 provides an automotive-specific definition that sums this up: a cybersecurity control is a measure that modifies risk.

8.2 Cybersecurity requirements and controls

The ISO/SAE 21434 definition of cybersecurity controls highlights the need for them because they are the very means of addressing and mitigating cybersecurity risks in the automotive industry and its products. The selection, design, and implementation of cybersecurity controls can have a significant impact on the operations and assets of organizations and on the well-being of their customers [102]. However, ISO/SAE 21434 does not provide a concrete answer to the question of what cybersecurity controls are needed to adequately manage cybersecurity risks and how such controls should be implemented. Instead, it provides a disciplined and structured approach to the definition of cybersecurity controls in the context of the organization's particular structure, products, and business cases. This approach is similar to that provided in NIST SP 800-53 [102].

At this point, it is crucial for automotive players to understand the relationship between cybersecurity requirements and cybersecurity controls. Cybersecurity requirements, broadly speaking, may refer not only to the cybersecurity and privacy obligations imposed on organizations but also to a statement of the stakeholder protection needs for a particular system or organization. They can be derived from multiple sources, including relevant legislation, executive orders, directives, regulations, policies, standards, stakeholder requirements, and the cybersecurity goals identified during a risk assessment according to ISO/SAE 21434. As shown below, cybersecurity requirements are collected and specified in the cybersecurity concept for an item or component in accordance with the description of relevant cybersecurity controls, in order to realize the cybersecurity goals that have been identified. Cybersecurity requirements describe how cybersecurity should be implemented within the overall item or component, taking into account the architecture and further specific non-cybersecurity requirements. Cybersecurity requirements should, of course, also fulfill the characteristics of well-written requirements, such as feasibility, consistency, necessity, measurability, clarity, and freedom from ambiguity.

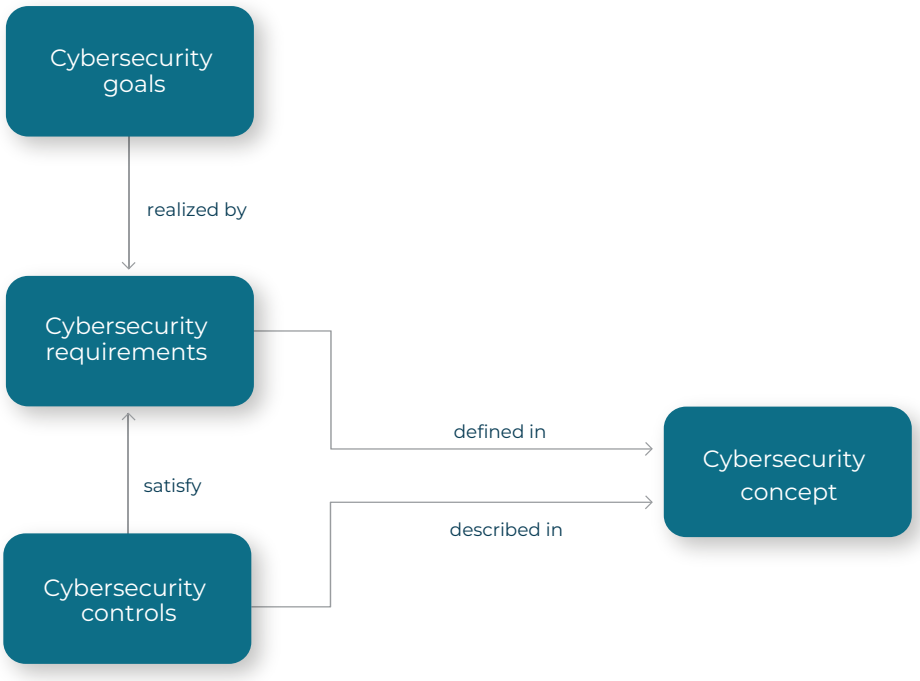


Figure 8.1 Relationship between cybersecurity requirements and controls

Cybersecurity controls, as opposed to cybersecurity requirements, are derived from the cybersecurity goals or from the cybersecurity specification at a higher level. They should therefore be selected with reference to the cybersecurity requirements and the architectural design laid down at the higher level and with reference to the product-specific risks that have been identified and are to be reduced. When searching for appropriate controls designed to mitigate the risk to a specific asset and help satisfy associated cybersecurity requirements, cybersecurity controls should not be arbitrarily selected and implemented. According to ISO/SAE 21434, they shall flow out of an organization's cybersecurity engineering and risk management process that identifies risk reduction measures that can be applied to reduce risks to an acceptable level, as defined by the organization. In other words: cybersecurity controls are company and product specific and are needed to achieve the cybersecurity goals.

Once an organization has selected technical and/or operational controls, the controls and how they interact to satisfy cybersecurity requirements and achieve cybersecurity goals must be described and documented. When describing the selected controls, organizations must consider the dependencies between the functions of the item and/or the stated cybersecurity claims. The description may include conditions for achieving cybersecurity goals (e.g. preventing, detecting, and monitoring compromise). It may also include functions dedicated to specific aspects of threat scenarios (e.g. using a secure communication channel).

ISO/SAE 21434 requires a cybersecurity concept but does not describe in detail what this should look like. Therefore, different interpretations exist within the industry.
One interpretation is as follows: The description of selected cybersecurity controls complements the specification and allocation of cybersecurity requirements and of requirements regarding the operational environment, which all together constitute the cybersecurity concept.

Another essential step is to ensure that the cybersecurity controls selected and implemented by an organization or within a particular project actually do their job. They should:

- satisfy the cybersecurity requirements imposed on the system or organization, and
- help achieve the cybersecurity goals by reducing the cybersecurity risks to an acceptable level as defined by the organization.

According to ISO/SAE 21434, this is ensured by appropriate cybersecurity verification and validation. This is discussed in detail in Chapter 9. The description of cybersecurity controls can be used to evaluate designs and identify targets for cybersecurity validation.

8.3 Selection of cybersecurity controls

To ensure compliance with ISO/SAE 21434, the actual selection of cybersecurity controls must reflect the cybersecurity goals and how these goals mitigate the respective risks. As indicated in the previous section, cybersecurity goals are achieved by technical and/or operational cybersecurity controls which are derived to cybersecurity requirements. The risk-based flow of ISO/SAE 21434 therefore forms the foundation for possible subsequent approaches to selecting cybersecurity controls.

The following sections focus on the risk framework used by ISO/SAE 21434 and potential approaches that may be based on it. Automotive organizations can use this risk framework to effectively derive and select cybersecurity controls from individual cybersecurity risks and requirements. In addition, several methods for classifying controls are described. These methods of classification can help to reduce the number of cybersecurity controls that are required for addressing a particular risk.

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

It is impossible to determine in advance all the potential threat scenarios that an automotive project will face, because the motivation and capabilities of adversaries are unpredictable. To overcome this challenge, automotive organizations need to continuously find out whether, where, and how their products are vulnerable, what damage is associated with each threat, and how they can deal with the impact of the threats and the emerging cyber risks. As a result, risk assessments, such as the TARA for the concept phase, are at the core of cybersecurity engineering and the development of an item or component in accordance with ISO/SAE 21434. The individual steps and elements of the risk-based approach to automotive cybersecurity engineering defined by ISO/SAE 21434, e.g. item definition, TARA, and cybersecurity concept, have already been described in detail in the corresponding sections of this book. However, this approach is summarized below to make the basis for the selection of cybersecurity controls more tangible:

1. **Item definition** defines the cybersecurity scope of a system or combination of systems by identifying its function, interfaces, operational environment, and interaction with other systems.
2. **Asset identification** identifies the assets belonging to an item that are worth protecting, assigns cybersecurity properties, and identifies damage scenarios, e.g. the worst possible scenario following an incident in which cybersecurity properties are compromised.
3. **Impact rating** evaluates the impact of damage scenarios according to the consequences that they may have for stakeholders.
4. **Threat scenario identification** examines selected assets and identifies general means by which assets can be compromised.

5. **Attack path analysis** identifies potential attack paths (i.e. the various steps performed by a hacker) and links them to one or more threat scenarios.
6. **Attack feasibility rating** assesses the feasibility of attack paths based on the ease of attack.
7. **Risk value determination** combines the impact of the damage and the feasibility of attack to determine a risk value for each threat scenario.
8. **Risk treatment decision** determines how the risk will be treated by selecting a suitable risk treatment option (avoidance, mitigation, sharing, transfer to third parties, or acceptance).
9. **Cybersecurity goals** and claims are specified on the basis of the outcome of the risk assessment and decisions about how to ultimately deal with the risks.
10. **Cybersecurity concept** is derived from the cybersecurity goals and specifies how the goals are to be met in practice by cybersecurity controls which assign the goals to the components of the item.

Following the completion of a TARA, the cybersecurity concept will serve as the primary work product for deciding which controls shall be established. As the results of the individual steps described above build on each other, the concept specifies the cybersecurity controls for the cybersecurity goals and thus defines how the identified risks to an item or component are to be managed effectively. On the basis of this information, the project can begin to decide what controls need to be put in place to ensure, on the one hand, that no residual risks remain – this can be done by making sure that all the cybersecurity goals and external cybersecurity requirements are addressed – and, on the other hand, that there is no overreaction to risks, because this would lead to the over-engineering of solutions. The following section describes two key approaches that can help organizations select cybersecurity controls.

8.3.2 The need for control selection approaches

As already mentioned, ISO/SAE 21434 neither provides a concrete approach for control selection, nor does it list actual cybersecurity controls. It only defines the risk-based process laying the foundation and creating the prerequisites for their selection. This flexibility is necessary to enable effective management of cybersecurity risks and to ensure that automotive players meet their cybersecurity due diligence obligations. As a result, organizations do not need to commit to a single approach to selecting controls but can choose the appropriate approach or combination of approaches depending on the circumstances [235]. Nevertheless, organizations need to establish an approach that enables them to select and implement controls in a [illegible] and cost-efficient manner and allows them to include

You have reached the end of this online reading sample.

The complete publication, "1000 Things Worth Knowing in Automotive Cybersecurity," has a total of nine chapters with +300 pages of practical expertise on ISO/SAE 21434, UN R155, and beyond. Purchase the entire publication or individual chapters online now.

Discover full publication at CYEQT Knowledge Base.

www.cyeqt.com

cymetris

Get access to

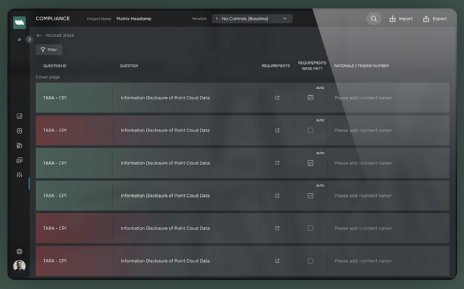
Cybersecurity Engineering next level

Software-based TARA risk analysis for your development project. **More structured, powerful and industry compliant.**

Discover the cybersecurity risk analysis of the future: the CYMETRIS solution takes the implementation of your Threat Analysis and Risk Assessment methodology (according to ISO/SAE 21434) to a new level. With intelligent features, well-designed functionality and a focus on efficiency, it bridges the gap between development efficiency and industry-specific cybersecurity requirements. For Original equipment manufacturers and suppliers. Ensuring the cybersecure future of mobility.

Find out more information

cymetris.com

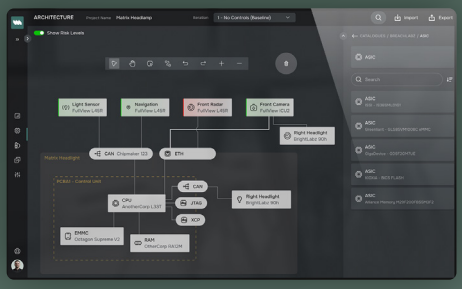


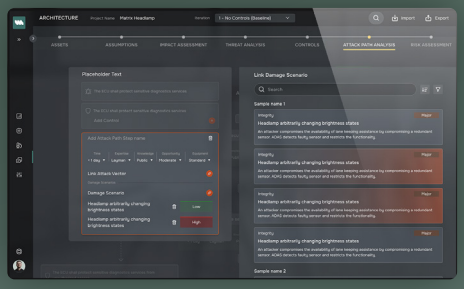
Tool-based compliance checking with UN R155, ISO/SAE 21434 and beyond

How would it be if you could simultaneously accelerate your software-based execution of TARA and take steps towards compliance and consistent application of industry standards and relevant regulations? The CYMETRIS approach includes ensuring compliance with ISO/SAE 21434, UN R155, GB 44495 & Co. from the outset, with a focus on consistency in risk analysis: Are all assets included in the TARA? Are risks assigned to all architectural components? Are cybersecurity goals and claims consistent? Seamless traceability and early detection of inconsistencies accelerate your TARA work while reducing errors.

Threat analysis at the architecture level within the TARA

How can a meaningful link be established between the architecture and the execution of the TARA risk analysis? There is often a gap between these two domains, which are usually separate from each other, and traditional tool approaches, such as Excel, cannot close this gap satisfactorily. It is not possible to ensure that cybersecurity risks and architecture (data, connections, interfaces) are consistently and holistically assigned and traceable. CYMETRIS links the threat analysis with the mapped architecture. This results in a comprehensible mapping that directly assigns threats to the central components and elements of the architecture, for each component over the entire lifecycle. This enables end-to-end traceability, promotes cross-team collaboration and, at the same time, meets the industry standard for mapping risks to architecture components.



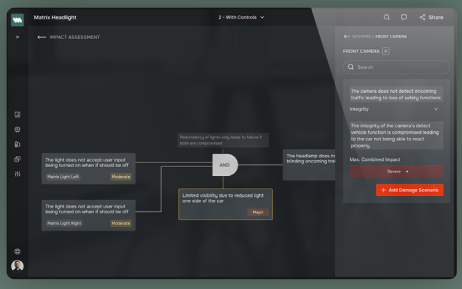


First-class visual representation of attack paths and changes in security mechanisms

You will no longer want to replace the visual representation of attack paths and dynamic threat modelling with repetitive Excel cells. CYMETRIS Attack Path Visualisation not only gives you an overview of all potential attack steps and combinations that could lead to the compromise of a component. You can also update threat scenarios yourself, for example by simulating the failure of a security mechanism. With helpful functions, you can navigate even the most complex attack paths without losing sight of the big picture.

TARA made easy: information exchange and collaboration between OEMs and suppliers

With the help of the granularly configurable options for information exchange and collaboration in the implementation of TARA, the CYMETRIS solution offers practical options for integration, collaboration and structured risk assessment on both the OEM and supplier side. This means that OEMs can integrate the TARA elaborations of their suppliers into their own risk analyses, while suppliers can perform their risk assessments only at the actual level, without having to make hundreds of assumptions about influencing factors. In this way, tool-supported collaboration becomes a success factor for effective risk analyses, without violating the requirements for the sharing of safety-critical information.



BOOK A DEMO

CYEQT

KNOWLEDGE BASE