AQI Automotive Quality Institute

Long-term software maintenance throughout the entire vehicle lifetime

Checklist

Dr. Björn Schünemann (bjoern.schuenemann@aqigmbh.de)

Automotive Quality Institute – About Us

AQI Automotive Quality Institute

Founded: 2015 (as a wholly owned subsidiary of the **German Association of the Automotive Industry (VDA)**)

Located: Berlin Mitte, Französische Straße 13-14, 14052 Berlin

Number of employees: 8

What we do: Carry out innovative research and development projects to improve and strengthen quality processes in companies in the automotive industry. The AQI addresses current challenges faced by manufacturers and suppliers from a quality perspective and creates forward-looking concepts and methods.

Subject areas

Big Data – Data Analysis

Automotive Cybersecurity

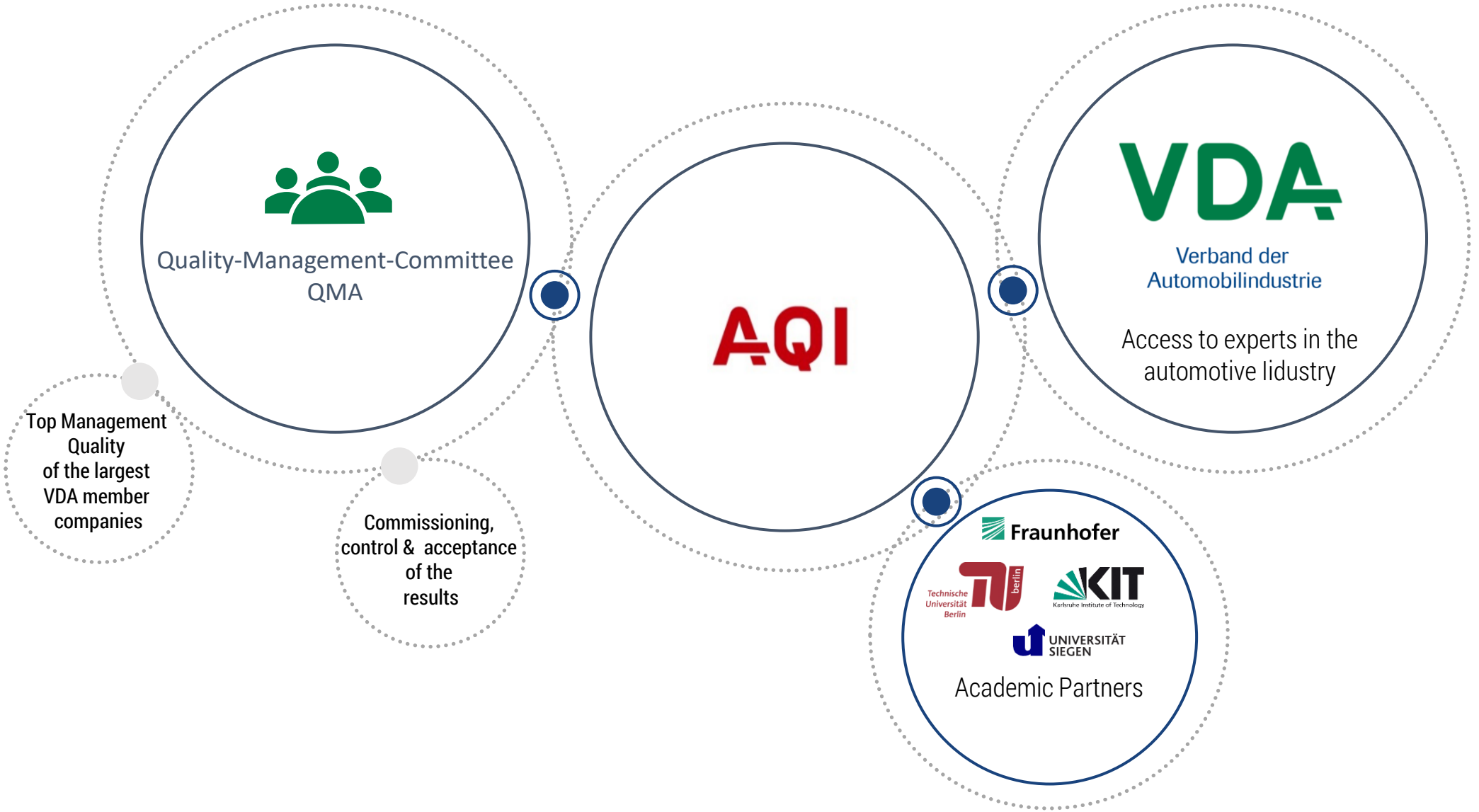
Connected/ Autonomous Driving

Electromobility

Methods and Processes

Connecting Economy and Science

AQI Automotive Quality Institute



Growing importance of software in the vehicle

0
lines of code

simply wired

Component-orientated,mechanics

50.000
lines of code

control units

First component orientation with software

1-3 Mio.
lines of code

control units and assistance systems

Component-, software- and network-orientated

10-100Mio.
lines of code

Many assistance systems with networking, over-the-air updates

- Complete networking-Embedding
- in ecosystem
- software platform for fully automated driving
- Software as a core competence

Function-orientated with the highest degree of networking

source: automotiveIT 25.05.2022

Why is this project so important?

Long-term software maintenance throughout the entire vehicle lifetime / Software updates until End-of-Life

AQI Automotive Quality Institute

Background

- As part of digital lifecycle management , the products must be kept up-to-date over the entire period of use (up to EOS/EOL) and also expanded with additional functionalities
- The technological or regulatory requirements must be ensured throughout the entire period
- This has an impact on, among other things Contracts/collaboration with suppliers, organizations at OEMs and suppliers, processes, etc.

Project goal

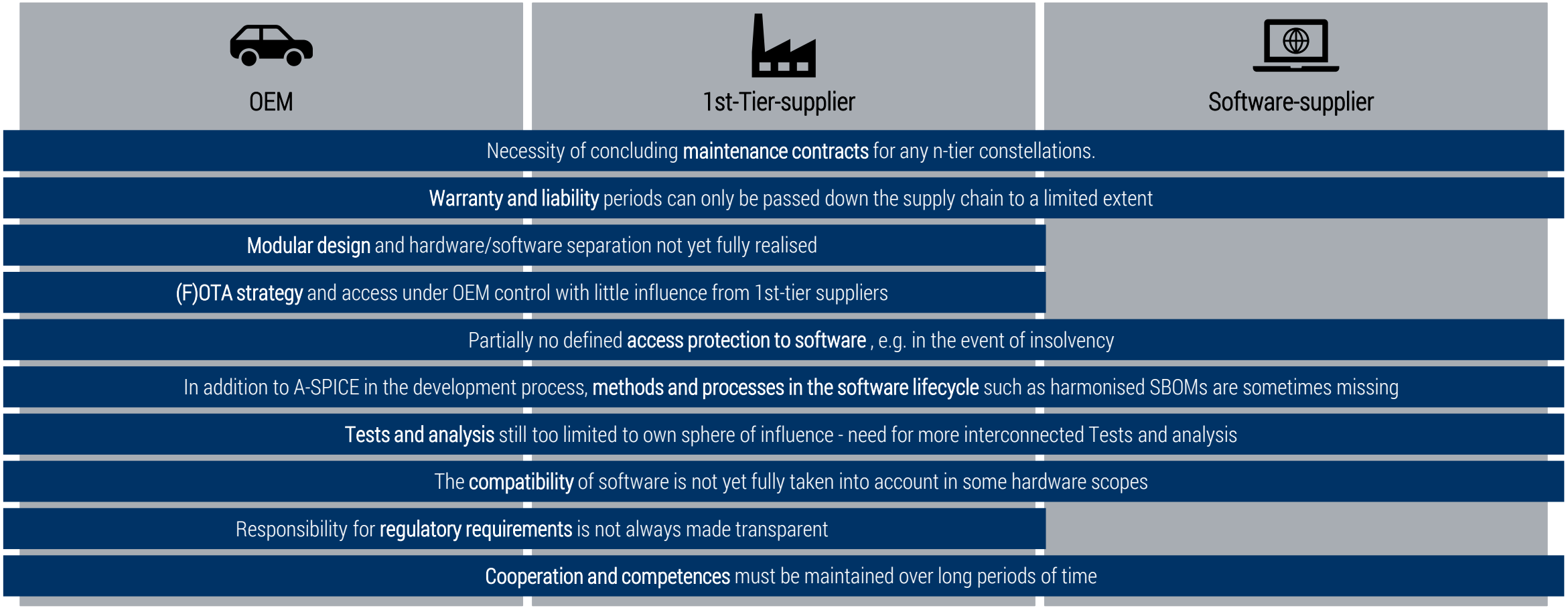
- From a quality perspective, these effects are currently not sufficiently taken into account in the cooperation between customer and supplier.
- The aim of the project is to analyze the effects of lifecycle management and identify existing gaps. Therefore, interviews and workshops are conducted with experts of several automotive companies.

Project results

- Identification of fields of action and the associated challenges
- Mapping of the requirements from the various sources (regulations, existing practice, ...) and allocation in the form of a checklist logic.

Summary of the challenges between OEM, 1st tier and software supplier

AQI Automotive Quality Institute



Checklist for long-term software maintenance over lifetime of software-intensive systems

AQI Automotive Quality Institute

1 Contract management

- Maintenance contracts
- Time periods
- Warranty and Liability
- Standard documents (e.g. general terms and conditions)
- Access protection

2 Vehicle Updates

- (F)OTA capability and interfaces
- Security and functional requirements

3 Maintenance & Testing

- Test strategies
- Development and testing environments
- Availability
- Knowledge management

4 Compatibility & modular design

- Compatibility strategy
- Modular design

5 Processes & Framework Conditions

- Open-Source Software
- A-Spice/VDA 6.3
- Cybersecurity

6 Risk management

- Risk assessment and -hedging
- Emergency and crisis management
- Legal framework and state of the art
- Disruptions and endcustomer behavior

7 Cooperation in a Tier N supplier structure

- Collaboration models (regarding (F)OTA, testing etc.)
- Cooperation with subcontractors
- Documentation (S-BOM)

1 Contract management

AQI Automotive Quality Institute

1.1 Maintenance Contracts : Clear definition and specification of maintenance contracts to ensure continuous software quality.

1.2 Time periods: Determination of the time periods in the project to ensure long-term maintenance and updates of the software.

1.3 Warranty and Liability : Warranty and liability agreements to regulate responsibilities in the event of a fault.

1.4 Standard documents: Use of standardised documents, such as general terms and conditions, to create a uniform contractual basis.

1.5 Access protection: Implementation of measures such as escrow agreements to ensure long-term access to software and source code.

1 Contract management

1.1 Maintenance contracts (1/2)

Checkpoints	Applies	Does not apply	Notes
The scope of the contract is clearly defined: The scope of the maintenance contracts is defined in detail, including all supported software modules, versions and hardware components.	☐	☐	
Responsibilities are clearly assigned: The responsibilities for all parties involved, including duties for updates, analysis, bug fixes and support, are clearly defined.	☐	☐	
Response times are clearly specifed: Binding response times for handling support requests and rectifying errors are set out in the contract.	☐	☐	
Key performance indicators (KPIs) are agreed: KPIs for maintenance services are defined to regularly monitor and evaluate service quality.	☐	☐	
Terms and renewal options are defined: The term of the maintenance contract as well as options and conditions for contract extensions are clearly regulated.	☐	☐	
Escalation processes are defined: Escalation levels and procedures in the event of disputes or non-compliance with contractual obligations are defined.	☐	☐	
Clear differentiation between bug fixing, the implementation of new features, and cybersecurity is contractually defined: The differentiation between "bug fixing," "implementation of new functions," and "cybersecurity measures" is specified to address potential discrepancies in service delivery.	☐	☐	
A maintenance team with the necessary expertise is contractually regulated and implemented: The implementation of a maintenance team with the required technical expertise and regular training is contractually defined.	☐	☐	

1 Contract management

1.1 Maintenance contracts (2/2)

Checkpoints	Applies	Does not apply	Notes
Cost structure is transparent: A transparent and comprehensible cost structure for all maintenance services, including regular updates and adjustments, has been created.	☐	☐	
Data security requirements are integrated: Requirements for data security and the protection of confidential information in the context of maintenance services are defined and implemented.	☐	☐	
Binding documentation requirements are defined: Binding requirements are defined to ensure traceability and transparency in the documentation of all maintenance work and changes	☐	☐	
Regular review and adjustment are agreed: Regular reviews of the maintenance contract are agreed upon. Adjustments to the maintenance contract are made if this is necessary to fulfil new technical or legal requirements.	☐	☐	

1 Contract management

1.2 Time periods

Checkpoints	Applies	Does not apply	Notes
Time periods for the development and maintenance phases are clearly defined: The lifecycle of a software product is divided into the development phase and the maintenance phase, and these time periods are explicitly defined in the maintenance contract.	☐	☐	
End-of-production (EOP) and end-of-service (EOS) are clearly defined : EOP and EOS, e.g., 15 years after the end of production, are clearly set with fixed dates and included in the maintenance contracts.	☐	☐	
Maintenance time periods cover the entire product life cycle: The defined maintenance periods cover the entire lifecycle, including active use and post-production support in the maintenance phase.	☐	☐	
Model maintenance and product upgrade cycles are defined: The cycles for model maintenance, product upgrades and software upgrades are clearly defined and adapted to the maintenance phases.	☐	☐	
Liability periods are regulated across the entire supply chain: The liability periods are transparent, clearly regulated and contractually stipulated throughout the entire supply chain.	☐	☐	
Adjustments for changes in the product lifecycle are considered: If the product lifecycle or production duration changes, the maintenance contracts are flexible enough to reflect these adjustment.	☐	☐	
All parties involved are informed about the time periods: The defined maintenance periods and their consequences are communicated transparently to all contractual partners and parties involved in the supply chain.	☐	☐	

1 Contract management

1.3 Warranty and liability

Checkpoints	Applies	Does not apply	Notes
Maximum limitation of liability (liability cap) is defined: Liability for damages is limited to a maximum sum in the form of a liability cap, e.g. twice the development costs for purely software-based solutions.	☐	☐	
Liability risks have been comprehensively analysed: All potential liability risks have been identified and considered in the contract to minimize unexpected costs.	☐	☐	
Contractual penalties for non-performance are defined: Contractual penalties are provided for if the contractually stipulated guarantee or liability conditions are not met.	☐	☐	
Liability limits are coordinated with suppliers: The defined liability limits are consistent across the entire supply chain and harmonised with the suppliers.	☐	☐	
Recourse claims are clearly regulated: The conditions for recourse claims in the event of defects or damages are clearly defined and contractually stipulated.	☐	☐	
Communication of liability conditions is ensured: All relevant parties in the supply chain are informed about the defined liability and warranty conditions and understand their obligations.	☐	☐	
The warranty period is defined over the entire service life of the product: When determining the warranty period, the entire service life of the product, including the post-production phase, is taken into account, and it's designed in such a way that parts can be actively included or excluded.	☐	☐	

1 Contract management

1.4 Standard documents

Checkpoints	Applies	Does not apply	Notes
Ensuring the use of standardised contract templates: All contracts and agreements are based on coherent, standardised document templates to ensure consistency and legal certainty.	☐	☐	
Accessibility of standard documents is ensured: Standard documents are easily accessible to all relevant parties, either via a central document management system or another agreed platform.	☐	☐	
Consistency across the supply chain is ensured: The use of standard documents is enforced across the supply chain to ensure consistent terms and procedures.	☐	☐	
The standard documents include legal requirements for data protection, liability, and confidentiality: All legally relevant clauses, including data protection, liability, and confidentiality, are comprehensively covered in the standard documents.	☐	☐	
Relevant GTC are known and accessible to all parties: All relevant General Terms and Conditions (GTC) are clearly documented, known to all parties involved and are always accessible.	☐	☐	
Archive, including version control, is implemented: All versions of the standard documents are archived in an audit-proof manner to ensure complete traceability and historical verification.	☐	☐	

1 Contract management

1.5 Access protection (1/2)

Automotive Quality Institute

Checkpoints	Applies	Does not apply	Notes
Access to source code and documentation is saved: The customer's access to the source code and the associated documentation of the software is clearly defined and contractually saved.	☐	☐	
Escrow agreements have been concluded: Escrow agreements exist to ensure access to necessary software components and documentation in the event of insolvency or other critical situations.	☐	☐	
Due diligence checks have been carried out: Comprehensive due diligence of individual vendors and subcontractors has been carried out to ensure the quality and reliability of suppliers, including the review of multi-vendor solutions.	☐	☐	
Code generation is comprehensively planned: Additional required engineering artifacts for code generation are identified to ensure that all necessary models can be correctly translated into code.	☐	☐	
Series releases are transferred to the escrow agent: It is ensured that all serial releases, including those prior to special events such as insolvencies, are transferred to the escrow agent in accordance with the escrow agreements.	☐	☐	
Clarity on multi-vendor strategies is ensured: The strategy for using multi-vendor solutions is clearly defined and considered to minimise dependency on a single vendor and strengthen access assurance.	☐	☐	
Regular reviews of escrow agreements is implemented: Escrow agreements are regularly reviewed and adjusted as necessary to ensure that they meet current requirements.	☐	☐	
Access rights are regulated transparently: All access rights to the source code, documentation and other critical software components are documented transparently and can be traced by all relevant parties.	☐	☐	

1 Contract management

1.5 Access protection (2/2)

Checkpoints	Applies	Does not apply	Notes
Contingency plans for access to software are in place: Contingency plans are implemented to ensure immediate access to important software components and documentation in the event that a provider fails or becomes insolvent.	☐	☐	

2 Vehicle Updates

AQI Automotive Quality Institute

2.1 (F)OTA capability and interfaces: Ensuring the technical requirements and interfaces for reliable over-the-air updates.

2.2 Security and functional requirements: Implementation of security standards and functional requirements to ensure the integrity and reliability of (F)OTA updates.

2 Vehicle Updates

2.1 (F)OTA capability and interfaces (1/2)

Checkpoints	Applies	Does not apply	Notes
Area of responsibility is clearly defined: The supplier's access and influence on (F)OTA updates are clearly defined and documented in the maintenance contract.	☐	☐	
Capability of the relevant control units is considered in the design: The ability of the control units (ECU) to support (F)OTA updates has already been considered in the design process and is clearly defined in the collaboration between OEM and supplier.	☐	☐	
Interfaces are standardized: The interfaces for (F)OTA updates are coherent and standardised across projects for both the OEM and the supplier.	☐	☐	
Processes for (F)OTA updates are standardised: All relevant processes for carrying out (F)OTA updates are clearly defined and implemented consistently across all project participants.	☐	☐	
Documentation strategy is clearly described: A clear documentation strategy is implemented that covers all aspects of (F)OTA updates, including the description and traceability of the update status.	☐	☐	
Update strategy is transparent: The strategy for carrying out updates is transparent and comprehensible for all parties involved, including the definition of priorities and schedules.	☐	☐	
Variant management is considered: Versions and updates are coordinated so that potentially all vehicles can be reached, and software versions can be updated in a targeted and efficient manner.	☐	☐	
Communication between OEM and supplier is ensured: Communication about (F)OTA updates between OEM and supplier is clearly regulated to ensure smooth coordination and implementation of updates.	☐	☐	

2 Vehicle Updates

2.1 (F)OTA capability and interfaces (2/2)

Checkpoints	Applies	Does not apply	Notes
Guaranteed consistency of (F)OTA processes: The processes for (F)OTA updates are designed consistently and without breaks to ensure that updates are carried out in a consistent and reliable manner.	☐	☐	
KPIs for (F)OTA updates are defined: Key performance indicators (KPIs) for the implementation of (F)OTA updates are defined in order to continuously monitor and evaluate the efficiency and quality of the updates.	☐	☐	
Test strategies for interfaces are established: Clear test strategies are established for all (F)OTA interfaces to ensure that they are comprehensively validated before the update rollout.	☐	☐	

2 Vehicle Updates

2.2 Security and functional requirements (1/2)

Checkpoints	Applies	Does not apply	Notes
The (F)OTA process is clearly defined: The entire (F)OTA process is clearly defined, including the security and functional requirements that must be met during the implementation of an update.	☐	☐	
A secure application of (F)OTA updates is ensured: The (F)OTA update process is protected by robust security mechanisms to prevent unauthorized access or manipulation during the transmission process.	☐	☐	
Process rate for (F)OTA updates is optimised: The process rate, e.g. the speed and efficiency with which (F)OTA updates are carried out, is optimised and ensures that updates are carried out within an acceptable time frame.	☐	☐	
Verification & Validation (V&V) is carried out comprehensively: Comprehensive Verification & Validation (V&V) processes are carried out before every (F)OTA update to ensure that the updates meet the specified security requirements and functional obligations.	☐	☐	
Data protection guidelines are implemented: Strict data protection guidelines are implemented to ensure that personal and security-relevant data remains protected during the (F)OTA process.	☐	☐	
Security standards are met: All (F)OTA updates meet the defined security standards and legal requirements to ensure the integrity and sucurity of the vehicle software.	☐	☐	
Security aspects are considered in the interfaces: All interfaces for (F)OTA updates are designed according to the highest security requirements to prevent unauthorised access.	☐	☐	
Regular security assessments are planned: Regular security assessments are planned to identify and rectify potential weaknesses in the (F)OTA processes at an early stage.	☐	☐	

2 Vehicle Updates

2.2 Security and functional requirements (2/2)

Checkpoints	Applies	Does not apply	Notes
Security protocols are continuously monitored: All security-relevant protocols and logs are continuously monitored in order to detect anomalies or security-critical events immediately.	☐	☐	
Data protection precautions have been taken: Special precautions have been taken to ensure that all (F)OTA updates are carried out in compliance with data protection regulations and to ensure that no sensitive information is disclosed.	☐	☐	

3 Maintenance & Testing

AQI Automotive Quality Institute

3.1 **Test strategies:** Development and implementation of clear test strategies to continuously monitor and ensure software quality.

3.2 **Development and test environments:** Provision and maintenance of development and test environments required for software development, as well as regular and comprehensive software testing.

3.3 **Availability:** Ensuring the long-term availability of tools and infrastructure to cover the entire product lifecycle.

3.4 **Knowledge management:** Implementation of a knowledge management system to ensure the long-term availability and transfer of expertise.

3 Maintenance & Testing

3.1 Test strategies (1/2)

Checkpoints	Applies	Does not apply	Notes
Test strategies and environments are defined and transparent: All test strategies, including the corresponding test environments and the "storage" of test data, are defined and comprehensibly regulated for all stakeholders.	☐	☐	
Contractual regulations for analysis and update capability are defined: Clear contractual regulations for the analysis and update capability of the software, including defined timeframes, are implemented.	☐	☐	
Test strategies for (F)OTA interfaces are established: Clear test strategies are defined for all (F)OTA interfaces to ensure that they are fully validated before the update rollout.	☐	☐	
Coordination of test strategies between all supply chain partners: There is clear coordination between all supply chain partners as to which changes require which tests, including the distinction between bug-fix verification and regression tests.	☐	☐	
Test period corresponds to the maintenance period: The test capability of the software is ensured over the entire maintenance period in order to guarantee continuous quality and reliability.	☐	☐	
Technology acceptance is clarified within the supply chain: The acceptance of the test technologies used is clarified among all partners, particularly regarding the handling of incomplete requirements.	☐	☐	
State-of-the-art is ensured: The test systems and models used are regularly reviewed and adapted to current standards and technologies to ensure that they meet the state-of-the-art.	☐	☐	
Specific test processes according to SOP are in place: According to the SOP, specific test procedures exist that have either been adopted from the development process or adapted accordingly to meet the requirements in series production.	☐	☐	

3 Maintenance & Testing

3.1 Test strategies (2/2)

Checkpoints	Applies	Does not apply	Notes
Changes and test requirements are coordinated: All changes to the software and the resulting test requirements are clearly coordinated between the partners involved to ensure smooth integration into the test process.	☐	☐	
Steadiness of tests is ensured: The continuity of testing processes is ensured throughout the entire product life cycle to ensure permanent compliance with all quality standards.	☐	☐	

3 Maintenance & Testing

3.2 Development and testing environments

Checkpoints	Applies	Does not apply	Notes
Tools and environments are strategically planned: It is ensured that development and testing tools, as well as their environments, are strategically planned and utilized effectively over the years. Continuous review and adjustments are carried out to avoid outdated systems.	☐	☐	
Long-term availability of the toolchain is guaranteed: The build and test toolchain is maintained over the specified periods to ensure continuous test capability throughout the entire product lifecycle.	☐	☐	
Development and testing environments are flexible and scalable for future requirements: The testing environments are designed to be flexible and adaptable to various requirements and scalable to meet future testing needs that were not known at the time of SOP.	☐	☐	
Responsibilities for development and testing environments are assigned across the entire supply chain: Responsibilities for the maintenance, updates, and operation of development and testing environments are clearly assigned across the supply chain for the deployment period up to EOS and are anchored in contracts.	☐	☐	
Technological currency of development and testing environments is ensured: Regular checks are conducted to ensure that development and testing environments are technologically up-to-date to enable state-of-the-art testing processes.	☐	☐	
Adjustments to development and testing environments are regularly made: Regular adjustments to development and testing environments are carried out when necessary to ensure they meet current and future requirements.	☐	☐	

3 Maintenance & Testing

3.3 Availabilities

AQI | Automotive Quality Institute

Checkpoints	Applies	Does not apply	Notes
Long-term availability of the test environments is ensured: It is ensured that all necessary test environments remain available throughout the entire product life cycle and are updated or replaced as required to maintain continuous testing and test capability.	☐	☐	
Redundancy for test tools and environments is planned: A redundancy strategy is implemented to provide alternative test tools and environments in case primary resources fail.	☐	☐	
Availability of test personnel is planned: The availability of qualified test personnel is ensured throughout the entire test and maintenance period, including training and resource planning.	☐	☐	
Capacity planning for testing resources is conducted across the entire supply chain until EOS: Thorough capacity planning ensures that sufficient test resources and capacities are available for all planned tests, especially during peak periods and after the end of production (EOP) or service (EOS).	☐	☐	
Regular functionality checks: The functionality of all test resources is checked regularly, and adjustments are made in order to react quickly to changes in requirements or technology.	☐	☐	

3 Maintenance & Testing

3.4 Knowledge management

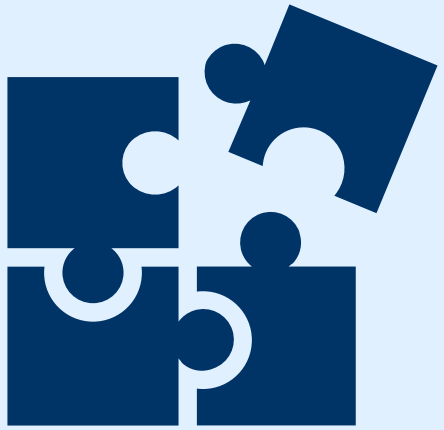
Checkpoints	Applies	Does not apply	Notes
Systematic documentation is implemented: All relevant information, processes and experiences are systematically documented and stored in a central knowledge management system to ensure access for everyone involved.	☐	☐	
Knowledge transfer is ensured: A formalised process for the transfer of knowledge between employees, teams and across the entire product lifecycle has been established to ensure that critical expertise is retained.	☐	☐	
Training concept for long-term technology use is in place: Regular training sessions and workshops are planned to ensure that knowledge remains up-to-date, new insights are continuously integrated, and expertise is maintained during long-term technology use.	☐	☐	
Knowledge management system is accessible and user-friendly: The knowledge management system is designed to be easily accessible and user-friendly for all relevant employees in order to promote effective use.	☐	☐	
Experience and best practices are regularly updated: Experience and best practices from day-to-day work and completed projects are regularly collected, evaluated and updated in the knowledge management system.	☐	☐	
Responsibilities for knowledge management are defined: Clear responsibilities are assigned for maintaining and updating the knowledge management system to ensure it is continuously relevant and up-to-date.	☐	☐	
Knowledge is integrated across the entire supply chain: Knowledge management includes not only internal information, but also knowledge from the entire supply chain to ensure a comprehensive view of all relevant processes and technologies.	☐	☐	
Software maintenance report is published: A software maintenance report with the operating status of the system, inspection and test results, Software changes, statistical analyses of errors and optimisation proposals etc. is created and made transparent.	☐	☐	

4 Compatibility & modular design

AQI Automotive Quality Institute

4.1 **Compatibility strategy:** Ensuring backward and forward compatibility of software and hardware throughout the entire lifecycle.

4.2 **Modular design:** Promotion of a modular software architecture that facilitates maintenance and expansion.



4 Kompatibilität & Modulare Bauweise

4.1 Compatibility strategy

Checkpoints	Applies	Does not apply	Notes
Compatibility strategy across the entire supply chain is defined: A comprehensive compatibility strategy that includes all levels of the supply chain is defined and ensures that both backward and upward compatibility is ensured across all suppliers.	☐	☐	
Backwards compatibility is ensured: Backward compatibility of software and hardware is strategically considered and implemented ensuring that new components remain compatible with older system.	☐	☐	
Forward compatibility of hardware is planned: The hardware forward compatibility strategy considers future requirements and includes measures to oversize hardware to facilitate future upgrades.	☐	☐	
Economic efficiency calculation for backwards compatibility has been prepared: A detailed profitability analysis to evaluate the costs and benefits of backwards compatibility has been carried out and taken into account in the strategic decision-making process.	☐	☐	
Regular compatibility checks are planned: Regular checks and tests are planned to ensure that the compatibility strategy is adhered to throughout the entire product life cycle.	☐	☐	
Documentation of compatibility requirements is transparent for the supply chain: All compatibility requirements are comprehensively documented and accessible to all parties in the supply chain to avoid misunderstandings.	☐	☐	
Long-term support for older systems is guaranteed: The strategy includes long-term support and maintenance of older systems to enable sustainable use of the existing infrastructure.	☐	☐	
Software-based implementation of functions is guaranteed : Functions are preferably implemented in software rather than hardware, considering long-term maintain-ability and costs. This approach ensures flexibility in responding to technological changes (e.g., mobile network shutdowns) with little to no hardware adjustments.	☐	☐	

4 Kompatibilität & Modulare Bauweise

4.2 Modular design

Checkpoints	Applies	Does not apply	Notes
Modular design has been implemented to manage complexity: A modular design has been introduced to manage the complexity of the system and enable flexible adaptation to future requirements.	☐	☐	
Strategy for disabling functions and components is defined: A clear strategy has been developed that makes it possible to switch off functions and components that are relevant to the use of the vehicle if necessary, in order to conserve resources and increase system stability.	☐	☐	
"Upgradeability of hardware" is taken into account: The possibility of expanding and upgrading the hardware, e.g. through memory expansions, is planned in order to be able to meet future requirements without having to completely replace the hardware.	☐	☐	
Strategy for modular expansion is defined: There is a clearly defined strategy for the modular expansion of the system, which ensures that new functions and components can be easily integrated without affecting the existing architecture.	☐	☐	
Regular review and adaptation of the modular strategy: The modular strategy is regularly reviewed and adapted to new technological developments and business requirements in order to maintain the competitiveness and efficiency of the system.	☐	☐	
The ability to switch off certain functions and components has been legally checked: The ability to switch off certain functions and components has been legally checked and is unobjectionable from a legal point of view.	☐	☐	

5 Processes & Framework Conditions

AQI Automotive Quality Institute

5.1 **Free and open source software (FOSS):** Integration and maintenance of open source software to ensure long-term maintainability and adaptability.

5.2 **A-Spice/VDA 6.3:** Compliance with standards such as A-SPICE and VDA 6.3 to ensure process quality in software development and maintenance.

5.3 **Cybersecurity:** Regular review and updating of cybersecurity measures to ensure protection against threats.

5 Processes & Framework Conditions

5.1 Free and Open Source Software (FOSS)

Checkpoints	Applies	Does not apply	Notes
License compliance is verfified: Compliance with all FOSS license terms has been legally verified and is aligned with the project's and company's goals.	☐	☐	
FOSS components are documented and traceable: All FOSS components used are fully documented and versions are clearly traceable to ensure consistent maintenance and updates.	☐	☐	
Security updates for FOSS components are implemented promptly: Security-relevant updates for FOSS components are checked and implemented promptly in order to avoid vulnerabilities in the system.	☐	☐	
Maintenance plans for open source components are defined: Clear maintenance plans are defined for all FOSS components used to ensure their long-term functionality and security.	☐	☐	
Compatibility of FOSS components is checked regularly: The compatibility of the FOSS components with the other systems is checked regularly in order to identify and rectify integration problems at an early stage.	☐	☐	
Risk analysis for FOSS use has been carried out: A comprehensive risk analysis regarding the use of FOSS components has been carried out to identify potential risks and plan appropriate measures.	☐	☐	
Strategy for dealing with FOSS dependencies is defined: A clear strategy for dealing with dependencies on FOSS components, including possible alternatives, is defined to ensure system stability even in the event of changes in the FOSS community.	☐	☐	
Development team available and guarantees Long Term Support (LTS): The FOSS development team is trustworthy, can ensure long-term maintenance of the software and guarantees LTS / The FOSS development team is reliable and ensures long-term maintenance of the software, providing "LTS".	☐	☐	

5 Processes & Framework Conditions

5.3 A-Spice/VDA 6.3

Checkpoints	Applies	Does not apply	Notes
A-SPICE assessment successfully completed: Internal or external A-SPICE assessment has been carried out successfully so that all relevant development and maintenance processes can be implemented in compliance with A-SPICE.	☐	☐	
VDA 6.3 audit successfully completed: A VDA 6.3 audit was successfully carried out, ensuring that the quality and performance of processes and their output meet the requirements of the VDA 6.3 standard.	☐	☐	
Process documentation is complete and up-to-date: All A-SPICE and VDA 6.3-relevant processes are comprehensively documented and are regularly checked to ensure they are up-to-date and effective.	☐	☐	
Regular training courses on A-SPICE/VDA 6.3 are held: Employees involved in the relevant processes receive regular training to ensure that they are familiar with the requirements and best practices.	☐	☐	
A-SPICE assessments and VDA 6.3 audits are repeated regularly: A-SPICE assessments and VDA 6.3 audits are repeated regularly to check compliance with the standards and identify opportunities for improvement.	☐	☐	

5 Processes & Framework Conditions

5.4 Cybersecurity

Checkpoints	Applies	Does not apply	Notes
Cybersecurity measures are comprehensively implemented: All relevant measures derived from normative legal frameworks and the state of the art have been fully implemented and adapted to current requirements.[1]	☐	☐	
Uniform implementation of cybersecurity measures across the supply chain is ensured: A long-term strategy ensures that all cybersecurity measures are consistently implemented throughout the entire supply chain, including adaptation to new legal regulations and the current state of the art.	☐	☐	

[1] Numerous standards/guidelines address cybersecurity. Depending on the context of application, the following standards/guidelines are relevant for the German automotive industry:

- UNECE R155: Cyber security and cyber security management system.
- UNECE R156: Software update and software update management system.
- ISO/SAE 21434: Road vehicles – Cybersecurity engineering.
- ISO 24089: Road vehicles – Software update engineering.
- ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems.
- ISO/TR 4804: Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation.
- IEC 62443: Security for industrial automation and control systems.
- VDA TISAX und ISA: Standards for information security assessments, specifically developed for the automotive industry.
- VDA guideline „Cybersecurity for vehicles“: VDA guide for security of vehicle software.
- ASPICE for Cybersecurity 2.0 (2025)

6 Risk management

AQI Automotive Quality Institute

6.1 Risk assessment and hedging: carrying out systematic risk assessments and implementing measures to minimize risks.

6.2 Emergency and crisis management: Development and implementation of processes for dealing with emergencies and crisis situations, especially cybersecurity incidents.

6.3 Legal framework and state of the art: Monitoring of legal and technical developments in order to plan and implement software adaptations in good time.

6.4 Disruptions and end customer behaviour: Identification and assessment of risks resulting from disruptions and changing end-customer behaviour.

6 Risk management

6.1 Risk assessment and hedging

AQI Automotive Quality Institute

Checkpoints	Applies	Does not apply	Notes
Regular risk assessments are implemented: Comprehensive risk assessments are carried out regularly in order to identify and document potential risks in software and system operation at an early stage.	☐	☐	
Risk categories are clearly defined: All relevant risks are categorised, e.g. technical risks, security risks, supply chain risks, to enable targeted analysis and prioritisation.	☐	☐	
Risk mitigation measures have been established: Specific risk mitigation measures have been defined and implemented for all identified risks in order to minimize the impact of potential risks.	☐	☐	
Responsibilities for risk management are defined: Clear responsibilities are defined for monitoring, assessing and managing risks throughout the entire product lifecycle.	☐	☐	
Risk management is integrated into decision-making processes: Risk management is firmly integrated into all strategic and operational decision-making processes to ensure that risks are considered in all important decisions.	☐	☐	
Continuous monitoring of risk measures is ensured: All implemented risk mitigation measures are continuously monitored and checked for effectiveness so that adjustments can be made if necessary.	☐	☐	
Documentation and communication of risks are ensured: All identified risks, their assessment and the measures taken are comprehensively documented and regularly communicated to all relevant stakeholders.	☐	☐	

6 Risk management

6.2 Emergency and crisis management

AQI Automotive Quality Institute

Checkpoints	Applies	Does not apply	Notes
Emergency plans are comprehensively defined: Comprehensive emergency plans are developed that contain clear instructions and protocols for dealing with various crisis scenarios, such as system failures or security incidents.	☐	☐	
Crisis management team is appointed: A specialised crisis management team has been appointed and is responsible for implementing the emergency plans and coordinating all activities in the event of a crisis.	☐	☐	
Regular emergency drills are carried out: Regular emergency drills and simulations are carried out to test the team's ability to respond and to identify and rectify weaknesses in the emergency plans.	☐	☐	
Communication protocols are defined: Clear communication protocols are defined in the event of a crisis to ensure that information is passed on quickly and effectively both internally and externally.	☐	☐	
Crisis management strategies are documented: Detailed crisis management strategies, including escalation levels and decision paths, are documented and regularly updated.	☐	☐	
Resources are available in the event of a crisis: All necessary resources, such as alternative IT infrastructures, spare parts or external service providers, are planned and quickly available in the event of a crisis.	☐	☐	
Learnings after crises are documented: A formalised process for the evaluation and documentation of findings from emergency exercises and real crisis cases is implemented to ensure continuous improvements in crisis management.	☐	☐	

6 Risk management

6.3 Legal framework and state of the art (1/2)

Checkpoints	Applies	Does not apply	Notes
Changes to the normative and legal framework are monitored regularly: Regular screening is conducted to identify legislative changes, court rulings, new regulations and standards at an early stage and assess their impact on the software and processes.	☐	☐	
Long-term software adjustments due to changes in legislation are planned : Long-term adjustments to the software, required by new legal demands, court rulings, or regulatory changes, are considered in the development and maintenance processes, including in the supply chain.	☐	☐	
Resposibility for legislative changes is defined: The responsibilities within the supply chain for updating software components due to legal changes are clearly defined.	☐	☐	
Global screening for legal changes is implemented: Global screening is carried out regularly in order to identify mid- and long-term legal and regulatory changes and incorporate them into software planning in good time.	☐	☐	
Changes in the state of the art are continuously monitored: Developments in the state of the art are continuously monitored to ensure that the software components and technologies used comply with current standards.	☐	☐	
Long-term software adaptations due to technical developments are planned: Long-term adjustments to the software necessitated by technological developments or new industry standards are planned and implemented throughout the supply chain.	☐	☐	
The area of responsibility for changes to the state of the art is clearly defined: The responsibilities for updating software components as a result of changes to the state of the art are clearly defined for all suppliers and parties involved.	☐	☐	
Implementing technological developments screenings: A proactive screening process, which identifies potential technological changes and their impact on software development in the medium and long term, is integrated into the planning process.	☐	☐	

6 Risk management

6.3 Legal framework and state of the art (2/2)

Checkpoints	Applies	Does not apply	Notes
Residual risks are continuously analyzed: The residual risks that remain after the application of security measures are regularly reviewed through Threat Assessment and Risk Analysis (TARA) and adjusted to changes in the state of the art to identify and minimize security vulnerabilities at an early stage.	☐	☐	

6 Risk management

6.4 Disruptions and end-customer behavior

AQI Automotive Quality Institute

Checkpoints	Applies	Does not apply	Notes
Risk management for temporary disruptions and infrastructure failures failures is implemented: Measures have been established to minimise the risk of temporary service disruptions, such as GPS failures or mobile network interruptions, in order to ensure the functionality of the software.	☐	☐	
Strategies for the end of supported protocols or standards are defined: Clear strategies and alternatives have been implemented in order to be able to react flexibly to the end of support for protocols in use or the shutdown of mobile communications standards.	☐	☐	
Proactive screening for long-term infrastructure changes: Technological changes, such as the discontinuation of mobile communications standards or protocols, are recognised at an early stage and integrated into long-term software planning in order to implement alternative solutions in good time.	☐	☐	
Changes in customer behavior are continuously monitored: The behavior of end customers, particularly with regard to data protection, user interaction and environmental awareness, is regularly analysed in order to be able to react to changing expectations at an early stage.	☐	☐	
Adjusting the user interface to customer needs is guaranteed: The user experience and user interface of the software are regularly adapted to the changing habits and expectations of end customers in order to prevent loss of acceptance and meet modern user requirements.	☐	☐	

7 Cooperation in a Tier N supplier structure

AQI Automotive Quality Institute

7.1 Collaboration models: Development and implementation of collaboration models between OEMs and suppliers to optimize (F)OTA, testing and other processes.

7.2 Cooperation with subcontractors: Ensuring smooth cooperation and coordination with subcontractors in the supply chain.

7.3 Documentation (SBOM, CBOM): The use and maintenance of Software Bills of Materials (SBOMs) and Cryptographic Bills of Materials (CBOMs) ensure a comprehensive inventory of all components of a software product, making it traceable and transparent across the entire supply chain.

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.1 Collaboration models

Checkpoints	Applies	Does not apply	Notes
Collaboration models are clearly defined: Clear collaboration models have been established between OEMs and suppliers that clearly regulate responsibilities, interfaces and communication channels / Clear collaboration models between OEMs and suppliers are established, defining responsibilities, interfaces, and communication paths.	☐	☐	
Regular coordination meetings are planned: Regular meetings between all parties involved are planned to coordinate cooperation and discuss any problems or changes that arise in a timely manner.	☐	☐	
Information exchange is transparent and standardised: A transparent and standardised process for the exchange of information between all partners is implemented to avoid delays and misunderstandings.	☐	☐	
Responsibilities and competencies are documented: All responsibilities and accountabilities within the collaboration models are clearly documented and assigned to the respective parties.	☐	☐	
Flexibility in collaboration is guaranteed: The collaboration models are designed to be flexible in order to be able to react quickly to changes in the supply chain, such as new requirements or partners.	☐	☐	
Risk and conflict management are integrated: Processes for risk and conflict management are integrated into the collaboration models in order to identify and overcome potential challenges in collaboration at an early stage.	☐	☐	
Continuous improvement of collaboration is ensured: Mechanisms have been implemented for the continuous improvement of collaboration that provide for regular feedback loops and optimisation measures.	☐	☐	

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.2 Cooperation with subcontractors

Checkpoints	Applies	Does not apply	Notes
Strategic knowledge management is implemented: A strategic knowledge management system has been established to ensure that the know-how of subcontractors is saved in the long term and passed on as required.	☐	☐	
Distribution of responsibilities is clearly defined: The distribution of competencies between OEMs, suppliers and subcontractors is clearly regulated and documented to ensure smooth cooperation.	☐	☐	
Documentation is transparent and accessible: All relevant documentation, including technical specifications and process descriptions, is accessible to all partners and is updated regularly.	☐	☐	
Future-proof standards are defined: Future-proof and state-of-the-art standards and programming languages are jointly defined and consistently applied by all parties involved.	☐	☐	
Use of common tools is guaranteed: It is ensured that OEMs, suppliers and subcontractors access a common tool infrastructure to maximize efficiency and consistency in collaboration.	☐	☐	
Transparent communication channels are established: Clear and transparent communication channels have been established between OEMs, suppliers and subcontractors in order to optimise the flow of information and coordination.	☐	☐	
Regular review of cooperation takes place: Collaboration with subcontractors is regularly reviewed and optimised to ensure that all partners continue to follow the defined standards and processes.	☐	☐	
Risk analysis and contingency plans for interruptions in the supply chain are implemented: Robust contingency plans and risk analyses are in place to ensure a rapid response to bottlenecks in software maintenance and support due to extreme situations such as political conflicts, environmental impacts or blocked trade routes.	☐	☐	

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.3 Documentation (SBOM, CBOM)

Checkpoints	Applies	Does not apply	Notes
SBOM implemented according to the state of the art: The handling of SBOMs (Software Bills of Materials) complies with the current state of the art and the recommendations/guidelines of authorities and other relevant institutions.[1]	☐	☐	
CBOM implemented according to the state of the art: The management of CBOMs (Cryptographic Bills of Materials) aligns with the current state of the art. All cryptographic mechanisms used in the product, including algorithms and key lengths, are thoroughly documented, and relevant guidelines are adhered to.	☐	☐	
Standardised implementation in the supply chain: The handling of SBOMs and CBOMs is standardised for the entire supply chain.	☐	☐	

[1] Today, there is no standardised way of dealing with SBOMs in the German automotive industry - the following sources provide recommendations for dealing with SBOMs, among others:

Recommendation for software manufacturers by the German Federal Office for Information Security (BSI). Part 2 of the Technical Guideline TR-03183 'Cyber Resilience

Requirements ": https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=5

Guidance from the National Telecommunications and Information Administration (NTIA): https://www.ntia.gov/page/software-bill-materials

Recommendations of the US Department of Defense: https://media.defense.gov/2023/Dec/14/2003359097/-1/-1/0/CSI-SCRM-SBOM-Management-v1.1.PDF

Recommendations of the US Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov/sbom