PROOF maturity model
Measure and improve your cyber-security management system

July 2024

Empowering Tomorrow's Automotive Software
www.etas.com

ETAS

Executive summary

ESCRYPT PROOF is a maturity model that covers automotive product cybersecurity-related organizational aspects such as strategies, processes, and cybersecurity risk management.

The maturity model enables automotive organizations regarding three major criteria:

- Completeness due to the coverage of cybersecurity-related activities across all related disciplines, as well as the whole product lifecycle
- Compliance towards national and international automotive cybersecurity frameworks
- Measurement of cyber maturity beyond compliance towards an efficient and continuously improved implementation

The model lays out the requirements for an organizations cybersecurity or software update management system. The model covers several national and international automotive cybersecurity frameworks, such as norms and standards. This unique approach enables organizations to measure their cyber maturity, implement cybersecurity management systems and continuously improve their product security related processes. In addition, it provides evidence of compliance towards the most important cybersecurity frameworks in the automotive industry.

Major benefits of the introduction of such a maturity model are the reduction of double efforts when applying several frameworks, the increased transparency through the quantification of automotive cyber maturity and the risk reduction due to an improved cybersecurity culture.

The paper describes the motivation and need for such a maturity model in the automotive industry, outlines the methodology of the framework in detail, and shows uses cases and possible adaptions.

Table of contents

1. Challenges in the automotive industry

The automotive industry has witnessed a rapid transformation in recent years, with the integration of advanced technologies and connectivity features in vehicles. The latest trends include autonomous driving or artificial intelligence, which require the vehicle to be highly connected with its environment, including cloud services, infrastructure, and other vehicles.

Despite the numerous advantages new functionalities bring, they also introduce new challenges, such as those related to cybersecurity risks. Cybersecurity vulnerabilities have led to several recalls (NHTSA, 2015) (NHTSA, 2022). But even long-established technologies, like CAN communication, can still be exploited (Corfield, 2023). As a result, numerous automotive-specific regulations were introduced that mandate the implementation of security measures (UNECE, 2021). Hardly surprising, then, that the top five business risks in the automotive manufacturing sector include cybersecurity incidents (Allianz, 2024). Cybersecurity has become a major business factor for modern vehicle manufacturers.

The increasing risks are based on several factors, for example:

- new technology and increasing amount of interfaces
- shorter development cycles which results in increasing time pressure on development teams
- changing types of attackers from automotive experts with physical access to vehicles to IT security experts focusing on remote attacks
- supply chain risks due to multiple, diverse suppliers including open-source-software
- a diverse regulatory landscape with national and international frameworks focusing on different aspects of automotive cybersecurity

The following chapters of this whitepaper will explain how a cyber maturity model is beneficial for organizations in tackling these challenges, and a solution on how to measure and improve an organization's cyber maturity will be provided. Chapter 2 of this whitepaper explains the benefits of a maturity model. In chapter 3 the PROOF maturity framework is illustrated. Chapter 4 describes how PROOF covers common development models. The adaptability of the framework is explained in chapter 7 and the tool-based implementation of the framework in chapter 8. Use cases of the framework are covered in chapter 9. As there is a need for continuous improvement in security, chapter 10 deals with this challenge. The whitepaper results in further development areas in chapter 11. The entire PROOF maturity model as well as a mapping of the maturity levels can be seen in the Annex.

2. The need for an automotive cyber maturity framework

As the automotive industry is facing complex challenges related to cybersecurity, there is a growing recognition of the need for a comprehensive framework to enhance cyber maturity. Such a maturity model should incorporate several features and attributes to address those challenges.

Multiple frameworks

Because of the diverse regulatory landscape, it is valuable to have a framework, that provides a unified approach and aligns various regulations. To avoid additional efforts when introducing multiple frameworks, for example because of different customer demands, a comparison and alignment of different regulations is needed. A maturity framework should include international frameworks such as ISO/SAE 21434, UN R 155 and UN R 156, but also regional frameworks, such as JasPar TD-CSP-12 to ensure products meet the requirements of all target markets. Combining frameworks that cover different disciplines like governance, development or production ensures that cybersecurity is sufficiently covered across all related disciplines and along the complete product lifecycle.

Measurability of process maturity

Assessing cyber maturity requires more than just a qualitative evaluation or a statement regarding compliance with a specific standard. It requires a comprehensive understanding of an organization's processes and a quantitative evaluation of their implementation. Process maturity should be assessed based on mean values that identify gaps, set improvement targets and track improvement progress over time. This ability to qualitatively and quantitatively measure cyber maturity enables a company to take a proactive approach towards cybersecurity risks and continuously enhance its capabilities.

Completeness

Cybersecurity in the automotive industry extends beyond the development phase of individual vehicles and components. It includes the entire product lifecycle: from design and, manufacturing, to deployment, and end-of-life. It also includes supplier and customer relationships as well as interactions with authorities. A corresponding maturity model should consider the entire product lifecycle and its supply chain to ensure a holistic view. Such a model enables companies to establish end-to-end security and effectively manage cybersecurity risks throughout the entire ecosystem.

From stakeholder confidence to competitive advantage

How does an organization know that a product is secure enough? Since there will never be a 100% secure system, organizations need to find the right balance between implementing the appropriate security features to cover all known vulnerabilities and keeping efforts and costs to a minimum. A maturity model helps an organization find the individual target maturity of processes and products. Once mature processes have been defined for developing and maintaining secure products, and once these processes have resulted in products, there is evidence and confidence that a product has reached its desired cyber maturity level. If this maturity is further improved to enable cost reductions, e.g., through tool-based or automated solutions, cybersecurity can even become a competitive advantage. Recent research indicates that there is a correlation between higher process maturity in decreasing budget needs. (Minzlaff, 2023)

Continuous improvement

As threats and risks evolve, it is necessary to continuously adapt cybersecurity practices. Companies need to improve their processes and stay up-to-date on cybersecurity measures. A maturity model should emphasize the importance of continuous improvement. Efficient implementation of processes beyond mere compliance ensures cost-saving measures. A maturity model should emphasize the importance of continuous improvement. Efficient implementation of processes beyond mere compliance ensures cost-saving measures. The model should provide guidance on how to stay up-to-date regarding the latest cybersecurity threats and countermeasures. This ensures that companies can effectively respond to new challenges and maintain a high level of cyber maturity. The need for continuous improvement applies to the underlying maturity model as well.

The following chapter will introduce the PROOF maturity model in detail and will explain how it can help tackle the outlined challenges.

3. PROOF maturity model – methodology

The **Pro**duct **O**rganization **F**ramework (PROOF) is a maturity model that focuses on the process maturity of automotive organizations with regard to cybersecurity. While many existing models focus on enterprise IT security aspects, PROOF focuses on processes related to product security. The model consists of three main elements: domains and subdomains, controls, and maturity level, which are explained in this chapter.

3.1. Domains and subdomains

The framework is structured into **domains and subdomains**. These aim to define a comprehensive structure and to allow for a differentiation of maturity on different levels. On the management level, results can be summarized based on domains; on the department level, results can be visualized based on subdomains. This structure ensures that all relevant areas are covered, especially all related disciplines, units, partners, and stakeholders of the organization. In addition, it helps to reflect the complete vehicle lifecycle.

The **Governance** domain includes all activities related to an organization's central management and ownership of product cybersecurity. All policies and processes are managed in this domain, and it defines the overall cybersecurity strategy.

The **Risk Management** domain contains all activities related to identifying, analyzing, and managing risks and (potential) vulnerabilities. Activities included in this domain are cybersecurity monitoring, threat and risk analysis (TARA), as well as vulnerability analysis and management.

The **Ecosystem** domain comprises the organizational relationships with internal and external stakeholders, such as suppliers or authorities.

The **Concept & Development** domain summarizes all activities related to an organization's product development phase. The activities include project planning, deriving security specifications from the security concept, secure implementation, and all security-related verification and validation activities.

The **Production & Operations** domain includes all activities during the production of the vehicle or components as well as their maintenance until end-of-life. This maintenance includes incident response and software update activities.

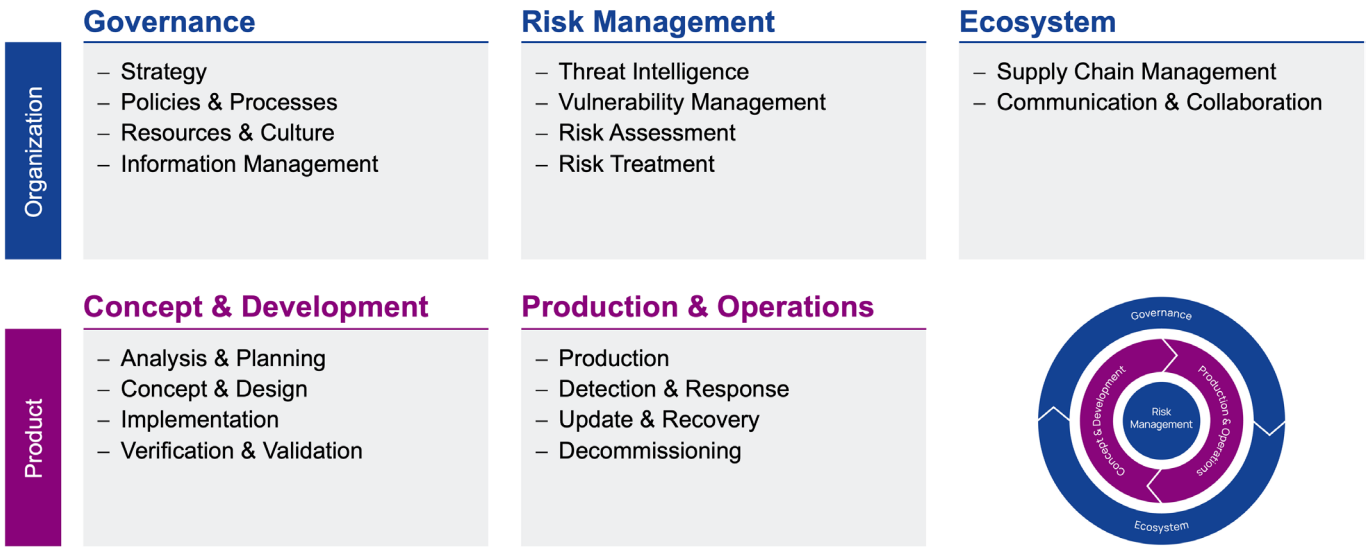

Figure 1: PROOF domains & subdomains

3.2. Controls

The lowest level of the structure and the main element of the maturity model are **controls**. Each control is developed based on various automotive cybersecurity frameworks, such as ISO/SAE 21434 or UN R 155.

Within each subdomain, controls describe the necessary activities that need to be carried out to ensure secure development and handling of automotive products. Controls include a title, a control text (purpose), key activities (performance indicators) and a linking to the specific requirements of the related framework. An example of a control can be seen in Table 1. All PROOF controls can be seen in Annex A: PROOF maturity model v2.6.

Field	Example
Domain / subdomain	Governance / Policies & Processes
ID: Control title	GOV B10: Cybersecurity policy, rules and processes
Control text	The organization shall develop an adequate cybersecurity policy and adherent rules and processes that reflect the necessity and importance of managing corresponding risks.
Key activities	A dedicated cybersecurity policy has been created. **AND** A set of cybersecurity rules and processes tailored to the organization's structure has been created and implemented. **AND** The rules and processes in place enable the implementation of all necessary cybersecurity activities.
Referenced frameworks	– ISO/SAE 21434:2021: [RQ-05-01], [RQ-05-02] – UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (a), 7.2.2.2 © – ISO/PAS 5112: Q1.1 – VDA ACSMS Red Volume (1st. Ed.): Q1.1, Q1.3, Q3.2 – KBA Prüfkatalog: A.2, A.5, A.6, B.2, B.3 – CN IVC Access Guide: Article 02, 03, 09 – NHTSA Best Practices 2022: [G.1] – PSIRT Services Framework 1.1: III.A.

Table 1: Overview and example of a PROOF control

3.3. Maturity level

Every control can be rated at one of five maturity levels. The **maturity levels** have been defined in alignment with other well-known maturity level definitions (see Annex B: Mapping of maturity level). This approach ensures compatibility with those descriptions in case they are already in use within an organization.

The lowest level, **Level 1: Initial**, describes the state where the key activities of a control are not performed or with large deviations. This leads to not achieving the objective of that specific control.

Level 2: Performed describes the phase where activities are performed, for example as part of a project, but not based on a well-defined process, or the described activities are performed with minor deviations even if a process description exists.

Level 3: Established describes the state where the necessary processes are fully described, and the projects in scope and other related disciplines fully follow these processes and fully perform the key activities described.

Level 3 enables an organization to ensure that products are securely developed and maintained throughout the whole lifecycle and that compliance with frameworks is achieved.

Starting with **Level 4: Advanced**, the focus is increased to not only cover mere documentation of processes and their performance, but to increase efficiency with tool-based solutions that allow for measurement of the status and the results of individual activities and processes.

The highest level, **Level 5: Optimizing**, describes the continuous effort to analyze process performance and to improve the processes based on those results in a systematic way.

In addition to the quantitative rating, each control is rated qualitatively by describing the exact state of implementation, best practices, and identified gaps.

3.4. Mapped frameworks

The PROOF maturity model 2.6 is based on three regulations, four standards and five guidelines.

The frameworks are:

- UN Regulation No. 155, describing the requirements for a type "approval of vehicles with regards to cyber security and cyber security management systems" (UNECE, 2021)
- UN Regulation No. 156, describing the requirements of a type "approval of vehicles with regards to software update and software updates management system" (UNECE, 2021)
- MIIT management guide for ICV manufacturer and product access
- ISO/SAE 21434:2021 Road vehicles - Cybersecurity engineering
- ISO/PAS 5112:2022 Road vehicles - Guidelines for auditing cybersecurity engineering
- ISO 24089:2023 Road vehicles - Software update engineering
- VDA Automotive SPICE for Cybersecurity (1st edition) 2021
- FIRST PSIRT Services Framework (v1.1) 2020
- JasPar TD-CSP-12 Automotive Cyber Security Quality Assurance Guide, (v1.10) 2019
- KBA Anforderungskatalog Auditierung von Cybersecurity/SU-Managementsystemen (Revision 1.1) 2021
- VDA Automotive Cybersecurity Management System Audit – Red Volume (1st edition) 2020
- NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles, 2022

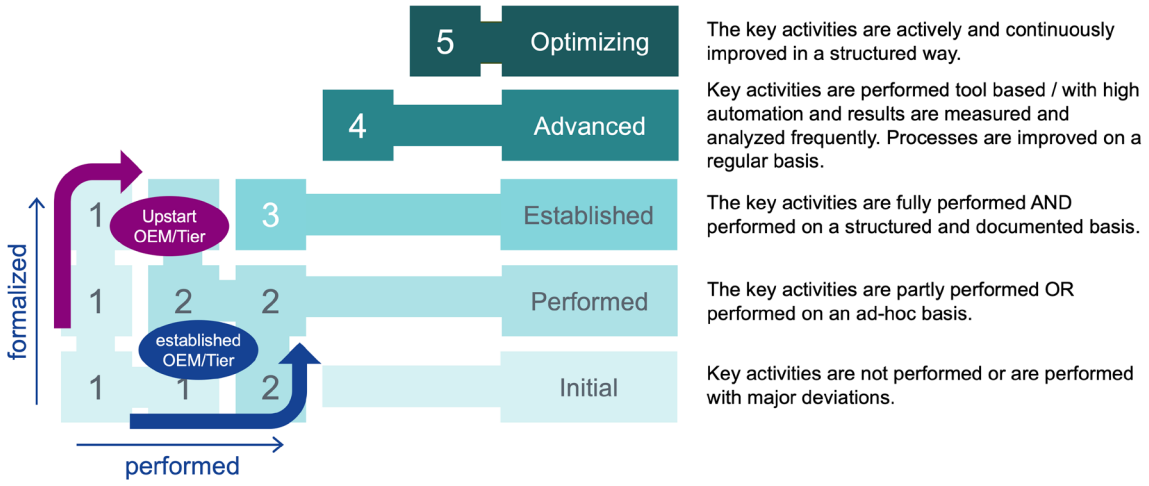

Figure 2: PROOF maturity level

4. Coverage of common development models

In the automotive industry, several development models are used by OEMs and tiers to develop, produce, and maintain their products. Two of the most common approaches are the V-Model and the DevOps cycle. While the V-Model describes the relationship of the specification and design activities to the verification and validation activities, as well as the breakdown from the vehicle level to the system and even the hardware and software levels, the DevOps cycle is well suited to describing the continuous approach to develop and improve (software) products. Both models, if enhanced with security activities like threat and risk analysis, secure implementation techniques, and security testing, or continuous activities like monitoring and vulnerability management, are well suited to enabling an organization to develop and maintain security products. There is no need to invent new process models, as the existing models can be enhanced with the necessary security activities and the maturity of those can be measured. The PROOF controls cover all necessary activities needed in both models. Figure 3 shows the mapping of PROOF (sub-) domains and controls to the DevOps cycle.

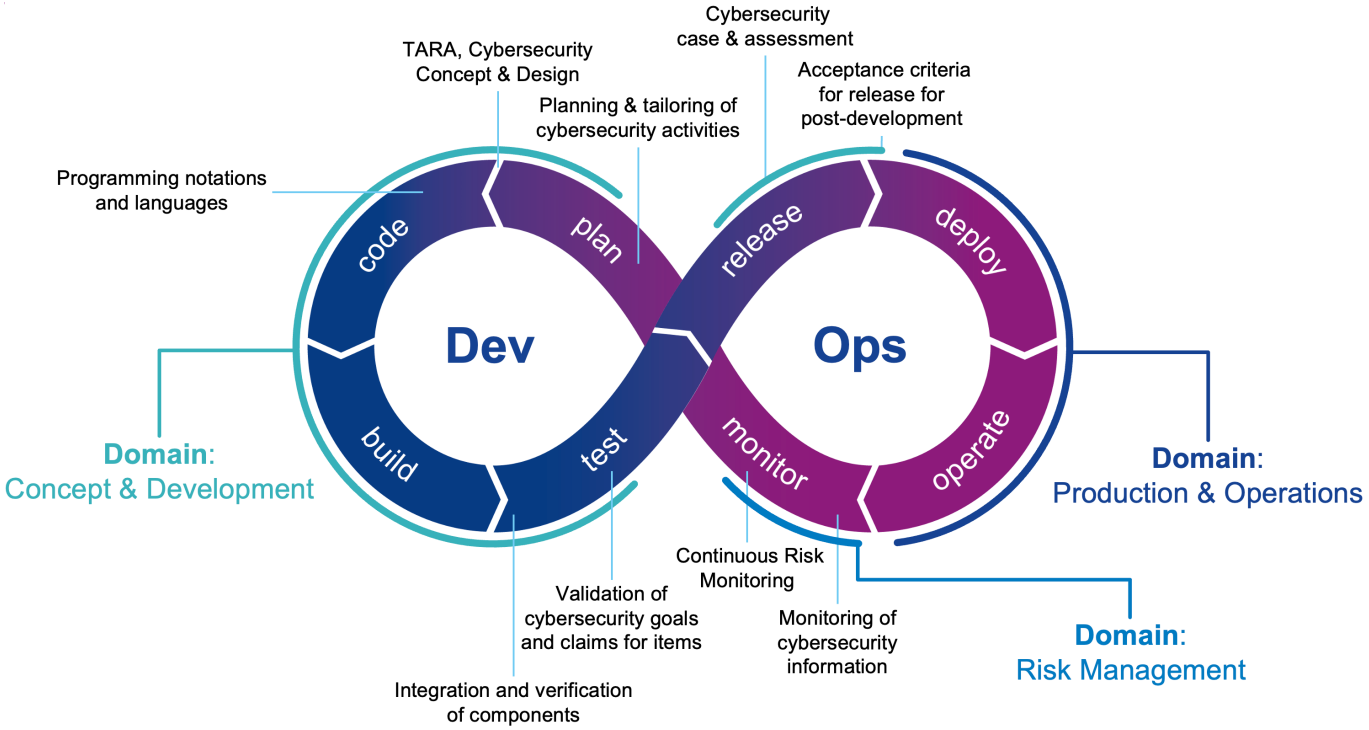

Figure 3: Mapping of PROOF controls to DevSecOps cycle

5. Comparison to other (automotive security) maturity models

While there are several regulatory frameworks describing various requirements for processes in automotive product development, such as ISO/SAE 21434:2021 or UN R 155, there is currently no maturity model that covers the entire product lifecycle including all disciplines. ASPICE for cybersecurity, which shares the ASPICE rating scheme, focuses on development activities, risk management, and the relationship to suppliers, but does not cover governance aspects or maintenance of the product over lifetime and other aspects.

While ISO/SAE 21434 covers most of the product lifecycle, some aspects are described only at a high level, such as production security, incident response, or software update management, and therefore need to be covered by other, more detailed frameworks. Also, ISO/SAE 21434 does not provide a maturity rating scheme in order to evaluate the maturity of process implementation. Other frameworks either do not cover the full scope or do not include a method for maturity evaluation.

6. Target maturity

While a five-level rating scheme might imply that the objective for each control is always to reach level five, it is much more crucial to define an organization-specific target maturity level for each control.

Each organization has its own business strategies, products, product complexity, target markets, risk aversion, and risk appetite. Therefore, the target process maturity varies for each organization as well. While some organizations might be focused on high product quality, others might focus on cost-effective solutions. Some organizations might see security as a competitive advantage, while others aim for compliance.

The reasons for different business targets can be diverse and need to be analyzed individually. Accordingly, the target maturity level needs to be set individually for each organization as well as for each control within the framework.

7. Adaptability of the framework

Every organization is different and therefore has different processes, methods, and tools as well as different people, competences, and mindsets.

To ensure a framework like the PROOF maturity model can be efficiently used within an organization, adaptions may be necessary. Because of the framework's modular structure, several modifications can easily be implemented. This chapter describes a few of the possible adaptions that can be made to incorporate the model into an organization's structure.

Restructuring the controls to organization specific domains and subdomains

Assuming an organization is structured in a specific way, for example responsibilities for specific topics are divided across various departments, some controls or even subdomains can be allocated to those departments. In such a scenario it might make sense to restructure the pre-defined domains and subdomains to align them with the target organization. For example, if the threat and risk analysis is performed by the same team that also creates the security specification, the subdomain risk assessment and concept and design could be combined in a domain that is named after that department.

Add technical controls

If it is not only the process maturity of an organization but also the technical maturity of a product that is to be evaluated, technical controls can be added. A technical control would describe a specific security feature, e.g. secure access, and the maturity level would describe different possibilities for how the feature can be implemented.

Control name: Secure diagnostic access

Control text
The product supports secure diagnsotic access.
Key activities
The product supports secure access options. **AND** The product uses cryptographic alogrithms for secure access with an appropraite key length. **AND** Measures are implemented to prevent brute force attacks. **AND** The implemented solution is resistant against glitching attacks. **AND** Routines to read or manipulate sensitive data is deactivated.

Table 2: Example for technical controls

Definition of control-specific maturity level

The PROOF maturity levels come with a generic definition of five maturity levels. These level definitions are identical for all controls. If an organization wants to describe in more detail under which conditions a level of a specific control is reached, control specific maturity levels can be described. These maturity levels would then describe the conditions that need to be fulfilled to reach a specific level for that control. Table 3 gives an example of one such control specific maturity level.

Control name	Cybersecurity policy, rules, and processes
Control text	The organization shall develop an adequate cybersecurity policy and adherent rules and processes that reflect the necessity and importance of managing corresponding risks.
Key activities	– A dedicated cybersecurity policy has been created. – A set of cybersecurity rules and processes tailored to the organization's structure has been created and implemented. – The rules and processes in place enable the implementation of all necessary cybersecurity activities..

Lv.	Generic PROOF maturity level	Control-specific maturity level (example)
1:	Key activities are not performed or are performed with major deviations.	There are no organization-specific rules or processes concerning cybersecurity.
2:	The key activities are partly performed OR performed on an ad hoc basis.	The implemented rules or processes are not complete or project work takes place without existing processes.
3:	The key activities are fully performed **AND** performed on a structured and documented basis.	All cybersecurity processes are documented and being followed in projects.

Table 3: Example of control specific maturity level

Mapping to internal directives

The PROOF maturity model is based on international or national frameworks such as norms, standards, or regulations regarding cybersecurity in the automotive industry. Some organizations might already have internal policies or directives that (partly) describe how to ensure product cybersecurity. To avoid introducing parallel processes, the PROOF maturity model can be mapped to those existing company internal rules. This way, the internal rules can be checked for completeness and the additional controls can easily be integrated. This ensures completeness and compliance of the organizational processes regarding both internal and external frameworks and policies.

8. Tool-based implementation of the model

The overarching discipline describing managerial responsibility within an organization, managing risks, and ensuring compliance with regulations is often called GRC: governance, risk, and compliance (Racz, Weippl, & Seufert, 2010). Compliance may focus on various regulations, such as those for quality, safety, or information security. In addition, each discipline usually has defined a specific method to analyze and measure risks. There are several tool and platform providers available offering commercial GRC solutions. While this white paper will not evaluate several tools nor give recommendations on single solutions, this chapter describes how a tool-based implementation of the PROOF maturity model can support the successful usage of the model.

GRC tools usually offer support for several steps during the maturity evaluation and improvement.

During the measurement phase, they provide guidance through the questions and document results, evidence, and ratings.

Once the measurement is complete, these tools usually also offer functions to visualize or report the results, for example through charts, graphs, or management summaries.

To support the implementation of controls and improvement of the processes, tools can also be used to define targets, address the requirements to specific stakeholders, and track progress during implementation. Therefore, tools should allow reevaluation of previously rated controls.

9. Use cases

This chapter describes several use cases that explain how the maturity model can be used and what type of organization it is best suited for.

Fit gap analysis

A fit gap analysis evaluates the status of existing (cybersecurity) processes and determines whether other existing processes (e.g., from functional safety, quality, or software development) can be reused. This analysis focuses on identifying existing processes or best practices. Assuming that the overall process maturity for cybersecurity processes is rather low, other disciplines such as quality management of functional safety can be included in the analysis to reuse existing processes. This approach is usually used for organizations that intend to implement a cybersecurity management system and therefore want to analyze the initial situation.

Process audits

The PROOF maturity model can also be used to perform regular process audits, for example on a yearly basis or in preparation for a certification audit. Audits focus on process maturity and are used for continuous improvement of these processes. The goal is to precisely identify missing requirements and to highlight potential improvements. This method is suited for organizations that have already established a cybersecurity management system and have reached a maturity level of at least two.

Improvement projects

Based on either a fit gap analysis or a process audit, improvement measures need to be managed. They need to be planned, tracked, and re-audited to provide evidence of implementation. PROOF supports the planning and tracking through its domain and subdomain structure. The processes and their improved implementation can be easily measured. If used continuously to measure (process audit) and improve processes, the PROOF maturity model can be integrated into a continuous improvement process (CIP) – for example, according to a plan-do-check-act (PDCA) cycle.

Supply chain evaluation

The same maturity model that is used internally to measure and improve the cybersecurity management system can be used to evaluate a supplier's cyber maturity and to proactively steer the improvement programs on the supplier side. Supplier handling is a challenging task due to the diversity of organizations. A unified framework allows fast and efficient measurement of the supplier's processes, continuous monitoring and improvement, as well as easy comparison between different suppliers. Combined with a supplier-specific target maturity, it allows fair treatment of each supplier considering the supplier specific context, product and technology.

10. Need for continuous improvement of maturity models

As described in chapter 4 and 9, there is a need to continuously improve product and process maturity to keep pace with to changing technical and regulatory requirements. This, of course, applies to any process, including maturity models and therefore also to the PROOF maturity model itself.

To illustrate why the maturity model needs to be continuously updated and improved, the following non-exhaustive list describes a few examples.

Technological advancements and evolving threat landscape

As described in chapter 1, the rapid technological and functional development in the automotive industry opens up new attack paths and a larger number of vulnerabilities. To tackle these changes, every organization needs to stay up-to-date on the latest best practices and measures to tackle these threats. Therefore, the maturity model used needs to evolve as well. Lessons learned, industry best practices, and general process improvements are to be considered to update the framework.

New or changing international and national frameworks

In the coming years, many new regulations will be published that try to define specific aspects of automotive cybersecurity. To identify additional requirements and to distinguish among those already in place, the PROOF maturity model will be continuously updated with the most relevant automotive security frameworks.

Some frameworks may be updated and improved themselves, and so the PROOF maturity model will also be updated to account for the latest requirements. For example, a second edition of the ISO/SAE 21434 is planned to be published sometime in the next few years. Added or changed requirements will also be updated in PROOF.

Other frameworks may adapt the scope that they apply to. For example, UN R 155 was once applicable only to vehicle types M, N, and O, and later updated to include vehicle type L (UNECE U. N.-I., 2024). Organizations that have used other guidelines or standards now need to consider new requirements or perform a type approval.

11. Summary

As the automotive attack surface and the threat landscape keep changing, organizations need to establish higher cyber maturity. ESCRYPT PROOF enables organizations to measure, define and improve their cybersecurity management systems while establishing a strong cybersecurity culture. New frameworks will be released to cover various aspects of automotive cybersecurity. PROOF ensures that organizations stay up to date with the latest requirements, achieve compliance, and implement the latest industry best practices. At the same time PROOF reduces efforts when implementing new requirements and provides guidance to consider product cybersecurity across all disciplines and throughout the entire product lifecycle.

About ETAS

Founded in 1994, ETAS GmbH is a wholly owned subsidiary of Robert Bosch GmbH with a local presence in all major automotive markets in Europe, North and South America, and Asia.

ETAS offers comprehensive solutions for the realization of software-defined vehicles in the areas of software development solutions, vehicle operating system, vehicle cloud services, data acquisition and processing solutions, integrated customer solutions and cybersecurity.

As industry pioneers in cybersecurity, we assist our customers in managing cybersecurity-related complexities, reducing cyber risks, and maximizing their business potentials with a proven on- and offboard portfolio of software products and professional security services.

ETAS automotive security solutions are safeguarding millions of vehicle systems around the world – and are setting standards for the cybersecurity of software-defined vehicles.

Annex A: PROOF maturity model v2.6

Overview domains & subdomain

	Governance	Risk Management	Ecosystem
Organization	– Strategy – Policies & Processes – Resources & Culture – Information Management	– Threat Intelligence – Vulnerability Management – Risk Assessment – Risk Treatment	– Supply Chain Management – Communication & Collaboration

	Concept & Development	Production & Operations
Product	– Analysis & Planning – Concept & Design – Implementation – Verification & Validation	– Production – Detection & Response – Update & Recovery – Decommissioning

Structure of domains

The PROOF 2.6 controls are listed below. The controls are shown in the following structure:

Domain (Domain abbreviation)

Domain order: Subdomain

Control ID: Control name

Control text
Key activities
Referenced frameworks

Governance (GOV)

A: Strategy

GOV A10: Definition of the scope of the CSMS

The organization shall define the scope of the CSMS.

The scope of the CSMS is defined (including processes, products, locations, ecosystem).

AND

Exceptions applied to the definition of the scope are justified and a rationale is provided.

– KBA Prüfkatalog: B.1

GOV A20: Management commitment

The executive management supports the cybersecurity activities.

Executive management has defined a strategy for managing road vehicle cybersecurity risks for all phases of the vehicles life cycle.

AND

The results are reflected in a cybersecurity policy including the acknowledgement of road vehicle cybersecurity risks and the executive management's commitment to manage these cybersecurity risks.

AND

The funding and commitment of related stakeholder are provided to enable all related cybersecurity activities.

– ISO/SAE 21434:2021: [RQ-05-01]
– UN R155: 7.2.2.1, 7.2.2.2 (a), 7.2.2.2 ©
– ISO/PAS 5112: Q1.1
– VDA ACSMS Red Volume (1st Ed.): Q1.1, Q1.3
– KBA Prüfkatalog: A.1, A.2, B.3
– NHTSA Best Practices 2022: [G.2]
– PSIRT Services Framework 1.1: I.A., I.E.

GOV A40: PSIRT charter

The PSIRT shall develop a charter or other documents (e.g., strategic plan, implementation plan, or concept of operations document) in which mission and constitution of the PSIRT are documented.

There is a public website with a responsible disclosure policy and clear information on how to report vulnerabilities.

AND

Vulnerability finders are publicly acknowledged and they can build up their reputation via these acknowledgements to construct an expertise portfolio.

AND

Bug bounty programs may be established. (optional)

– PSIRT Services Framework 1.1: I.C.

GOV A50: Acknowledgement to vulnerability finders

Vulnerability finders shall be acknowledged for their effort to disclose product vulnerabilities and there should be a clear and publicly accessible disclosure policy.

There is a public website with a responsible disclosure policy and clear information on how to report vulnerabilities.

AND

Vulnerability finders are publicly acknowledged and they can build up their reputation via these acknowledgements to construct an expertise portfolio.

AND

Bug bounty programs may be established. (optional)

– PSIRT Services Framework 1.1: 1.2.1, 1.5.4, 1.6.1, 1.6.2, 5.2.1

GOV B10: Cybersecurity policy, rules and processes

The organization shall develop an adequate cybersecurity policy and adherent rules and processes that reflect the necessity and importance of managing corresponding risks.

A dedicated cybersecurity policy has been created.
AND
A set of cybersecurity rules and processes tailored to the organization's structure has been created and implemented.
AND
The rules and processes in place enable the implementation of all necessary cybersecurity activities.

- ISO/SAE 21434:2021: [RQ-05-01], [RQ-05-02]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (a), 7.2.2.2 ©
- ISO/PAS 5112: Q1.1
- VDA ACSMS Red Volume (1st. Ed.): Q1.1, Q1.3, Q3.2
- KBA Prüfkatalog: A.2, A.5, A.6, B.2, B.3
- CN IVC Access Guide: Article 02, 03, 09
- NHTSA Best Practices 2022: [G.1]
- PSIRT Services Framework 1.1: III.A.

GOV B12: Business continuity for critical processes

The organization shall identify critical processes of the CSMS and apply business continuity management for these processes.

Critical processes of the CSMS relevant for product development, the production phase and the post-production phase are identified.
AND
Business continuity management (including crisis management with escalation and recovery plans) is implemented and applied for these processes.

- KBA Prüfkatalog: A.15, A.16, B.16, B.17, B.18

GOV B14: Identify, Protect, Detect, Respond and Recover

The organization's cyber security framework shall be structured around the five principle functions: "Identify, Protect, Detect, Respond and Recover"

Critical processes of the CSMS relevant for product development, the production phase and the post-production phase are identified.
AND
Business continuity management (including crisis management with escalation and recovery plans) is implemented and applied for these processes.

- NHTSA Best Practices 2022: [G.1]

GOV B16: Software update engineering rules and processes

The organization shall develop adequate software update engineering rules and processes tailored to software update activities, that reflect the compliance of relevant requirements and assign resources and responsibilities.

The organization created and implemented a set of software update engineering rules and processes, tailored to the corresponding activities and responsibilities across all those involved in software update engineering.
AND
Any software update engineering activities are performed in accordance with these rules and processes.

- ISO 24089:2023: 4.3.1.1, 4.3.1.2
- UN R156: 7.1.1.1
- KBA Prüfkatalog: A.2, B.1, B.2

GOV B17: Compliance relevant for software update engineering

The organization shall be compliant with requirements of relevant standards, guidelines and regulations and shall sustain quality control in the software development process.

The organization's software update engineering activities are compliant with applicable content of ISO/SAE 21434, ISO 26262-6 and ISO 26262-8.

- ISO 24089:2023: 4.3.1.3, 4.3.4.5
- CN ICV Access Guide: Annex1_3.9

GOV B20: Cybersecurity roles

The organization shall assign all relevant cybersecurity responsibilities and the corresponding authority.

Roles regarding cybersecurity are defined and assigned in order to carry out the relevant tasks.

AND

The authority and responsibilities regarding cybersecurity are assigned and adequately communicated.

- ISO/SAE 21434:2021: [RQ-05-03]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 © , 7.2.2.2 (a)
- ISO/PAS 5112: Q1.2
- VDA ACSMS Red Volume (1st. Ed.): Q1.2
- KBA Prüfkatalog: A.1, A.3, B.3
- CN IVC Access Guide: Annex1_2.1
- NHTSA Best Practices 2022: [G.2]
- PSIRT Services Framework 1.1: I.B., I.D.

GOV B40: Implementation of management systems supporting the organization's processes

The organization shall design and implement appropriate management systems that support the organization's processes.

There are all necessary management systems (i.e., quality management, information security, change management, documentation management, configuration management and requirements management, if needed) in place which are needed to support the organization's processes (e.g., for cybersecurity and/or software update engineering).

- ISO/SAE 21434:2021: [RQ-05-11], [RC-05-13], [RC-05-16]
- ISO 24089:2023: 4.3.2.2, 4.3.4.1, 4.3.4.2, 4.3.4.3, 4.3.4.4, 4.3.4.5, 4.3.4.6
- UN R156: 7.1.1.1
- ISO/PAS 5112: Q1.2
- KBA Prüfkatalog: A.13
- NHTSA Best Practices 2022: [G.1], [G.20], [G.36], [G.37]

GOV B50: Audits of processes

The relevant organization's processes shall regularly and independently be audited.

Audits (e.g., cybersecurity or software update engineering) are performed to independently judge whether the organizational processes comply to the objectives agreed.

AND

he outcome of audits is monitored and any identified deficiencies are tracked until fixed.

- ISO/SAE 21434:2021: [RQ-05-08]
- ISO 24089:2023: 4.3.5.1
- ISO/PAS 5112: Q1.2
- KBA Prüfkatalog: A.7, A.12, B.3, B.29, B.31, B.32, B.36
- CN ICV Access Guide: Annex1_2.10
- NHTSA Best Practices 2022: [G.38], [G.39]

GOV B80: Real-name registration in China

The organization shall establish a real-name registration system for the internet of vehicles (IoV) cards.

A real-name registration system for the internet of vehicles (IoV) cards is established.

AND

When selling a car in China, the purchaser's identity information is recorded by the OEM.

AND

Real-name registration requirements for IoV cards are implemented by the OEM together with telecommunication companies.

- CN ICV Access Guide: Annex1_2.8

GOV C20: Allocation of adequate resources

The organization shall provide adequate resources in order to accomplish all necessary tasks related to the relevant management system.

Adequate resources are provided in order to fulfil all tasks related to the relevant management system.

- ISO/SAE 21434:2021: [RQ-05-04]
- ISO 24089:2023: 4.3.1.2
- ISO/PAS 5112: Q1.2
- VDA ACSMS Red Volume (1st. Ed.): Q1.2
- KBA Prüfkatalog: A.10, B.3
- NHTSA Best Practices 2022: [G.2]
- PSIRT Services Framework 1.1: II.A., II.B., II.C.

GOV C40: Cybersecurity culture

The organization shall foster and maintain a strong cybersecurity culture.

The organization fosters and maintains a resilient and sustainable cybersecurity culture that creates awareness and ensures sufficient competences.

- ISO/SAE 21434:2021: [RQ-05-06], [RQ-05-07]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (a)
- ISO/PAS 5112: Q1.3
- VDA ACSMS Red Volume (1st. Ed.): Q1.3, Q1.4
- KBA Prüfkatalog: A.9, A.11, A.12, A.13, B.3
- CN ICV Access Guide: Annex1_2.12
- PSIRT Services Framework 1.1: III. B., 6.2.1, 6.3.1, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7

GOV C50: Continuous improvement process

The organization shall establish and maintain a continuous improvement process.

The organization maintains an established process which includes appropriate and proactive measures for continuous improvement.

- ISO/SAE 21434:2021: [RQ-05-08]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (a)
- ISO 24089:2023: 4.3.2.1, 4.3.2.2
- ISO/PAS 5112: Q1.3
- VDA ACSMS Red Volume (1st. Ed.): Q1.3
- KBA Prüfkatalog: A.9, A.11, A.12, A.13, B.3
- CN ICV Access Guide: Annex1_2.12
- PSIRT Services Framework 1.1: III.B., 1.1.3, 3.1.2, 6.5

GOV C60: PSIRT Training

The PSIRT Staff shall be trained sufficiently.

PSIRT members receive regular training including:
- technical training
- communications training
- process training
- tools training including security testing

AND

All training initiatives are tracked, including the ones for stakeholders.

- NHTSA Best Practices 2022: [G.34]
- PSIRT Services Framework 1.1: 2.4.2, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5

GOV C80: Cybersecurity assurance team

The organization shall foster a full-time cybersecurity assurance team for securing products throughout the lifecycle.

As part of overall security assurance, the organization fosters a full-time cybersecurity assurance team responsible for securing products throughout the lifecycle.

AND

The organization's security assurance requirements encompass cybersecurity requirements and software update management requirements next to functional safety and SOTIF requirements.

- CN ICV Access Guide: Annex1

GOV C90: Collaboration in education and workforce development

Vehicle manufacturers, suppliers, universities, and other stakeholders shall work together to help support educational efforts targeted at workforce development in the field of automotive cybersecurity.

The organization works with other vehicle manufacturers, suppliers, universities, and other stakeholders to help support educational efforts targeted at workforce development in the field of automotive cybersecurity.

- NHTSA Best Practices 2022: [G.40]

GOV D10: Communication and collaboration across organizational units

Communication and collaboration across all organizational units related to cybersecurity shall be coordinated.

The organizational units related to or interacting with cybersecurity are identified.

AND

Communication channels between those functions exist to integrate processes and tools and to exchange information.

- ISO/SAE 21434:2021: [RQ-05-05]
- ISO/PAS 5112: Q1.2
- VDA Automotive SPICE Cybersecurity: 13-04
- KBA Prüfkatalog: A.2, A.6, A.9, B.2, B.3
- NHTSA Best Practices 2022: [G.2]
- PSIRT Services Framework 1.1: I. B., 1.1.1, 1.1.2, 1.1.3

GOV D20: Managing and sharing of information

The organization shall define criteria regarding classification and sharing of information.

The organization has defined the circumstances under which sharing of information is required, permitted, or prohibited internal or external to the organization (concerning classification, relevant laws and the obligation to share information).

AND

The organization aligned its information security management of the shared data with other parties.

- ISO/SAE 21434:2021: [RQ-05-09], [RC-05-10]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.4 (b)
- ISO 24089:2023: 4.3.3.1
- ISO/PAS 5112: Q1.2
- KBA Prüfkatalog: A.9, A.17, B.28
- JasPar TD-CSP-12 (V1.10): 11 (3.2.1), 34 (3.3.4.1)
- PSIRT Services Framework 1.1: 1.4.1, 1.5.1, 1.5.2, 1.5.3, 1.5.4, 4.2.3, 4.3.3, 5.1.1, 5.1.2, 5.2.1, 5.2.2, 5.3.1, 5.3.2, 5.3.3, 5.3.4

GOV D30: Tool management

The organization shall design and implement a tool management process that protects the organization's cybersecurity related systems and applications from intentional or unaware malicious tool use.

All tools that can impact the cybersecurity of an item, of a system or of a component are managed adequately.

- ISO/SAE 21434:2021: [RQ-05-14], [RC-05-15]
- UN R156: 7.1.1.1
- ISO/PAS 5112: Q1.2
- KBA Prüfkatalog: A.8

GOV D40: Information security during development, production and post-production

The organization shall design and implement an information security management system for the infrastructure relevant for the product lifecycle.

The organization has defined an information security management system according to recognized standards (e.g., ISO27001 or TISAX) for the infrastructure relevant for product development, production and post-production.

AND

The information security management system ensures adequate risk management and processes for information security, including the interfaces between different locations and organizational units.

- ISO/SAE 21434:2021: [RC-05-16]
- KBA Prüfkatalog: A.14, B.9, B.16, B.17, B.18
- CN ICV Access Guide: Annex1_2.7

GOV D50: Information related to software updates for type approved systems

Relevant information for type approved systems before and after software updates shall be documented.

Initial and updated software versions/configurations of each type approved system are uniquely identified and documented (including software versions, integrity validation data, relevant hardware components).

AND

If applicable, for each software update and for each vehicle type, information related to type approval is documented (including effects on type approval requirements/ parameters and application for approval of the update by an approval body).

- UN R156: 7.1.1.2, 7.1.2.2
- KBA Prüfkatalog: B.20
- CN ICV Access Guide: Annex1_3.6, Annex1_3.7

GOV D60: Information related to software updates

Relevant information before and after software updates shall be collected, stored and secured.

For each software update and for each vehicle type, information (incl. the purpose of the update, affected systems/functions and conditions/execution of the update, configurations, versions, integrity validation data, relevant hardware components) is collected, stored and secured.

- ISO 24089:2023: 7.3.2.1, 7.3.2.2, 9.3.3.1
- UN R156: 7.1.1.1, 7.1.2.5, 7.1.3.2.
- KBA Prüfkatalog: B.21, B.22
- CN ICV Access Guide: Annex1_3.6, Annex1_3.7
- NHTSA Best Practices 2022: [G.10], [G.11]

GOV D70: Information related to the RXSWIN of vehicle types

If applicable, relevant information related to the RXSWIN of a vehicle type shall be documented.

If applicable, for each vehicle type the RXSWIN and the related documentation (including software versions, integrity validation data and relevant hardware components) can be accessed and updated in an auditable register.

AND

If applicable, for each component of a type approved system, the software versions are consistent with the relevant RXSWIN.

- UN R156: 7.1.1.3, 7.1.1.4, 7.1.2.3
- KBA Prüfkatalog: B.21, B.22, B.23

GOV D80: PSIRT Metrics

All necessary processes and mechanisms to collect and report on metrics from the PSIRT and its relevant stakeholders shall be implemented.

PSIRT metrics definition are provided (including stakeholder metrics, vulnerability discovery metrics, vulnerability release metrics and vulnerability disclosure metrics).

AND

Data is stored in a PSIRT metrics repository.

AND

Tools and processes are used to obtain PSIRT metrics.

AND

Reports are published on a regular basis internally within the PSIRT as well as with internal stakeholders.

- NHTSA Best Practices 2022: [G.29]
- PSIRT Services Framework 1.1: III. B., 1.7.1, 1.7.2, 1.7.3, 1.7.4, 2.5.1, 2.5.2, 4.4.1, 4.4.2, 5.4.1

Risk Management (RSK)

A: Threat Intelligence

RSK A10: Monitoring of cybersecurity information

All relevant sources shall be monitored to provide a comprehensive list of relevant cybersecurity information on product level.

Internal sources (e.g. TARA, cybersecurity claims, product specifications, past vulnerability analyses and information received from the field like vulnerability scanning reports, repair information and consumer usage information) are monitored.

AND

External sources (e.g. researchers, commercial or non-commercial sources, organization's supply chain, customers of the organization and/or government sources, market surveillance information of OEMs, sources recommended by JasPar) are monitored.

AND

The development area of each target product (including software) is monitored.

- ISO/SAE 21434:2021: [RQ-08-01]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (g), 7.2.2.4 (a)
- ISO/PAS 5112: Q2.1
- VDA ACSMS Red Volume (1st Ed.): Q7.1
- VDA Automotive SPICE Cybersecurity: 14-08
- KBA Prüfkatalog: B.10, B.11, B.17, B.35
- CN ICV Access Guide: Annex1_2.4
- NHTSA Best Practices 2022: [G.12], [G.18]
- JasPar TD-CSP-12 (V1.10): 23 (3.2.2.1), 33 (3.3.4.1), 35 (3.3.4.2)
- PSIRT Services Framework 1.1: 2.1.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5, 2.4.1

RSK A20: Triage of cybersecurity information

Cybersecurity events are determined from cybersecurity information collected on product level.

The organization ensures that cybersecurity information on product level is collected and treated accordingly.

AND

There are defined triage triggers to divide cybersecurity information into adequate categories.

AND

Cybersecurity information is triaged to determine if it becomes one or more cybersecurity events.

- ISO/SAE 21434:2021: [RQ-08-02], [RQ-08-03]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (g), 7.2.2.4 (a), 7.2.2.4 (b), 7.4.1
- ISO/PAS 5112: Q2.1
- VDA ACSMS Red Volume (1st Ed.): Q7.2
- KBA Prüfkatalog: A.14, B.10
- CN ICV Access Guide: Annex1_2.4
- NHTSA Best Practices 2022: [G.16]
- PSIRT Services Framework 1.1: 3.1.1

RSK A30: Identification of cybersecurity events

All identified cybersecurity events on product level shall be analyzed adequately in order to determine if any of the organization's products are affected.

The organization follows a comprehensive analysis approach for all cybersecurity events to identify weaknesses in products.

- ISO/SAE 21434:2021: [RQ-08-04]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (g), 7.2.2.2 (h), 7.2.2.4 (b)
- ISO/PAS 5112: Q2.2
- VDA ACSMS Red Volume (1st Ed.): Q7.2, Q7.3, Q8.1
- VDA Automotive SPICE Cybersecurity: 14-51
- KBA Prüfkatalog: B.10, B.17
- CN ICV Access Guide: Annex1_2.4
- PSIRT Services Framework 1.1: 3.1.1

RSK A40: Continuous Risk Monitoring

The organization shall continuously reevaluate risks.

The organization uses a systematic and ongoing process to periodically re-evaluate risks

AND

The organization makes appropriate updates to processes and designs due to changes in the vehicle cybersecurity landscape.

- UN R155: 7.2.2.4
- VDA Automotive SPICE Cybersecurity: 08-14, 08-19, 13-20, 14-08, 15-09
- NHTSA Best Practices 2022: [G.21], [G.24]

RSK A50: Monitoring of vehicle data and logs

Vehicle data and vehicle logs shall be included in cybersecurity monitoring.

Internal sources for cybersecurity information do explicitly include vehicle data and vehicle logs (e.g. information from the field like vulnerability scanning reports, repair information and consumer usage information).

- UN R155: 7.2.2.1 ©, 7.2.2.4 (b)
- KBA Prüfkatalog: B.11, B.35
- CN ICV Access Guide: Article 08

RSK A60: Compliance of monitoring with legal requirements

The monitoring shall comply with legal requirements (e.g. privacy).

There is a process in place to identify relevant legal requirements related to cybersecurity monitoring activities.

AND

All requirements identified as relevant are complied with.

- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.4 (b)
- VDA ACSMS Red Volume (1st Ed.): Q7.1
- KBA Prüfkatalog: A.17
- CN ICV Access Guide: Article 03, Annex1_2.4

RSK B10: Analysis of vulnerabilities

All identified cybersecurity weaknesses related to the product level are adequately analyzed in order to identify vulnerabilities in products.

All identified cybersecurity weaknesses related to the product level are adequately analyzed.
AND
Identified vulnerabilities in products are reported accordingly.
AND
A rationale is provided for a weakness that is not identified as a vulnerability.

- ISO/SAE 21434:2021: [RQ-08-05], [RQ-08-06]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (g), 7.2.2.4 (b), 7.4.1
- ISO/PAS 5112: Q2.3
- VDA ACSMS Red Volume (1st Ed.): Q7.3
- VDA Automotive SPICE Cybersecurity: 08-19, 14-51, 14-08, 15-08
- KBA Prüfkatalog: B.10, B.11
- CN ICV Access Guide: Annex1_2.4, Annex1_2.6
- NHTSA Best Practices 2022: [G.15], [G.30], [G.31], [G.35]
- PSIRT Services Framework 1.1: 3.1.1

RSK B20: Management of vulnerabilities

All identified vulnerabilities on product level are adequately managed so that the treatment of underlying risks is enabled.

All cybersecurity risks related to weaknesses are analyzed and treated appropriately such that no unreasonable risks remain.
AND
Vulnerabilities are eliminated by applying an available remediation independent of a TARA.
AND
If cybersecurity incident response is necessary for the risk treatment, the according processes are followed.

- ISO/SAE 21434:2021: [RQ-08-07], [RQ-08-08]
- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (f), 7.2.2.2 (g)
- ISO/PAS 5112: Q2.4
- VDA ACSMS Red Volume (1st Ed.): Q6.1, Q7.4
- VDA Automotive SPICE Cybersecurity: 08-14, 08-19, 13-20, 14-08, 15-09
- KBA Prüfkatalog: B.10, B.11
- CN ICV Access Guide: Annex1_2.4, Annex1_2.6
- NHTSA Best Practices 2022: [G.15], [G.17], [G.30], [G.31], [G.35]
- PSIRT Services Framework 1.1: 4.1.1, 4.1.2, 4.1.3, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.3.1, 4.3.2, 4.3.3

RSK B30: Vulnerability information repositories and communication channels

Vulnerability information repositories or data bases and communication channels with an appropriate security level shall be implemented.

A repository or data base for storing and tracking vulnerability information is implemented.
AND
Communication channels to share vulnerability information are implemented.
AND
Vulnerability information repositories and communication channels have an adequate security level.

- PSIRT Services Framework 1.1: 1.5.1, 1.5.2, 1.5.3, 1.5.4, 3.3.4

RSK B40: Vulnerability coordination

Processes shall be established to ensure that vulnerability management activities are coordinated with all the relevant stakeholders including vulnerability finders and other involved vendors.

There is a process to receive, acknowledge and follow-up on vulnerability reports.
AND
All relevant external stakeholders such as vulnerability finders and other involved vendors are provided with the information they need to know regarding the handling of the vulnerability in a timely manner.
AND
Vulnerability disclosure is done in coordination with all affected stakeholders

PSIRT Services Framework 1.1: 5.2.1, 5.2.2

RSK B50: Vulnerability disclosure

Processes shall be established to ensure that vulnerability disclosure activities are done in a coordinated and transparent way following well- established criteria that ensures that all interested parties know about the vulnerability and how to fix it or mitigate it.

Criteria for responsible disclosure is well established so release notes and /or security advisories are produced and reviewed and CVEs are issued, when required.

AND

Disclosure is done in coordination with and it is communicated to all relevant internal stakeholders.

AND

Release notes and /or security advisories are made available to all affected customers.

– NHTSA Best Practices 2022: [G.27]
– PSIRT Services Framework 1.1: 5.3.1 , 5.3.2 , 5.3.3, 5.3.4

RSK B60: Vulnerability reproduction

The PSIRT shall ensure that the vulnerabilities reported are reproducible in order to validate and understand the conditions which lead to the vulnerable state.

Vulnerabilities are reproduced to validate vulnerability reports.

AND

A process for vulnerability reproduction is established considering:
- Expected timeline or SLAs
- Test environment and tools
- Evidence repositories
- Evaluation of all impacted products

– PSIRT Services Framework 1.1: 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5

RSK B70: Vulnerability remediation

Processes shall be established to ensure that a remedy is delivered on a predictable schedule so all relevant stakeholders can plan accordingly for the test and deployment of these remedies.

Processes are established to ensure that a remedy for a vulnerability is delivered.

AND

The process ensures that the deployment of the remedy is communicated to all relevant stakeholders.

– PSIRT Services Framework 1.1: Service 4.2 Remediation
  – Function 4.2.1 Analysis
  – Function 4.2.2 Remedy Resolution
  – Function 4.2.3 Remedy Delivery
  – Function 4.2.4 Risk Management Process
  – Function 5.1.2 Coordinators

RSK B80: Inventory system for vehicles

The organization shall address newly identified vulnerabilities dependent on vehicles in the field, vehicles built but not yet distributed to dealers, vehicles delivered to dealerships but not yet sold to consumers, as well as future products and vehicles.

Newly identified vulnerabilities are addressed to:
consumer-owned vehicles in the field

AND

vehicles built but not yet distributed to dealers

AND

vehicles delivered to dealerships but not yet sold to consumers

AND

future products and vehicles.

NHTSA Best Practices 2022: [G.32]

RSK C10: Assets and damage scenario identification

Assets, their cybersecurity properties and their damage scenarios are identified in appropriate quality.

All assets with cybersecurity properties are enumerated.
AND
A comprehensive set of damage scenarios is identified and documented.

- ISO/SAE 21434:2021: [RQ-15-01], [RQ-15-02]
- UN R155: 7.2.2.1 (a), 7.2.2.2 (b)
- ISO/PAS 5112: Q3.2
- VDA ACSMS Red Volume (1st Ed.): Q2.1
- VDA Automotive SPICE Cybersecurity: 08-19, 4-51, 14-52
- KBA Prüfkatalog: B.5, B.7, B.8, B.9
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.35]

RSK C15: Risk analysis prioritization

The analysis of risks shall be prioritized according to the highest potential impact.

Initial risk priorization based on impact is created before the risk analysis (prioriization might change in later stages).
AND
risks with the highest potential damage are analyzed first.

- VDA Automotive SPICE Cybersecurity: 13-04

RSK C20: Threat scenario identification

Appropriate threat scenarios shall be identified.

Appropriate threat scenarios are identified comprehensively (e.g. by misuse-case elicitation or threat modelling approaches) and documented with all relevant information (e.g.,. including the targeted asset and the cause of compromise of the cybersecurity property.).

- ISO/SAE 21434:2021: [RQ-15-03]
- UN R155: 7.2.2.1 (a), 7.2.2.2 (b)
- ISO/PAS 5112: Q3.2
- VDA ACSMS Red Volume (1st Ed.): Q2.1
- VDA Automotive SPICE Cybersecurity: 08-19, 14-51, 14-52
- KBA Prüfkatalog: B.7
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.35]

RSK C21: Management of software update risks in the vehicles

Functional safety risks, safety risks due to misuse and cybersecurity risks of the software update process in the vehicle and/or its components are managed.

Functional safety risks, and cybersecurity risks of the software update process in the vehicle and/or its components are managed by identification, analysis, evaluation and treatment of risks.
AND
Implications of failures during the software updates are analyzed, considered in the risk treatment and validated.

- ISO 24089:2023: 7.3.1.1, 7.3.1.2, 7.3.1.3, 8.3.3.5

RSK C30: Threats from UN R 155 Annex 5, Part A

The threats from Annex 5, Part A of the UNECE Regulations No. 155 shall be considered.

All threats from Annex 5, Part A of the UNECE Regulation No.155 are taken into account when defining threat scenarios.
AND
The threat scenarios are tailored to the system.

- UN R155: 7.2.2.1 (a), 7.2.2.2 (b)
- VDA ACSMS Red Volume (1st Ed.): Q2.1
- KBA Prüfkatalog: B.7

RSK C40: Impact rating

The impact on the defined damage scenarios shall be determined for all relevant categories.

All damage scenarios are assessed against potential adverse consequences for stakeholders.

AND

The assessment includes all of the independent impact categories: safety, financial, operational, and privacy.

AND

In case of further impact categories, they are documented.

AND

The impact rating is either 'severe', 'major', 'moderate' or 'negligible' and safety related impacts are derived from ISO26262-3:2018.

- ISO/SAE 21434:2021: [RQ-15-04], [RQ-15-05], [RQ-15-06]
- UN R155: 7.2.2.1 (a), 7.2.2.2 ©
- ISO/PAS 5112: Q3.1, Q3.2
- VDA ACSMS Red Volume (1st Ed.): Q3.1
- VDA Automotive SPICE Cybersecurity: 08-19, 14-08
- KBA Prüfkatalog: A.17, B.7
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.5], [G.35]

RSK C50: Attack path analysis

For all threat scenarios attack paths shall be identified.

For each threat scenario, a comprehensive set of attack paths that realizes the threat scenario is identified.

AND

The attack paths include a reference to the threat scenarios that can be realized by the attack path.

- ISO/SAE 21434:2021: [RQ-15-08], [RQ-15-09]
- UN R155: 7.2.2.1 (a), 7.2.2.2 (b)
- ISO/PAS 5112: Q3.2
- VDA ACSMS Red Volume (1st Ed.): Q2.1
- VDA Automotive SPICE Cybersecurity: 08-19
- KBA Prüfkatalog: B.7
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.6], [G.35]

RSK C60: Attack feasibility rating

Attack feasibility shall be determined for all attack paths.

The organization has defined criteria in order to rate attack feasibility for attack paths to "high", "medium", "low" or "very low".

AND

Attack feasibility is rated for all attack paths.

- ISO/SAE 21434:2021: [RQ-15-10], [RC-15-11], [RC-15-12], [RC-15-13], [RC-15-14]
- UN R155: 7.2.2.1 (a), 7.2.2.2 ©
- ISO/PAS 5112: Q3.1, Q3.2
- VDA ACSMS Red Volume (1st Ed.): Q3.1
- VDA Automotive SPICE Cybersecurity: 08-19
- KBA Prüfkatalog: B.7, B.8
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.35]

RSK C70: Risk determination

The risk value of each threat scenario shall be determined from the impact of the associated damage scenario and the attack feasibility of the associated attack paths.

The risk value of each threat scenario (1 lowest risk and 5 highest risk) is determined via a risk matrix. The determination criteria are the impact of the associated damage scenario and the attack feasibility of the associated attack paths.

AND

In case the threat scenario corresponds to more than one attack path, the maximum of the feasibility levels of the corresponding attack paths is assigned.

- ISO/SAE 21434:2021: [RQ-15-15], [RQ-15-16]
- UN R155: 7.2.2.1 (a), 7.2.2.2 ©
- ISO/PAS 5112: Q3.1, Q3.2
- VDA ACSMS Red Volume (1st Ed.): Q3.1
- VDA Automotive SPICE Cybersecurity: 08-19, 15-08
- KBA Prüfkatalog: B.7, B.8
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.35]

RSK D10: Risk treatment decision

For every risk a risk treatment option shall get defined.

A risk treatment option for each risk that considers impact categories, attack paths and the results from the risk determination is determined in accordance with recent technologies (e.g. the use of current cryptographic procedures). The risk treatment option can involve avoiding the risk, reducing the risk, sharing the risk or retaining the risk.

- ISO/SAE 21434:2021: [RQ-15-17]
- UN R155: 7.2.2.1 (a), 7.2.2.2 ©
- ISO/PAS 5112: Q3.2, Q3.3
- VDA ACSMS Red Volume (1st Ed.): Q3.2
- VDA Automotive SPICE Cybersecurity: 07-07, 08-14, 08-19, 13-20, 14-08, 15-09
- KBA Prüfkatalog: B.12
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.7], [G.8]

RSK D20: Communication of risk assessment results to key stakeholders

The organization shall have a process for communicating the risk assessment to the enterprise level.

The results are effectively communicated to the decision makers in a timely manner.

AND

The outcome from the risk assessments are kept simple and managed by key decision makers.

- UN R155: 7.2.2.1 (a), 7.2.2.1 (b), 7.2.2.1 ©, 7.2.2.2 (b), 7.2.2.2 ©, 7.2.2.2 (d), 7.2.2.2 (f)
- VDA Automotive SPICE Cybersecurity: 13-04

RSK D30: Technical requirements in the US Best Practices

All technical requirements in the US Best Practices shall be evaluated and an risk oriented implementation shall be decided.

All technical requirements in the US Best Practices are evaluated

AND

Risk oriented implementation is decided.

- NHTSA Best Practices 2022: [T.1]-[T.25], [G.6], [G.41], [G.42], [G.43]
- Ecosystem (ECO)

ECO A10: Demonstration and evaluation of supplier capabilities

Supplier capabilities for distributed cybersecurity activities shall be demonstrated and evaluated.

Supplier evaluation criteria are defined

AND

Candidate supplier selection is based on cybersecurity capability evaluation, and candidate suppliers must be able to demonstrate that they can develop according to CSMS.

AND

Cybersecurity capabilities of suppliers are evaluated before distributed activities start. If applicable, this includes the capabilities to perform post-development activities.

AND

Requests for quotation to candidate suppliers include a formal request to comply with relevant standards related to cybersecurity, the expectation to fulfill responsibilities for distributed activities, and the relevant cybersecurity goals or the related set of cybersecurity requirements.

- ISO/SAE 21434:2021: [RQ-07-01], [RC-07-02], [RQ-07-03]
- UN R155: 7.2.2.1 (a), 7.2.2.5
- ISO/PAS 5112: Q6.1
- VDA Automotive SPICE Cybersecurity: 12-01, 14-05, 15-21, 18-50 KBA Prüfkatalog: B.26, B.27, B.33
- NHTSA Best Practices 2022: [G.44]

ECO A20: Alignment of responsibilities for distributed cybersecurity activities

Interactions, dependencies, and responsibilities for distributed cybersecurity activities shall be aligned on.

Cybersecurity interface agreements are in place for all distributed activities with suppliers and customers and cover all relevant specifications (including points of contact regarding cybersecurity; distribution/joint performance of cybersecurity activities and if applicable their tailoring, sharing of information and work products, milestones and definition of the end of cybersecurity support).

AND

The actions and responsibilities required to respond to identified vulnerabilities are agreed between customer and supplier.

AND

Customer and supplier each notify the other if requirements are unclear, not feasible, or conflict with other cybersecurity requirements or requirements from other disciplines and appropriate decisions and actions are taken.

- ISO/SAE 21434:2021: [RQ-07-04], [RC-07-05], [RQ-07-06], [RQ-07-07], [RC-07-08]
- UN R155: 7.2.2.1 (a), 7.2.2.1 ©, 7.2.2.2 (g), 7.2.2.5
- ISO/PAS 5112: Q6.1
- VDA ACSMS Red Volume (1st. Ed.): Q7.4, Q9.1
- VDA Automotive SPICE Cybersecurity: 02-00, 02-01, 02-50, 08-20, 14-02
- KBA Prüfkatalog: B.26, B.33, B.35
- CN ICV Access Guide: Annex1_2.9
- NHTSA Best Practices 2022: [G.9], [G.28], [G.43], [G.44]

ECO A30: Final specification agreement between customer and supplier

The final specification agreement for development shall be agreed on between customer and supplier.

There is a final specification agreement between customer and supplier on timing and responsibility regarding all known vulnerabilities that should be fixed during development.

- JasPar TD-CSP-12 (V1.10): 1 (3.1.1)

ECO A40: Alignment of responsibilities for vulnerability management after development

The responsibilities for vulnerability management after development shall be aligned between customer and supplier.

For vulnerabilities detected after development and before production, all related parties agree on a specific treatment and on a reason for the selected treatment.

AND

All untreated vulnerabilities are managed as remaining risks and related agreements are recorded (including long term-responses like planning of next developments or enhanced monitoring of risk factors).

– JasPar TD-CSP-12 (V1.10): 8 (3.2.1), 9 (3.2.1)
– PSIRT Services Framework 1.1: 1.3.1, 1.3.2, 1.4.1, 4.2.4

ECO A50: Alignment of responsibilities for vulnerability management in uncovered cases

The responsibilities for vulnerability management in uncovered cases after development shall be aligned between customer and supplier.

A concept is determined between customer and supplier for the occurrence of new vulnerabilities in uncovered cases with unassigned responsibilities that cannot be handled under the conventional quality framework (including role assignment, responsibility assignment, cost sharing and respond times).

– JasPar TD-CSP-12 (V1.10): 20 (3.2.2), 21 (3.2.2), 22 (3.2.2)
– PSIRT Services Framework 1.1: 1.3.1, 1.3.2, 1.4.1

ECO A60: Alignment of responsibilities for PSIRT activities

The responsibilities for PSIRT activities shall be aligned between customer and supplier.

Suppliers (of parts/services installed in products) perform incident response activities and maintain a PSIRT structure in a long-term lifecycle in alignment with the customer and the OEM.

– JasPar TD-CSP-12 (V1.10): 2 (3.2.1), 3 (3.2.1), 4 (3.2.1), 5 (3.2.1)
– PSIRT Services Framework 1.1: 1.2.2, 1.4.1

ECO A70: Validation of PSIRT activities along the supply chain

The PSIRT activities shall be validated along the supply chain.

The PSIRT structure chart, the contact points list and communication lines are regularly reviewed internally and between organizations.

AND

The OEM ensures that PSIRT monitoring is properly performed in the whole supply chain by auditing the vulnerability information monitoring status (including regular requests and checks of vulnerability information monitoring status reports).

AND

Incident response and vulnerability response trainings are conducted regularly internally and along the supply chain.

– JasPar TD-CSP-12 (V1.10): 10 (3.2.1), 15 (3.2.1), 16 (3.2.1), 17 (3.2.1), 19 (3.2.1)

ECO A80: Alignment of responsibilities for monitoring

The responsibilities for monitoring shall be aligned between customer and supplier.

Monitoring status reports requested by the customer from the supplier include all relevant information (source, date of obtaining/judging information, judge/approver, triage results and reason).

AND

In case of an investigation request sent from the customer (or from the OEM over the supply-chain) to the supplier, the supplier will start impact analysis in the next steps according to that instruction. The activity is recorded.

AND

Responsibility assignment and cost sharing for monitoring are determined between customer and supplier.

– JasPar TD-CSP-12 (V1.10): 24 (3.2.2.1), 25 (3.2.2.1), 26 (3.2.2.1), 27 (3.2.2.1), 28 (3.2.2.1)

ECO A90: Alignment of responsibilities for event assessment

The responsibilities for event assessment shall be aligned between customer and supplier.

Event assessment reports requested by the customer from the supplier include all relevant information (including all information required in JasPar, e.g. reason of judgment if there is no impact and in case of impacts: impact range, assumed issues and a recommended countermeasure proposal).

AND

Results of performed assessments are recorded and all relevant information is documented by the customer (including all information required by JasPar, e.g. impact range at vehicle level, final judgment results and its reason)

AND

Responsibility assignment and cost sharing for event assessment are determined between customer and supplier.

- JasPar TD-CSP-12 (V1.10): 29 (3.2.2.2), 30 (3.2.2.2), 31 (3.2.2.2), 32 (3.2.2.2)

B: Communication & Collaboration

ECO B20: Reporting outcome of monitoring to authorities

The organization shall report at least once a year to its type approval authority/technical service the outcome and related actions of their monitoring activities.

Outcome from the monitoring activities is reported at least once a year to the type approval authority/ technical service that verified the compliance of the organization's CSMS

AND

The reporting includes all relevant information (on new cyber-attacks and on any additional actions taken) and confirmation that the organization's cybersecurity mitigations are still effective

AND

The reporting frequency is increased if events such as cyber-attacks are observed.

- UN R155: 7.4.1
- VDA ACSMS Red Volume (1st. Ed.): Q8.1
- KBA Prüfkatalog: B.4

ECO B21: Information exchange with type approval authority

The information exchange with type approval authorities is established.

Information exchange with type approval authorities is established.

AND

Information is exchanged regularly.

- KBA Prüfkatalog: B.4

ECO B30: Reporting of software update relevant information to authorities

The organization shall report relevant information for its software updates to type approval authorities or technical services.

Relevant information for software updates is reported to the type approval authority or technical service (e.g. for the purpose of type approval, conformity of production, market surveillance, recalls or periodic technical inspection).

AND

All information relevant to software updates, and if applicable, information relevant to any RXSWIN can be made available to the type approval authority or technical service.

AND

Documentation on the target vehicles of a software update and their compatibility can be made available to the type approval authority or technical service.

– UN R156: 7.1.1.1, 7.1.1.12
– KBA Prüfkatalog: B.11, B.21, B.23

ECO B31: Notification of related parties regarding updates

Related parties shall be notified about updates. The notification shall include all related information.

Vehicles users are notified about available updates (I.e., purposes, criticality, safety instructions, change log, affected functions during update process, estimated update duration, etc...) update operation.

AND

The identified information about the content of the software update campaign, is communicated to related parties that are documented in the software update campaign plan, including any changes to the user manual.

AND

Vehicle users are informed by the software update campaign about the relevant information, before the execution of the software update process.

– ISO 24089:2023: 6.3.3.1, 9.3.2.9, 9.3.2.10, 9.3.2.11, 9.3.2.17
– UN R156: 7.1.1.11, 7.2.2.2, 7.2.2.4
– KBA Prüfkatalog: B.21
– CN ICV Access Guide: Article 04, Annex1_3.9, Annex3_5.4

ECO B40: Reporting to J-Auto-ISAC

The organization shall report relevant information to J-Auto-ISAC.

New vulnerability information and relevant information after performing incident response or vulnerability response is provided to J-Auto-ISAC after discussion.

– JasPar-TD-CSP-12 (V1.10): 36 (4.1)

ECO B41: Chinese national security support

The organization shall provide technical support and assistance to maintain Chinese national security and carry out industry supervision as required by Chinese laws.

Providing technical support and assistance to maintain Chinese national security is included in the organization's policy.

AND

Technical support and assistance is provided when necessary to Chinese national security authorities/ executive powers.

– CN ICV Access Guide: Annex1_2.13

ECO B50: Reporting to CISA

Any incidents shall be reported to CISA/United States Computer Emergency Readiness Team (US-CERT) in accordance with the US-CERT Federal Incident Notification Guidelines.

Cyber security incidents are reported to CISA/United States Computer Emergency Readiness Team (US-CERT) in accordance with the US-CERT Federal Incident Notification Guidelines.

– NHTSA Best Practices 2022: [G.33]

ECO B60: Participate in Auto-ISAC activities

The organization shall actively participate in Auto-ISAC.

The organization actively participates in Auto-ISAC and other recognized standards development organizations

AND

the organization shares timely information concerning cybersecurity issues, including vulnerabilities, and intelligence information with the Auto-ISAC

AND

the organization collaborates in expeditiously exploring containment options and countermeasures to reported vulnerabilities, regardless of an impact on their own systems.

– NHTSA Best Practices 2022: [G.18], [G.23], [G.25], [G.26]

ECO B70: PSIRT reachability

The PSIRT communication shall be defined and the PSIRT shall be reachable.

Vulnerability reporting system/methods are set up, advertised and reachable, e.g. website, email, phone.
AND
Secure Communication for vulnerability reporting is ensured. (e.g., PGP/encryption)

– PSIRT Service Framework 1.1: 1.5.1, 1.5.2, 2.1.1, 5.1.3

ECO B71: PSIRT relevant external stakeholders list

The PSIRTs shall build and maintain a documentation about relevant external stakeholders.

The PSIRT documents all relevant external stakeholders, i.e.,
– Relevant PSIRTs (e.g. from customers and suppliers)
– Relevant security vendors
– Relevant Bug Bounty vendors
to convey information about product security vulnerabilities or during incident response events.

– PSIRT Service Framework 1.1: 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.3.1, 1.3.2, 1.4.1

ECO B72: Vulnerability finders list

A knowledge base shall be built with information about vulnerability finders.

Finder Database or document registering history and outcomes from interactions with different vulnerability reporters/ finders including their profiles and quality of their reports is maintained.
AND
For well-established finders consider accelerated handling of information.

– PSIRT Service Framework 1.1: 3.2.1, 3.2.2, 3.2.3, 3.2.4

ECO B80: Software update campaign termination

The end of software update campaigns shall be communicated to the vehicle user and related parties.

The end of each software update campaign is communicated to the vehicle user and related parties.

– ISO 24089:2023: 9.3.3.2

ECO B90: End of cybersecurity support

The end of cybersecurity support for products shall be communicated.

A procedure is in place to communicate to customers when the organization decides to end the cybersecurity support for a product.
AND
Configuration information is available for all products in the field until end of cybersecurity support.

– ISO/SAE 21434:2021: [RQ-14-01], [RQ-05-12]
– ISO/PAS 5112: Q5.5

Concept & Development (C&D)

A: Analysis & Planning

C&D A10: Planning of cybersecurity activities

The organization shall follow a robust procedure during the planning of cybersecurity activities

The organization analyses which cybersecurity activities are needed (determining cybersecurity relevance and applicability of reuse or tailoring).

AND

All cybersecurity activities necessary for concept and development are planned considering all relevant aspects (activity objectives, dependencies, responsible persons, resources, starting point, duration, work products).

AND

The cybersecurity plan and the work products are continuously updated and appropriate management is applied (e.g. configuration, documentation, change and requirements management).

AND

If cybersecurity activities are distributed, customer and supplier each define a cybersecurity plan regarding their respective cybersecurity activities and interfaces.

- ISO/SAE 21434:2021: [RQ-06-02], [RQ-06-03], [RQ-06-04], [RQ-06-05], [RQ-06-06], [RQ-06-07], [RQ-06-09], [RQ-06-10], [RQ-06-11], [RQ-06-12]
- UN R155: 7.2.2.1 (a), 7.2.2.2 (f), 7.2.2.5
- ISO/PAS 5112: Q1.4
- VDA ACSMS Red Volume (1st. Ed.): Q6.1, Q9.1
- VDA Automotive SPICE Cybersecurity: 08-19, 14-08
- KBA Prüfkatalog: B.6, B.14, B.18, B.26
- CN ICV Access Guide: Annex1_2.2
- NHTSA Best Practices 2022: [G.3], [G.19], [G.35]

C&D A11: Software update project plan

The organization shall develop and establish a plan for each software update project.

A plan for each software update project is developed, implemented and maintained (e.g., containing activities for developing and/or adapting the infrastructure, responsibilities, vehicle capabilities and processes).

- ISO 24089:2023: 5.3.1.1, 5.3.1.3

C&D A12: Assignment of responsibilities

Responsibilities regarding activities, under the organization's relevant management system(s), within projects shall be assigned and communicated.

The responsibilities regarding the activities under the organization's relevant management system(s) within projects are assigned and communicated.

- ISO/SAE 21434:2021: [RQ-06-01]
- ISO 24089:2023: 5.3.1.3
- ISO/PAS 5112: Q1.4
- KBA Prüfkatalog: A.4, A.11
- NHTSA Best Practices 2022: [G.2]
- PSIRT Service Framework: I. D., 1.1.1

C&D A20: Tailoring of cybersecurity activities in projects

The tailoring of the cybersecurity activities of projects shall be carried out appropriately, if it is necessary.

Cybersecurity activities can be tailored. In this case, a rationale for the adequacy and the necessity of this tailoring is provided.

AND

If items/components are reused, a formal reuse analysis is performed to address cybersecurity appropriately.

AND

If components developed out-of-context or off-the-shelf components are integrated, cybersecurity is considered and addressed appropriately.

- ISO/SAE 21434:2021: [PM-06-13], [RQ-06-14], [RQ-06-15], [RQ-06-16], [RQ-06-17], [RQ-06-18], [RQ-06-19], [RQ-06-20], [RQ-06-21], [RQ-06-22]
- ISO/PAS 5112: Q1.4
- KBA Prüfkatalog: B.14, B.18

C&D A21: Tailoring of software update projects

The tailoring of software update projects shall be carried out appropriately if it is necessary.

Software update projects can be tailored. In this case, a rationale for the adequacy and the necessity of this tailoring is provided.

- ISO 24089:2023: 5.3.2.1, 5.3.2.2

C&D A30: Item definition

All items in the scope of development shall be adequately defined during the concept phase.

Item definitions include all relevant information (i.e., including item boundary, item functions, preliminary architecture, information on constraints and applicable cybersecurity standards, and the operational environment of the item or assumptions about it).

- ISO/SAE 21434:2021: [RQ-09-01], [RQ-09-02]
- ISO/PAS 5112: Q4.1
- KBA Prüfkatalog: B.5
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.35]

C&D A40: Cybersecurity goals and cybersecurity claims

Based on TARA results, Cybersecurity goals shall be specified and cybersecurity claims shall be stated.

A TARA is thoroughly conducted, from which risk treatment decisions are determined for each threat scenario.

AND

Cybersecurity goals are specified if the risk treatment decision involves reducing the risk.

AND

Cybersecurity claims are stated if the risk treatment decision involves sharing the risk or retaining of the risk due to one or more assumptions.

AND

A process is established that confirms the completeness, correctness, and consistency of the TARA, the risk treatment decisions and the cybersecurity goals and claims.

- ISO/SAE 21434:2021: [RQ-09-03], [RQ-09-04], [RQ-09-05], [RQ-09-06], [RQ-09-07]
- UN R155: 7.2.2.1 (a), 7.2.2.2 ©, 7.2.2.2 (d)
- ISO/PAS 5112: Q3.3, Q4.1
- VDA ACSMS Red Volume (1st. Ed.): Q3.2, Q4.1
- VDA Automotive SPICE Cybersecurity: 08-19, 13-19, 13-22, 15-01, 17-11, 17-12, 17-51
- KBA Prüfkatalog: B.5, B.7, B.13, B.16
- CN ICV Access Guide: Annex2_3.1
- NHTSA Best Practices 2022: [G.4], [G.35]

C&D A50: Analysis of the architectural design for weaknesses

The architectural design defined by cybersecurity specifications shall be analyzed for weaknesses.

A comprehensive approach is used to analyze the architectural design defined by cybersecurity specifications to identify weaknesses.

AND

Weaknesses identified in the architectural design are resolved by changes, or are analyzed for vulnerabilities and vulnerabilities are managed in accordance with the general processes for vulnerability analysis and vulnerability management.

- ISO/SAE 21434:2021: [RQ-10-07]
- ISO/PAS 5112: Q2.3, Q4.2
- VDA Automotive SPICE Cybersecurity: 04-04, 04-05, 04-06, 15-50
- KBA Prüfkatalog: B.10
- CN ICV Access Guide: Annex2_3.3

C&D B10: Cybersecurity concept

A cybersecurity concept is specified to achieve the cybersecurity goals.

Cybersecurity controls in place and their interactions to achieve the cybersecurity goals are described.

AND

Cybersecurity requirements are specified to achieve all cybersecurity goals, taking into account the entire life cycle of the item and/or component.

AND

All cybersecurity requirements are allocated to the item, and if applicable to one or more components or the operational environment

AND

A process is established that confirms the completeness, correctness, and consistency (with respect to cybersecurity goals and cybersecurity claims) of the concept.

- ISO/SAE 21434:2021: [RQ-09-08], [RQ-09-09], [RQ-09-10], [RQ-09-11]
- UN R155: 7.2.2.1 (a), 7.2.2.2 (e)
- ISO/PAS 5112: Q4.1
- VDA ACSMS Red Volume (1st. Ed.): Q5.1
- VDA Automotive SPICE Cybersecurity: 04-06, 13-19, 13-22, 17-52
- KBA Prüfkatalog: B.12, B.13, B.16
- CN ICV Access Guide: Annex2_3.2

C&D B11: Development of software updates and update capabilities

Cybersecurity shall be considered appropriately for the development of software updates and update capabilities.

Updates and update capabilities are developed fully according to the established development processes regarding cybersecurity.

AND

Updates and recovery options are taken into account in the concept and development phases.

- ISO/SAE 21434:2021: [RQ-13-03]
- ISO/PAS 5112: Q5.4
- KBA Prüfkatalog: B.17
- CN ICV Access Guide: Article 02, Annex1_3.1, Annex1_3.2, Annex1_3.9

C&D B12: Vehicle-side management of software update processes

Functions to maintain vehicle-side management of relevant software update processes shall be established.

Proccesses are in place to ensure that functions are implemented to enable vehicle-side management of relevant software update procedures (e.g., for distributing and operating software updates, providing information to related parties, determining in-vehicle resources, handling interruptions, verifying integrity and authenticity, checking compability, ensuring a safe vehicle state, enabling simultaneous software update processes).

- ISO 24089:2023: 7.3.3.1, 7.3.3.2, 7.3.4.1, 7.3.4.2, 7.3.4.3, 7.3.4.4, 7.3.4.5, 7.3.4.6, 7.3.4.7, 7.3.4.8, 7.3.4.9, 7.3.4.10

C&D B20: Cybersecurity specifications

The cybersecurity specifications shall be defined comprehensively.

The cybersecurity specifications are based on the specifications from higher level of architectural abstraction and if applicable, on the selected cybersecurity controls and the existing architectural design.

AND

Cybersecurity requirements are allocated to components of the architectural design.

AND

Cybersecurity implications of post-development are considered and procedures to ensure cybersecurity after development are specified, if applicable.

- ISO/SAE 21434:2021: [RQ-10-01], [RQ-10-02], [RQ-10-03], [RC-10-06]
- VDA ACSMS Red Volume (1st. Ed.): Q5.1
- VDA Automotive SPICE Cybersecurity: 13-22, 17-11, 17-12
- KBA Prüfkatalog: B.15
- CN ICV Access Guide: Annex2_3.2

C&D B21: Verification of cybersecurity specifications

The cybersecurity specifications shall be verified to conform to the cybersecurity specifications from higher levels of architectural abstraction.

Verification of cybersecurity specifications covers completeness, correctness, adequacy with the cybersecurity requirements from higher level and consistency with the architectural design from higher level.

AND

Suitable verification methods are selected (e.g. review, analysis, simulation, prototyping).

– ISO/SAE 21434:2021: [RQ-10-18]
– ISO/PAS 5112: Q4.2
– VDA Automotive SPICE Cybersecurity: 13-19
– KBA Prüfkatalog: B.12, B.13
– CN ICV Access Guide: Annex2_3.4, Annex3_4.1 ~ 4.7

C&D B25: Cybersecurity design

The cybersecurity architectural design shall be defined comprehensively.

The cybersecurity architectural design is detailed based on the specifications and design from higher level of architectural abstraction and if applicable, on the selected cybersecurity controls.

AND

Cybersecurity related interfaces are refined considering the architectural design and the operating environment.

AND

Verification of cybersecurity architectural design covers completeness, correctness, adequacy with the cybersecurity requirements from higher level and consistency with the architectural design from higher level.

– VDA Automotive SPICE Cybersecurity: 04-04, 04-05, 04-06, 13-19, 13-22

C&D B40: State-of-the-art consideration related to cybersecurity

During development, the recent state-of-the-art for cybersecurity is taken into consideration.

The recent state-of-the-art for the design and implementation of cybersecurity is taken into consideration during development.

AND

Secure coding guidelines are according to the recent state-of-the-art.

– KBA Prüfkatalog: B.15
– NHTSA Best Practices 2022: [G.22], [G.23]

C&D B60: Access by alternative third-party repair services

The automotive industry shall provide strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner.

Strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner are provided

AND

Serviceability is considered

– NHTSA Best Practices 2022: [G.44], [G.45]

C&D C10: Programming notations and languages

Comprehensive criteria shall be used to select programming notations and languages for the cybersecurity specifications or their implementation.
Criteria for selecting design, modelling or programming notations or languages for the cybersecurity specifications or their implementation consider all relevant aspects (especially the use of secure design and implementation techniques). **AND** criteria for programming languages that are not sufficiently addressed by the language itself are covered by coding guidelines, or by the development environment.
– ISO/SAE 21434:2021: [RQ-10-04], [RQ-10-05] – VDA Automotive SPICE Cybersecurity: 11-05 – KBA Prüfkatalog: B.15

C&D D20: Integration and verification of components

Components shall comply with the cybersecurity specifications and no undesired functionalities regarding cybersecurity shall be contained.

Integration and verification activities are specified covering all relevant aspects (including the cybersecurity specifications, sufficient capability to support the specified functionality, and if applicable: configurations for series production and conformity with modelling, design and coding guidelines).

AND

The specified integration and verification activities are carried out to verify that the implementation and integration of components fulfil the defined cybersecurity specifications.

AND

If no testing for the verification activities is performed, a rationale is provided.

AND

If testing is performed for the verification activities, pass/fail criteria are specified and test coverage by test cases for the completeness of testing activities is determined.

AND

A process is established that confirms the completeness, correctness, and consistency of the verification specification with respect to the cybersecurity requirements and design.

- ISO/SAE 21434:2021: [RQ-10-09], [RQ-10-10], [RQ-10-11], [RC-10-12], [RQ-10-13]
- ISO/PAS 5112: Q4.2
- VDA ACSMS Red Volume (1st. Ed.): Q5.2
- VDA Automotive SPICE Cybersecurity: 08-50, 08-52, 13-22, 13-25, 13-50, 19-10
- KBA Prüfkatalog: B.10, B.11, B.12, B.13, B.14, B.30
- CN ICV Access Guide: Article 09, Annex2_3.4, Annex3_4.1 ~ 4.7

C&D D30: Validation of cybersecurity goals and cybersecurity claims for items

Cybersecurity goals and cybersecurity claims for items shall be validated.

Validation activities (e.g. penetration testing, reviews of work products related to cybersecurity goals and reviews of management of risks) at the vehicle level for the item considering the configurations for series production are performed to confirm consistency and achievement of the cybersecurity goals, validity of the cybersecurity claims and validity of the requirements on the operational environment, if applicable.

AND

The weaknesses identified during validation activities are analyzed for vulnerabilities and identified vulnerabilities are managed.

AND

A rationale for the selection of validation activities is provided.

- ISO/SAE 21434:2021: [RQ-11-01], [RQ-11-02]
- UN R155: 7.2.2.1 (a), 7.2.2.2 (e), 7.2.2.2 (g)
- ISO/PAS 5112: Q4.3
- VDA ACSMS Red Volume (1st. Ed.): Q5.2, Q7.6
- VDA Automotive SPICE Cybersecurity: 08-50, 13-04, 13-19, 13-22, 13-24, 19-11
- KBA Prüfkatalog: B.10, B.11, B.12, B.13, B.14, B.30
- CN ICV Access Guide: Article 09, Annex2_3.4, Annex3_4.1 ~ 4.7
- NHTSA Best Practices 2022: [G.13]

C&D D40: Cybersecurity case

A cybersecurity case shall be created for each project which provides an argument for the achieved degree of cybersecurity.

There are convincing arguments for the agreed and/or achieved degree of cybersecurity and these arguments are documented in comprehensive and structured way.
OR
There is a formal cybersecurity case, which is comprehensively supported by work products in order to provide the argument for the achieved degree of cybersecurity.

- ISO/SAE 21434:2021: [RQ-06-23]
- ISO/PAS 5112: Q.14
- KBA Prüfkatalog: B.14

C&D D50: Cybersecurity assessment

A cybersecurity assessment shall be performed that judges the achieved degree of cybersecurity, if applicable.

The decision if a cybersecurity assessment is performed for a project is based on a rationale (taking into account the risk of non-achievement of the needed degree of cybersecurity), which is independently reviewed.

AND

If applicable, cybersecurity assessment independently and competently judges the achieved degree of cybersecurity of a project taking into account all relevant information for the project (the cybersecurity plan and related all work products, the treatment of the cybersecurity risks, implemented cybersecurity controls, performed cybersecurity activities and provided rationales).

AND

If applicable, the results of cybersecurity assessment are provided in a report before the release for post-development and including a recommendation for acceptance, conditional acceptance, or rejection of the achieved degree of cybersecurity.

- ISO/SAE 21434:2021: [RQ-06-24], [RQ-06-25], [RQ-06-26], [RQ-06-27], [RQ-06-28], [RQ-06-30], [RQ-06-31], [RQ-06-32]
- ISO/PAS 5112: Q1.4
- KBA Prüfkatalog: B.6

C&D D60: Acceptance criteria for release for post-development

Acceptance criteria regarding cybersecurity shall be in place for the release for post-development.

The release for post-development follows a formal decision process.

AND

Prior the decision, the relevant information is available and sufficient in content and quality (including a comprehensive cybersecurity case with a convincing argument for the achieved degree of cybersecurity; if applicable, the cybersecurity assessment report, confirming the cybersecurity case; and, if applicable, the accepted cybersecurity requirements for post-development).

- ISO/SAE 21434:2021: [RQ-06-33], [RQ-06-34]
- ISO/PAS 5112: Q5.1
- VDA ACSMS Red Volume (1st. Ed.): Q5.4
- KBA Prüfkatalog: A.3, A.6

C&D D70: Cybersecurity tests according to CN ICV Access guide Annex 3.IV

Cybersecurity tests shall be performed during verification and validation based on CN ICV Access guide Annex 3_4.1 to 4.7.

Vehicle cybersecurity tests meet at least the requirements of CN ICV Access guide Annex3_4.1 to 4.7 (i.e., security threats during information transmission can be addressed, no published network vulnerabilities should exist, cybersecurity risks triggered by legal users' maloperation can be managed, security threats created by outside connections of the vehicle can be tackled, illegal critical data theft and damage can be prevented, the threat that a system is physically manipulated can be defended against, data loss and vehicle data leakage can be prevented).

- CN ICV Access Guide: Annex3_4.1 ~ 4.7

C&D D80: Independent Testing

Test stages shall employ qualified testers that are independent of the development team.

Test stages employ qualified testers.

AND

The testers have not been part of the development team.

AND

The testers are highly incentivized to identify vulnerabilities.

- NHTSA Best Practices 2022: [G.14]

Production & Operations (POP)

A: Production

POP A10: Production control plan

A production control plan shall be implemented that applies the cybersecurity requirements for production.

A production control plan is created that applies the cybersecurity requirements for post-development and includes all relevant information for cybersecurity during production (including sequence of steps that apply the cybersecurity requirements, production tools and equipment, cybersecurity controls to prevent unauthorized alteration during production, methods to confirm that the cybersecurity requirements for post-development are met).

AND

The production control plan is implemented.

- ISO/SAE 21434: [RQ-12-01], [RQ-12-02], [RQ-12-03]
- UN R 155: 7.2.2.1 (b), 7.2.2.2 (e)
- ISO/PAS 5112: Q5.2
- VDA ACSMS Red Volume (1st Ed.): Q5.3
- KBA Prüfkatalog: B.11, B.13, B.16, B.18
- CNC IVC: Annex1_2.3

POP A20: Conformity of production

The conformity of production shall comply with the 1958 agreements.

A production control plan is created that applies the cybersecurity requirements for post-development and includes all relevant information for cybersecurity during production (including sequence of steps that apply the cybersecurity requirements, production tools and equipment, cybersecurity controls to prevent unauthorized alteration during production, methods to confirm that the cybersecurity requirements for post-development are met).

AND

The production control plan is implemented.

- KBA Prüfkatalog: B.34

B: Detection & Response

POP B20: Cybersecurity incident response plan

An incident response plan shall be implemented for each cybersecurity incident.

For all cybersecurity incidents a cybersecurity incident response plan is created that includes all relevant information (including remedial actions, a communication plan, responsibilities for remedial actions, a procedure to record new relevant cybersecurity information, a method for progress determination, criteria for closure of the cybersecurity incident response and actions for closure).

AND

The cybersecurity incident response plan is implemented.

- ISO/SAE 21434:2021: [RQ-13-01], [RQ-13-02]
- UN R155: 7.2.2.1 ©, 7.2.2.2 (g), 7.2.2.3
- ISO/PAS 5112: Q5.3
- VDA ACSMS Red Volume (1st. Ed.): Q7.5
- VDA Automotive SPICE Cybersecurity: 08-14
- KBA Prüfkatalog: B.11, B.17
- CN ICV Access Guide: Annex1_2.5, Annex1_2.12
- NHTSA Best Practices 2022: [G.28], [G.30]
- PSIRT Services Framework 1.1: 4.3.1, 4.3.2, 4.3.3

POP B30: Deployment of PSIRT activities

PSIRT activities shall be deployed by the organization.

PSIRT activities include vulnerability information monitoring, assessment, and response.

AND

Occurred incidents and decisions of responsible persons are recorded, recurrence prevention is connected and related parties are informed.

AND

A list of contact points and an organization structure chart of PSIRT are prepared.

AND

The PSIRT processes are regularly evaluated and continuously improved.

- NHTSA Best Practices 2022: [G.30]
- JasPar TD-CSP-12 (V1.10): 6 (3.2.1), 7 (3.2.1), 12 (3.2.1), 13 (3.2.1), 14 (3.2.1), 18 (3.2.1)

POP C10: Software update campaign plan

The organization shall create, establish and maintain a software update campaign plan and implement processes that support software update campaign planning.

For each software update campaign, a software update campaign plan is created including purpose of the campaign, roles and responsibilities, and communication methods for informing related parties concerning the software update campaign.

AND

The software update campaign plan includes the confirmation of approval of software update packages that are part of the software update, required conditions and ressources needed, what vehicle configuration information that will be affected by the campaign, distribution methods for the software update execution, considerations for corrective actions in the event of a software update process failure in a vehicle, and considerations for special equipment, trained personal and vehicle user confirmation.

AND

Measures related to cybersecurity (at vehicle and/or infrastructure level) on the software update campaign are analyzed and determined based on all the requirments for each software update package.

– ISO/SAE 24089:2023: 9.3.1.1, 9.3.1.2, 9.3.1.3, 9.3.1.4, 9.3.1.5, 9.3.1.6, 9.3.1.7, 9.3.1.8, 9.3.1.10, 9.3.1.11, 9.3.1.12, 9.3.1.13, 9.3.1.14, 9.3.1.15

POP C12: Over-the-air update processes and procedures

Over-the-air updates shall be conducted safely and appropriately.

Processes and procedures ensure that over-the-air updates will not impact safety, if conducted during driving.

AND

Processes and procedures ensure that over-the-air updates are performed or overseen by a skilled person if required.

– UN R 156: 7.1.4.1, 7.1.4.2
– KBA Prüfkatalog: B.19, B.20, B.25
– CNC IVC: Annex1_3.8

POP C13: Over-the-air updates on vehicle level

The vehicle level for over-the-air updates is taken into account.

For over-the-air updates, the vehicle is ensured to have sufficient energy to complete the update.

AND

In case an over-the-air update is not carried out successfully, the vehicle software is set to the previous state.

– KBA Prüfkatalog: B.24

POP C15: Managing software update project information

The organization shall manage and store documentation for each software update project.

Documentation for each software update project is managed and stored according to documentation management and requirements management processes.

– ISO 24089:2023: 5.3.1.2

POP C17: Interoperability of infrastructure and vehicle capabilities for software updates

The interoperability of the infrastructure for software updates and software update-capable vehicles and components shall be confirmed.

The interoperability of the infrastructure for software updates and software update-capable vehicles and components is confirmed.

– ISO 24089:2023: 5.3.3.1

POP C18: Infrastructure capabilities for software updates

The organization shall maintain infrastructure that provides necessary and adequate capabilities for software updates.

Cybersecurity risks in the infrastructure for the software update process are managed.

AND

The infrastructure has functions for receiving, storing, processing, and distribution of relevant data to its relevant recipients (incl. failure notifications).

AND

The infrastructure has functions to verify the compatibility of the software update package and necessary invehicle resources.

AND

The infrastructure has functions to maintain the integrity of software updates packages, their contents and the collected configuration data (within the infrastructure and from the infrastructure to vehicles).

- ISO 24089:2023: 6.3.1.1, 6.3.2.1, 6.3.2.2, 6.3.2.3, 6.3.2.5, 6.3.3.1, 6.3.3.2, 6.3.4.1, 6.3.4.2, 6.3.4.3, 6.3.4.4, 6.3.4.5, 6.3.4.6, 6.3.4.7

POP C20: Verification and validation of software updates

Software updates shall be verified and validated.

Software functionality and the code of software updates are verified and validated appropriately before release.

AND

All software update packages are verified and validated to ensure only the intended software and metadata are included.

AND

The inclusion of necessary cybersecurity actions of the software update and necessary actions for the software update by the vehicle user or a skilled person are validated and verified.

- ISO/SAE 24089:2023: 8.3.3.1, 8.3.3.6, 8.3.3.7, 8.3.3.8
- UN R156: 7.1.3.3
- KBA Prüfkatalog: B.11, B.14
- CN IVC: Article 09, Annex1_3.4

POP C50: Influences of update packages on systems

Influences of updated systems to other systems shall be identified, assessed, recorded and validated.

Interdependencies of each software update with the target are identified and compability is checked.

AND

Influences on other hardware and software systems by the updated systems are assessed, identified, recorded and validated (including whether the target vehicles have sufficient in-vehicle capabilities to apply a specific update).

AND

This includes effects to type approved systems, systems required for the safe and continued operation of the vehicle, and modifications to functionality of the vehicle type (effects on previous test results, parameters/ functions defined within legislation, and type approval).

- ISO 24089:2023: 6.3.2.4, 6.3.4.5, 8.3.1.4, 8.3.3.3, 8.3.3.4, 9.3.1.9
- UN R 156: 7.1.1.5, 7.1.1.8, 7.1.1.9, 7.1.1.10
- KBA Prüfkatalog: B.21
- CNC IVC: Annex1_3.3

POP C60: Target vehicles for software updates

Target vehicles for software updates shall be identified and the compatibility information shall be provided and validated.

The target vehicles (incl. target ECUs) and related recipients for each software update are identified.

AND

Documentation listing target vehicles (on VIN-level) for each update and confirmation and validation of the compatibility of the last known configuration of those vehicles with the update is provided.

AND

The constraints on the distribution of the software update and necessary resources and conditions in the vehicle are identified and met.

- ISO 24089:2023: 6.3.4.2, 6.3.4.3, 7.3.2.3, 8.3.1.1, 8.3.1.3, 8.3.1.5, 8.3.1.6, 8.3.3.2, 9.3.2.1, 9.3.2.2
- UN R 156: 7.1.1.6, 7.1.1.7, 7.1.2.4
- KBA Prüfkatalog: B.21
- CNC IVC: Annex1_3.5
- NHTSA Best Practices 2022: [G.11]

POP C61: Software update campaign execution

For the execution of software update campaigns, processes, functions and instructions shall be in place.

Before start of each software update operation, it is confirmed that all required steps are completed regarding the development of the software update package, and regarding the software update campaign plan.

AND

Before start of each software update operation, the compatibility of the software update packages are confirmed and it is ensured that the necessary conditions to perform the software update operation are met.

AND

Processes regarding informing related parties, instructions for execution (including operation by trained persons) and handling of failures and unsafe states (e.g., by multiple requests) are established and maintained.

- ISO/SAE 24089:2023: 9.3.2.3, 9.3.2.4, 9.3.2.5, 9.3.2.6, 9.3.2.8, 9.3.2.12, 9.3.2.13, 9.3.2.14, 9.3.2.15, 9.3.2.16

POP C70: Assembling of software update packages

The content of software update packages shall be identified and adequately assembled.

The software and associated metadata (e.g., safe vehicle state, conditions, compatbility information, dependencies between ECUs, version information, in-vehicle ressources) for the identified targets of the software update process are identified including an unique identifier for the software update package.

AND

A process is established to ensure that only the intended software and metadata is assembled into the software update package (including verification and validation).

AND

A process is established to identify necessary actions for the software update package regarding cybersecurity and to determine necessary actions by the vehicle user or a skilled person.

- ISO/SAE 24089:2023: 8.3.1.2, 8.3.2.1, 8.3.2.2, 8.3.2.3, 8.3.1.7, 8.3.1.8, 8.3.3.6

POP C80: Confirmation of successful software updates

Confirmation shall be provided for software update packages.

For each software update and for each vehicle type, confirmation is provided that the software update will be conducted safely and securely.

AND

For each software update and for each vehicle type, confirmation is provided before release that the software update package was successfully verified and validated.

- ISO 24089:2023: 8.3.4.1
- UN R 156: 7.1.2.5
- KBA Prüfkatalog: B.22, B.25
- CNC IVC: Annex3_5.1, Annex3_5.3, Annex3_5.5, Annex3_5.6, Annex3_5.7

POP C90: Security of software updates and update processes

Security of software updates and update processes shall be ensured.

Processes are established to ensure the integrity of software update packages (incl. meta data) along the supply chain and the organizations internal infrastructure

AND

Software updates are protected against manipulation before the software is activated by ensuring integrity and authenticity of software update packages.

- ISO 24089:2023: 5.3.4.1, 9.3.2.7
- UN R 156: 7.1.3.1, 7.1.3.2
- KBA Prüfkatalog: B.9, B.10, B.17
- CNC IVC: Annex3_5.2

D: Decommissioning

POP D10: Information for secure decommissioning

Information for secure decommissioning shall be made available.

The cybersecurity requirements for post-development with regard to secure decommissioning are considered.

- ISO/SAE 21434:2021: [RQ-14-02]
- ISO/PAS 5112: Q5.6
- KBA Prüfkatalog: B.17
- CN ICV Access Guide: Annex1_2.11

Annex B: mapping of maturity level

PROOF	ASPICE ISO/ IEC 33020	NIST CSF	C2M2	OWASP SAMM	ENISA CSIRT	SPE	SSE-CMM	CMMI	ISO/PAS 5112 (2021-03-26)	VDA ACSMS Red Volume (1st edition)
Level 1: Initial	Process capability Level 0: **Incomplete process**	Tier 1: **Partial**			Under-basic	Security Level 0		Maturity Level 0: **Incomplete**	Fail	C: Audit failed
Level 2: Performed	Process capability Level 1: **Performed process**	Tier 2: **Risk Informed**	MIL1: **Initiated**	Maturity level 1	Basic	Security Level 1	Level 1 – **Performed Informally**	Maturity Level 1: **Initial**	Conditional pass	B: Audit failed; measures must be defined
Level 3: Established	Process capability Level 2: **Managed process**	Tier 3: **Repeatable**	MIL2: **Performed**	Maturity level 2	Intermediate	Security Level 2	Level 2 – **Planned and Tracked**	Maturity Level 2: **Managed**	Pass	A: Audit passed
	Process capability Level 3: **Established process**		MIL3: **Managed**				Level 3 – **Well Defined**	Maturity Level 3: **Defined**		
Level 4: Advanced	Process capability Level 4: **Predictable process**	Tier 4: **Adaptive**			Advanced	Security Level 3	Level 4 – **Quantitatively Controlled**	Maturity Level 4: **Quantitatively Managed**		
Level 5: Optimizing	Process capability Level 5: **Innovating process**			Maturity level 3: Regularity Improve		Security Level 4	Level 5 – **Continuously Improving**	Maturity Level 5: **Optimizing**		

Bibliography

Allianz. (2024, 01). Allianz Risk Barometer 2024. Retrieved 01 31, 2024, from https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Corfield, G. (2023, 4 9). Thieves are hacking into cars through their headlights, experts warn. Retrieved 3 4, 2024, from The Telegraph: https://www.telegraph.co.uk/business/2023/04/09/thieves-hacking-cars-through-headlights/

Minzlaff, D. M. (2023, 07). Automotive Cyber Maturity Report 2023. ETAS GmbH. Retrieved 04 05, 2024, from ETAS: https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-cyber-security-maturity-report-2023-20130802.pdf

NHTSA. (2015, 07 23). Safety Issues & Recalls (NHTSA ID 15V461000). Retrieved 01 31, 2024, from www.nhtsa.gov/recalls

NHTSA. (2022, 05 25). Safety Issues & Recalls (NHTSA ID 22V190000). Retrieved 01 31, 2024, from www.nhtsa.gov/recalls

UNECE. (04.03.2021). UN Regulation No. 155 – Cyber security and cyber security management system. Retrieved 01 31, 2024, from https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

UNECE, U. N.-I. (2024, January 26). UN extends its cyber security management regulation to motorcycles and scooters. Retrieved from United Nations Economic Commission for Europe: https://unece.org/media/press/387828

Contact information

ETAS GmbH
Ridlerstraße 57
80339 Munich
Germany

Marc-Oliver Schandera
T +49 89 356478100
info@etas.com
www.etas.com

Last updated: 07/2024