AQI Automotive Quality Institute

Training content for long-term software maintenance throughout the entire vehicle lifetime

Detailed Project Overview

Dr. Björn Schünemann (bjoern.schuenemann@aqigmbh.de)
Christof Lorenz (christof.lorenz@automotive-quality-consulting.com)

Agenda

AQI Automotive Quality Institute

- Project description of the approach
- Project contents
- Checklist reference – Timeline and responsibilities

Training content for long-term software maintenance throughout the entire vehicle lifetime

AQI Automotive Quality Institute

Follow-up project 2025

Description of the situation and problem

- As part of digital lifecycle management, products must be kept up to date throughout their **entire service life** and **expanded with additional functionalities**. This has an impact on, among other things, **contracts/cooperation in customer-supplier relationships**, as well as on **organizations and processes** at OEMs and suppliers.
- The AQI developed a **10-point plan** in the 2023 project and a comprehensive **checklist** in the 2024 project, which can be used immediately in companies. These results help to meet the challenges of ensuring the long-term software maintenance throughout the entire vehicle lifetime.
- In order to further support implementation in companies, **training content** is to be developed from these materials and the further project results in the current project. To this end, it is necessary to determine the **skills/knowledge required of employees** in addition to the **technical requirements** developed in the two previous projects and to create a **mapping** between the technical requirements and the skills/knowledge required of employees.
- The training content should be developed in two stages, if necessary: as **a self-learning program** and as a **training course**.

Purpose and benefits

- **Objective:** To ensure software quality in the customer-supplier relationship during the series production/maintenance phase
- **Benefits:** Necessary elements for training on long-term software quality in the automotive industry have been developed

Solution

- The insights gained in the AQI projects on long-term software maintenance throughout the entire vehicle lifetime in 2023 and 2024 will be used to develop the training content.
- Experience from other AQI projects (e.g., training for digital quality managers) will also be used in the project.

Project results

- Detailed training content on the topic of long-term software maintenance throughout the entire vehicle lifetime (possibly in two stages: self-study program and training course)
- Target audience for the training courses: Employees in companies who are responsible for implementation (e.g., also in software development companies that do not work exclusively for the automotive industry à raising awareness of long-term quality).
- Input for VDA 2 and VDA-Group AK13 (A-SPICE))

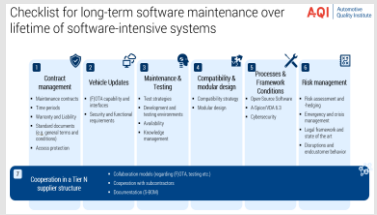
Overview

Project „training content for long-term software maintenance throughout the entire vehicle lifetime “

Project goal	Support the applicability and **implementation of the checklist contents** in companies and develop **the necessary elements for training in long-term software maintenance throughout the entire vehicle lifetime** → The **technical requirements** of the checklist should be mapped to **company organization and processes, responsibilities, and roles/employee profiles**
Planned project results	**Implementation concept for long-term software quality** in companies (“training”) → **Target audience:** Managers and employees who are responsible for **fulfilling (parts of) the checklist**
Note	This project does not involve the development of **didactic concepts** for teaching the content developed in training courses. The method of knowledge transfer is not part of the project.

Project details

Evaluation according to checklist

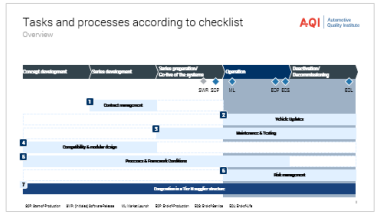


Checklist with 7 main categories and a total of 38 pages

All test points evaluated according to responsibility (RASI) and time classification

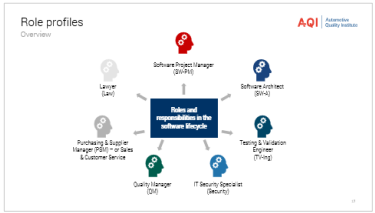
"Training content: long-term software maintenance throughout the entire vehicle lifetime " or implementation concept

Processes



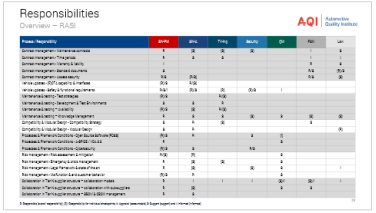
Is there a need to establish new or adapted processes within the company?

Role profiles



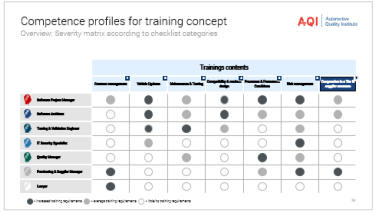
Which roles are involved? Where could which tasks best be anchored?

Responsibilities



What responsibilities are there for individual tasks (evaluation, e.g., using the RASI matrix)?

Training modules



Which training modules are required with which skills?

Results

Implementation concept (this document)

Enabling companies to fulfill the checklist and ensure long-term software maintenance throughout the entire vehicle lifetime

"Processes"

"Role profiles"

"Responsibilities"

and "training modules"

Agenda

AQI Automotive Quality Institute

- Project description of the approach
- **Project contents**
  - **Processes**
  - Role profiles
  - Responsibilities
  - Training modules
- Checklist reference – Timeline and responsibilities (JURSI)

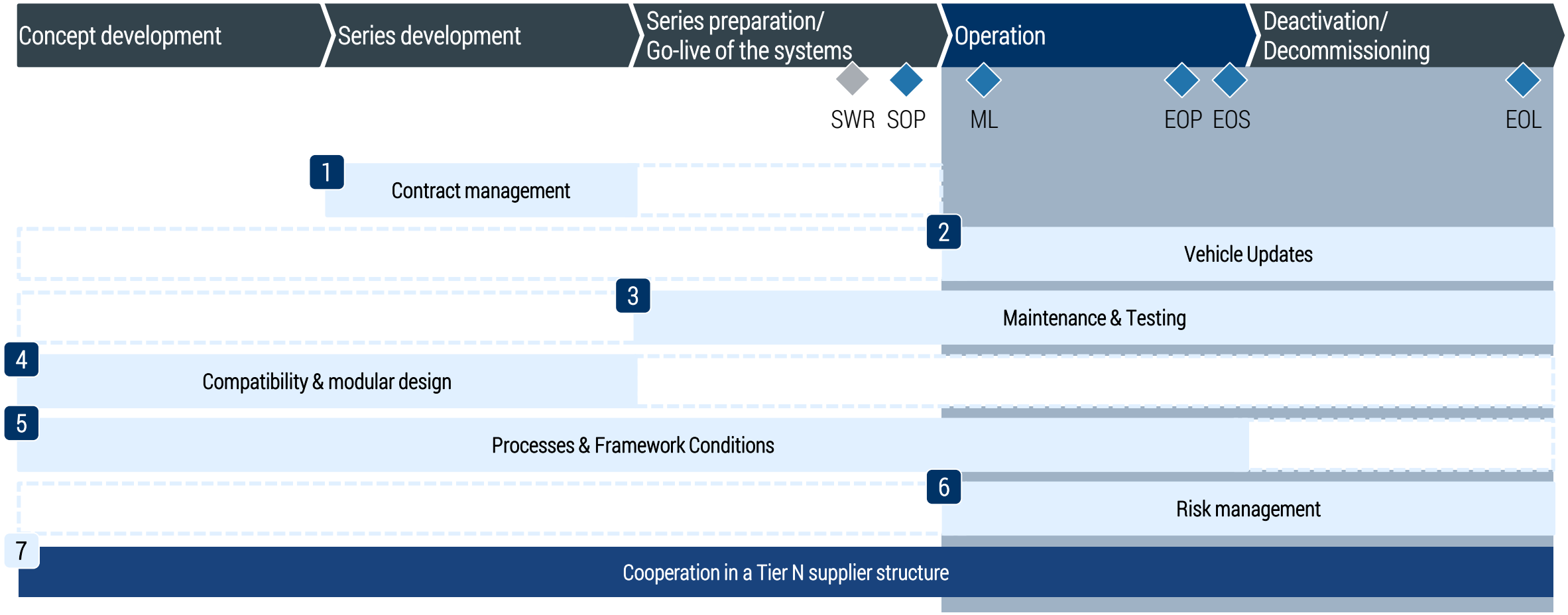
Processes

Objective

- Identification and definition of the **relevant processes** required to ensure long-term software quality.
- Ensuring that all necessary **technical, organizational, and regulatory processes** are in place.
- Adaptation of existing and implementation of new **processes for software maintenance, updates, testing, and cybersecurity.**
- Integration of the **checklist for long-term software maintenance throughout the entire vehicle lifetime.**
- Avoidance of risks through **clear process flows for e.g. (F)OTA updates and risk management.**

Tasks and processes according to checklist

Overview



SOP: Start-of-Production SWR: (Initiales) Software-Release ML: Market Launch EOP: End-of-Production EOS: End-of-Service EOL: End-of-Life

Core tasks/process elements according to checklist

1. Contract management

1.1 Maintenance contracts

- **Requirement definition:** Collection of requirements from development, testing, and after-sales
- **Contract creation:** Drafting of maintenance contracts (including update scope, response times, KPIs
- **Negotiation & conclusion:** Coordination with Tier 1, legal department, purchasing
- **Review & approval:** Legal review and QM approval
- **Implementation:** Integration into project and supplier structure
- **Regular review:** Regular updates in line with technical/regulatory status

1.2 Time periods

- **Define lifecycle model:** SOP, EOP, EOS, EOL
- **Set support periods:** minimum terms for maintenance and security updates
- **Contractual anchoring:** fixing the periods in the contract
- **Plan maintenance cycles and renewals:** option clauses and change management
- **Establish lifecycle documentation:** integration into project and QMS structure

1.3 Warranty and Liability

- **Analyze liability risks:** Legal & technical scenarios
- **Regulate liability frameworks:** Caps, recourse, warranty
- **Clarify responsibilities:** Technical and legal along the supply chain
- **Define fallbacks:** Protection through escrow, SLAs, insurance
- **Create communication & awareness:** Clear presentation internally and externally

1.4 Standard documents (e.g. general terms and conditions)

- **Identify contract templates:** Select relevant templates (terms and conditions, SLAs, MSAs)
- **Adapt to software context:** Integrate checklist requirements
- **Centralized management:** Use a contract management system
- **Establish version control and review processes:** Ensure that contracts are up to date and compliant

1.5 Access protection

- **Perform criticality assessment:** code, certificates, keys, documentation
- **Formulate contract clauses:** access rights, escrow, disclosure obligations
- **Document access paths:** Who is allowed to do what, when, and how?
- **Prepare crisis mechanisms:** For insolvency, technical failure, supplier withdrawal

Core tasks/process elements according to checklist

2. Vehicle Updates

2.1 (F)OTA capability and interfaces	2.2 Security and functional requirements	Update process management	Responsibility allocation & supplier integration
▪ **Define updateability:** Identify technical requirements for (F)OTA (memory, bandwidth, control units) ▪ **Adapt system architecture:** Integrate update components and modular software containers ▪ **Standardize interfaces:** Define communication interfaces between backend, gateway, and control units ▪ **Establish technical approval processes:** Release management for OTA-enabled components and systems ▪ **Integrate testing and validation:** Set up fallback mechanisms, test environments, and security checks	▪ **Define security requirements:** Secure communication ▪ **Verify update content:** Structured checks for integrity, authenticity, compatibility ▪ **Clarify roles and responsibilities:** Who is authorized to sign, approve, and distribute releases? ▪ **Develop update policies:** Which updates are rolled out when and how? ▪ **Integrate regulatory requirements:** UNECE R156-compliant update approvals & change logs	▪ **Define update cycles:** Strategic planning (e.g., monthly, quarterly, event-based) ▪ **Plan and implement rollout:** Systematic rollout by region, model series, or security level ▪ **Ensure compatibility:** Ensure backward/forward compatibility through testing and migration strategies ▪ **Documentation and reporting:** Who has which version on which vehicle and when? ▪ **Establish feedback mechanisms:** Detect errors in the field and trace them back to their source	▪ **Define responsibilities:** OEM/Tier 1/Tier 2 responsibilities for update delivery, validation, and support ▪ **Add contract clauses:** Binding commitments to long-term update capability and maintenance ▪ **Require security commitments:** Commitment to regular security patches and response times ▪ **Require update documentation:** Standardized logs of delivered software versions and approvals ▪ **Ensure auditability:** Prepare processes, tools, and evidence for audits and access by authorities

Core tasks/process elements according to checklist

3. Maintenance & Testing

AQI | Automotive Quality Institute

3.1 Test strategies

- **Develop test concepts:** Derive from architecture, security requirements, and update cycles
- **Define test types:** Regression tests, compatibility tests, endurance tests
- **Plan degree of automation:** Tool-supported tests and continuous integration/continuous delivery
- **Determine coverage and depth:** Which components, variants, and releases will be tested and how?
- **Integration with release and update process:** Tests as release criteria and fallback strategy

3.2 Development and testing environments

- **Specify test environments:** Requirements for hardware, virtualization, databases
- **Ensure availability:** Infrastructure throughout the entire project and maintenance period
- **Define access and user concepts:** Rights, logging, approvals
- **Synchronization with development:** Environment maintenance parallel to product maturity
- **Archiving and reproducibility strategies:** Restoration of test environments even years later

3.3 Availability

- **Plan availability strategies:** Ensure tools, platforms, and resources are in place
- **Secure availability through contracts:** Test infrastructure and support guaranteed by suppliers
- **Set up redundancy and backup systems:** Minimization of test failures
- **Generate and maintain long-term test data:** e.g., anonymized field feedback
- **Implement monitoring and KPIs:** Measurement of usage and maturity of the test infrastructure

3.4 Knowledge management

- **Build up knowledge base:** Document test cases, coverage strategies, lessons learned
- **Enable role-based training:** Training plans for testers, DevOps, quality
- **Maintain versioning and history:** Ensure documentation requirements and reproducibility
- **Structure handover:** Knowledge transfer during team changes or EOL transitions
- **Maintain tool and process documentation:** Ensure comprehensibility and applicability in the long term

Core tasks/process elements according to checklist

4. Compatibility & modular design

4.1 Compatibility strategy	4.2 Modular design	Reuse & variant management
▪ **Define compatibility goals:** Backward/forward compatibility, platform strategy ▪ **Analyze dependencies:** Identify critical components and interfaces ▪ **Build a compatibility matrix:** Which combinations have been tested and approved? ▪ **Develop test concepts:** Special tests for compatibility & migration scenarios ▪ **Ensure maintenance throughout the life cycle:** Tracking of variants & updates	▪ **Plan modularization:** Divide into clearly defined, maintainable software modules ▪ **Establish interface standardization:** Clean, documented APIs with stable contracts ▪ **Manage versioning & dependencies:** Structured handling of release statuses & component assignment ▪ **Ensure maintainability in the design**: Consider encapsulation, interchangeability, and reusability early on ▪ **Introduce documentation and review processes:** Architecture approvals and change management	▪ **Define reuse strategies:** Reusable modules across projects and series ▪ **Establish configuration management:** variant logic, feature sets, and parameterization ▪ **Introduce tool-supported traceability:** Systematically map variants and release statuses ▪ **Promote standardization:** Reduce special solutions to simplify maintenance and updates ▪ **Clarify organizational responsibilities:** Who maintains, who decides, who approves?

Core tasks/process elements according to checklist

5. Processes & Framework Conditions

5.1 Open Source Software (FOSS)

- **Define FOSS strategy:** Which OSS components may be used and how?
- **Establish license review & approval process:** License compatibility, prohibitions, obligations
- **Maintain SBOM documentation:** Component directory, origin, version, license
- **Integrate compliance toolchain:** e.g., OSS Review Toolkit
- **Include obligations in contracts:** disclosure obligations, support, updates, audit rights
- **Conduct training and awareness measures:** technical and legal for developers and purchasing

5.2 A-SPICE / VDA 6.3

- **Implement processes in accordance with A-SPICE:** planning, development, testing, approval, and support
- **Apply maturity model:** Levels 1–5 for continuous process improvement
- **Define auditors and roles:** project QM, process owner, supplier interface
- **Conduct supplier audits:** evaluation of software development quality at Tier 1/Tier 2
- **Ensure links to other standards:** ISO 26262, ISO 21434, UNECE, etc.

5.3 Cybersecurity

- **Define and track security requirements:** From architecture, TARA, risk analysis
- **Embed security by design:** Early involvement in concept and development
- **Operate a cybersecurity management system (CSMS):** UNECE R155 compliant
- **Document security evidence:** Approvals, patches, vulnerability management
- **Establish incident response processes:** Detection, response, reporting

Core tasks/process elements according to checklist

6. Risk management

6.1 Risk assessment and -hedging	6.2 Emergency and crisis management	6.3 Legal framework and state of the art	6.4 Disruptions and endcustomer behavior
▪ **Define risk categories:** functional, technical, operational, legal, organizational ▪ **Carry out risk identification:** e.g. using FMEA, TARA, expert workshops ▪ **Assessment & prioritization:** Probability of occurrence × impact, maturity level, risk indicators ▪ **Derive mitigation measures:** Redundancies, tests, contract clauses, monitoring ▪ **Establish risk review & approval processes:** Regular reassessment & status review	▪ **Define emergency processes:** Procedures for security breaches, update errors, incompatibility ▪ **Define roles and escalation chains:** Who decides, who informs, who acts? ▪ **Prepare communication plans:** internal, suppliers, customers, authorities ▪ **Conduct crisis simulations:** preparation for zero-day, OTA failure, mass recalls ▪ **Embed lessons learned:** derive systematic improvements after incidents	▪ Identify **legal minimum requirements:** product safety law, product liability, ISO 21434, UNECE R155/R156 ▪ **Define and monitor the "state of the art":** Industry and technology status at the relevant point in time ▪ **Regular legal assessment and documentation:** Internal coordination with legal, QM, and security departments ▪ **Integration into development and contracts:** Operationalize and secure requirements ▪ **Ensure auditability:** Evidence, risk documentation, change logs	▪ **Analyze external factors**: Network availability, customer usage, regional regulations ▪ **Simulate end customer scenarios:** Update interruptions, operating errors, delayed usage ▪ **Plan risk buffers and fallbacks:** retry strategies, service concepts ▪ **Develop communication strategies:** transparency toward customers regarding security-related changes ▪ **Establish field monitoring:** early detection and response to usage patterns

Core tasks/process elements according to checklist

7. Cooperation in a Tier N supplier structure

AQI | Automotive Quality Institute

7.1 Collaboration models (regarding (F)OTA, testing etc)

- **Define cooperation models:** direct control vs. cascade model, delineation of responsibilities
- **Establish communication interfaces:** technical and organizational contact persons for each tier
- **Pass on requirements along the chain:** ensure transparency – no loss of information
- **Introduce synchronization routines:** regular meetings, joint review and coordination formats
- **Coordinate tool and data compatibility:** Compatible systems and formats (e.g., SBOM, test reports)

7.2 Cooperation with subcontractors

- **Contractual protection beyond Tier 1:** "Pass-through clauses," transparency obligations
- **Clarify responsibilities:** Who is responsible for what in the supply chain (RASI)?
- **Conduct risk analysis in the chain:** evaluate technical and organizational risks posed by sub-suppliers
- **Define approval criteria for each tier:** document and audit technical and formal requirements
- **Monitor the supply chain:** monitoring, escalation paths, and escalation levels

7.3 SBOM & CBOM Management

- **Define SBOM/CBOM requirements:** structure, content, format
- **Contractually regulate obligations for creation and maintenance:** frequency, timeliness, access rights
- **Introduce validation processes:** checking for completeness, timeliness, FOSS compliance
- **Pass SBOM along the supply chain:** OEM vs. Tier 1 vs. Tier 2 vs. suppliers
- **Track security updates and license evidence:** support for vulnerability management

Auditability & verification

- **Define audit obligations:** Who must provide which evidence and when?
- **Prepare audit documentation:** Checklists, templates, evidence of cooperation and quality
- **Integrate regulatory requirements:** UNECE R155/R156, product liability, IT security law
- **Introduce review mechanisms along the chain:** maturity assessment, QA measures
- **Establish training and awareness measures in the supply chain:** also for Tier 2/Tier 3

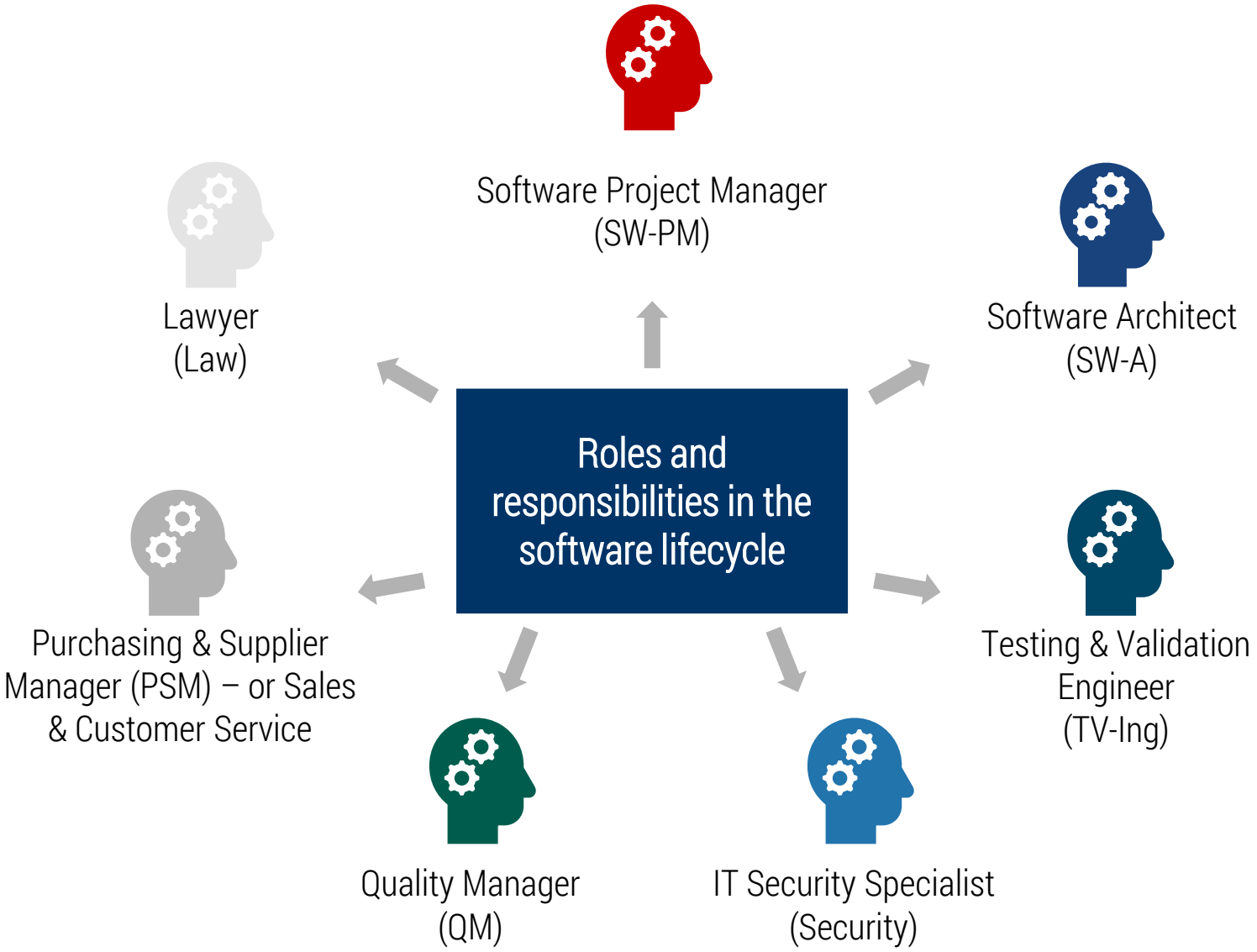
Agenda

AQI Automotive Quality Institute

- Project description of the approach
- **Project contents**
  - Processes
  - **Role profiles**
  - Responsibilities
  - Training modules
- Checklist reference – Timeline and responsibilities

Role profiles

Overview



Role profiles

Contents – Relevant role profiles & responsibilities

AQI Automotive Quality Institute

- **Software Project Manager:** Responsible for project-related coordination of all long-term software maintenance throughout the entire vehicle lifetime measures, integration of long-term quality targets and the checklist, ensuring deadlines, documentation, and cross-departmental implementation.
- **Software Architect:** Responsible for a modular, maintainable architecture and the long-term compatibility of software components and interfaces for long-term software maintenance throughout the entire vehicle lifetime.
- **Testing & Validation Engineer:** Plans and executes test strategies for compatibility, regression, and lifetime, and ensures the reusability of test cases (including long-term test strategies).
- **IT Security Specialist:** Assesses cybersecurity risks (TARA), update security, patch management, and auditability in accordance with ISO 21434 / UNECE R155, vulnerability management, and advises on secure architecture.
- **Quality Manager:** Ensures compliance with quality standards, responsible for auditability and quality assurance along the supply chain (supplier evaluation & quality assurance in software projects).
- **Purchasing & Supplier Manager/Sales:** Designs and negotiates contracts for maintenance, FOSS, manages Tier 1/Tier 2 with regard to software quality & contract compliance, supplier assurance with regard to maintenance, updates, FOSS.
- **Lawyer:** Reviews and drafts contracts with a focus on update obligations, availability, liability, open source compliance, and regulatory requirements (e.g., UNECE), regional regulations.

Role profiles

Overview and description of tasks

Software Project Manager	Responsible for project planning, control, and coordination of all activities related to long-term software quality: ▪ Integration of the checklist and all long-term quality goals into the project structure and milestones. ▪ Coordination of development, testing, security, and supplier activities. ▪ Risk management, documentation, and progress monitoring. ▪ Coordination with purchasing, architecture, testing, security, QM, and legal departments. ▪ Escalation and communication interface to overall project management.
Software Architect	Responsible for the design, documentation, and strategic development of the software architecture with a focus on modularity, compatibility, and updatability: ▪ Development of modular, maintainable architectures with a focus on updatability and compatibility. ▪ Definition of stable interfaces (APIs) and backward/forward compatibility. ▪ Integration of (F)OTA capability, security mechanisms, and versioning into the architecture design. ▪ Documentation of architecture decisions, release statuses, and variants. ▪ Close coordination with development, testing, security, purchasing, and project management.
Testing & Validation Engineer	Responsible for planning, implementing, and maintaining test strategies that make long-term software maintenance throughout the entire vehicle lifetime measurable and verifiable: ▪ Developing and executing regression and compatibility tests. ▪ Development of testable (F)OTA scenarios and fallback strategies. ▪ Maintenance of long-term test environments and tools. ▪ Ensuring traceability from requirements to test results. ▪ Support with audits, approvals, and field feedback.
IT security specialist	Responsible for the long-term security of software solutions, update processes, and supply chains: ▪ Conducting TARA (Threat and Risk Assessment) for new software components. ▪ Embedding security requirements in architecture, maintenance, and testing. ▪ Developing and maintaining methodologies to ensure IT security. ▪ Responding to vulnerabilities in the field (incident response). ▪ Supporting security audits, documentation requirements, and reporting.
Quality Manager	Controls and monitors process and quality assurance throughout the entire software life cycle: ▪ Implementation and monitoring of quality standards. ▪ Evaluation of suppliers with regard to software quality and compliance. ▪ Process approvals, review of maturity levels and escalation capabilities. ▪ Ensuring documentation requirements (checklists, evidence, audit documentation) ▪ Coordination of the internal “long-term software maintenance board“
Purchasing & Supplier Manager/Sales	Central interface for contractual and procedural safeguarding of requirements along the supply chain: ▪ Drafting and negotiating contracts regarding update obligations, maintenance, and support. ▪ Incorporating FOSS/open source compliance clauses into supplier contracts. ▪ Controlling and evaluating Tier 1/Tier 2 regarding long-term software maintenance throughout the entire vehicle lifetime. ▪ Conducting supplier audits and verification tests. ▪ Collaborating with legal, architecture, QM, and security departments in supplier selection.
Lawyer	Legally responsible for the legally compliant design and safeguarding of all long-term software maintenance throughout the entire vehicle lifetime -related obligations: ▪ Reviewing and helping to draft contracts for maintenance, updates, and availability. ▪ Integrating regulatory requirements such as UNECE R155/R156, ISO 21434, and regional differences. ▪ Assessment of license risks (e.g., open source GPL), product liability, and recourse scenarios. ▪ Support in escalations and crisis/incident management. ▪ Collaboration with purchasing, QM, architecture, PM, and IT security.

Profile

Software Project Manager (SW-PM)

AQI | Automotive Quality Institute

Function of the role

- Responsible for planning, managing, and implementing software-intensive projects.
- Central interface between technology, purchasing, legal, quality, and external partners.
- Ensuring the integration of long-term software maintenance throughout the entire vehicle lifetime aspects throughout the entire project life cycle.

Key tasks

- Project planning, milestones, resource management
- Integration of Long-term software maintenance checklist into all project phases
- Control of updates, risk and change management
- Communication interface & escalation coordination
- Interface to purchasing, IT security, testing, legal, and after-sales

Competence profile

- Project management: Classic & agile PM, resource planning, milestone tracking
- Technical understanding: Architecture, modularization, (F)OTA capability, basic understanding of testing
- Communication & leadership: Stakeholder coordination, moderation, reporting
- Regulatory & standards: A-SPICE, ISO 21434, UNECE R155/156
- Risk management: Assessment & control of technical and organizational risks
- Contract understanding: Basics of maintenance contracts, warranty, delivery obligations
- Change & configuration: Handling software changes, release management
- Quality understanding: Anchoring quality assurance measures in the project

Checklist reference – Responsibilities

1. Contract management: maintenance contracts, time frames, standard documents
2. Vehicle updates: (F)OTA capability, safety requirements
3. Maintenance & testing: development environments, availability, test strategies
4. Compatibility & modular design: compatibility strategy
5. Risk management: Crisis management, legal framework
6. Processes & framework conditions: A-SPICE, FOSS, cybersecurity
7. Cooperation Tier N structure: Collaboration models, SBOM management

Profile

Software Architect (SW-A)

AQI Automotive Quality Institute

Function of the role

- Conceptualization and design of modular, maintainable software architectures
- Ensuring compatibility, updatability, and maintainability throughout the entire life cycle
- Integration of technical requirements for long-term software quality into the architecture strategy

Key tasks

- Architectural decisions, technology selection, interface definition
- Technical coordination with development, testing, IT security, and project management
- Documentation and maintenance of the architecture throughout its lifecycle
- Compliance with security, maintenance, and EOL requirements in the architecture

Competence profile

- Software architecture: Modularization, design patterns, architecture standards
- Compatibility management: Strategies for backward/forward compatibility
- API and interface design: Design of maintenance-friendly, clearly documented interfaces
- Update & lifecycle strategy: Consideration of EOL, (F)OTA & versioning in the architecture
- Cybersecurity integration: Security architecture, threat modeling, ISO 21434Open source & compliance: Consideration of FOSS, SBOM, licensing requirements
- Documentation & modeling: Use of tools & standards for structured architecture maintenance
- Communication & moderation: Collaboration with technical and non-technical stakeholders

Checklist reference – Responsibilities

2. Fahrzeug-Updates: (F)OTA-Schnittstellen, Sicherheitsanforderungen

3. Wartung & Testing: Teststrategien unterstützen durch architekturelle Entscheidungen

4. Kompatibilität & Modulare Bauweise: Kompatibilitätsstrategie, Modularer Aufbau

5. Risikomanagement: Technikfolgenabschätzung, Architektur-Risikobewertung

6. Prozesse & Rahmenbedingungen: FOSS-Strategie, Integration von Cybersecurity in die Architektur

Profile

Testing & Validation Engineer (TV-Ing)

AQI Automotive Quality Institute

Function of the role

- Planning, executing, and evaluating software tests to ensure long-term software maintenance throughout the entire vehicle lifetime
- Responsibility for test coverage of updateability, compatibility, maintainability, and security requirements
- Close collaboration with development, architecture, and quality management to verify compliance with specifications and requirements

Key tasks

- Development of test concepts and strategies, including long-term aspects
- Setup and maintenance of test environments, regression test chains, and validation tools
- Validation of (F)OTA functionalities, compatibility, backward/forward integration
- Error documentation, traceability, and test reporting
- Support with audits and release decisions (e.g., SOP, releases, maintenance updates)

Competence profile

- Test strategy & planning: Development of targeted strategies for different types of testing
- Test automation: Knowledge of test frameworks, scripting, and tools
- Compatibility testing: Planning of cross-version, cross-platform, and cross-component tests
- (F)OTA test methodology: Testing update cycles, fallback mechanisms, validation of security patches
- Traceability & documentation: Ensuring traceability to requirements & test cases
- Long-term testing & EOL verification: Testing maintainability and performance over the entire service life
- Tool expertise: e.g., Jenkins, Python, Vector Tools, CANoe, Git
- Communication: Coordination with development, architecture, quality, and project management

Checklist reference – Responsibilities

2. Vehicle updates: Validation of updateability, safety and functional testing
3. Maintenance & testing: Test strategies, test environments, availability
4. Compatibility & modular design: Backward/forward compatibility testing
5. Risk management: Error analysis, test coverage of critical functions
6. Processes & framework conditions: Evidence for A-SPICE, audit preparation, SBOM validation

Profile

IT Security Specialist (Security)

AQI Automotive Quality Institute

Function of the role

- Responsibility for the cybersecurity of software-intensive systems throughout the entire product lifecycle
- Assessment and implementation of security requirements (e.g., according to ISO 21434, UNECE R155/156)
- Support in ensuring protective measures that are also effective during updates, maintenance, and in the EOL state

Key tasks

- Performing/maintaining threat and risk analyses (TARA)
- Developing and validating security concepts and architectures
- Defining requirements for cryptographic components, secure boot, and secure updates
- Reviewing and documenting security-related functions and safeguards
- Advising other departments (architecture, testing, purchasing, legal) on security issues
- Providing support in the event of security incidents and incident management

Competence profile

- Cybersecurity standards: ISO 21434, UNECE R155/156, NIST, BSI basic protection
- TARA methodology: Implementation and maintenance of threat and risk assessments
- Security by design: Integration of security aspects into architecture and development process
- Update security: Cryptographically secured (F)OTA processes, key and certificate management
- Incident response: Analysis, coordination, and escalation in the event of security incidents
- Tool expertise: e.g., Security Analyzer, TARA Tools, penetration testing tools
- Consulting and interface work: Communication with PM, testing, legal, architecture, purchasing

Checklist reference – Responsibilities

1. Contract management: Access security requirements and security clauses in the contract
2. Vehicle updates: Security requirements, secure updates, certificate management
3. Maintenance & testing: Securing maintenance access, security validation
5. Risk management: Threat analyses, incident handling, emergency management
6. Processes & framework conditions: Cybersecurity requirements (ISO 21434, UNECE R155), security concepts
7. Tier N cooperation: Securing third-party software, risk analysis in the supply chain

Profile

Quality Manager (QM)

AQI Automotive Quality Institute

Function of the role

- Ensuring compliance with all quality-related processes, norms, and standards throughout the life cycle of software-intensive systems
- Responsibility for implementing and monitoring quality assurance measures with a focus on long-term availability and maintainability
- Supporting internal and external audits and continuously improving quality-related processes

Key tasks

- Development, maintenance, and monitoring of quality-related processes (e.g., A-SPICE, VDA 6.3)
- Supporting specialist departments in the correct implementation of quality requirements
- Traceability and consistency of software quality evidence (e.g., testing, review, audit)
- Auditing suppliers with regard to software quality and long-term capability
- Training teams in quality standards and processes
- Error analysis and derivation of systematic improvement measures

Competence profile

- Quality standards & norms: A-SPICE, ISO 9001, VDA 6.3, ISO 26262 (if applicable), ISO 21434
- Process management: Definition, monitoring, and improvement of quality assurance processes
- Audit expertise: Conducting internal and external audits, supplier audits
- Evaluation of long-term software maintenance: Analysis of maintainability, compatibility, and EOL concepts
- Understanding of software quality: Evaluation of technical measures, test coverage, updateability
- Communication & assertiveness: Mediation between technology, management, and suppliers
- Tool expertise: e.g., QMS systems, DOORS, APIS IQ, audit software

Checklist reference – Responsibilities

1. Contract management: Ensuring quality-relevant contract components
2. Vehicle updates: Verification of updateability
3. Maintenance & testing: Knowledge management, test strategies, documentation
4. Compatibility & modular design: Test and regression coverage
5. Risk management: Quality assurance of escalation and emergency management
6. Processes & framework conditions: A-SPICE, VDA 6.3, quality processes and process standards
7. Tier N cooperation: Review of SBOM/CBOM, supplier audits

Profile

Purchasing & Supplier Manager (PSM) – or Sales & Customer Service

AQI Automotive Quality Institute

Function of the role

- Responsibility for contract drafting and supplier management in the area of software-intensive systems
- Ensuring that suppliers fulfill their obligations with regard to software maintenance, updates, compatibility, and cybersecurity
- Managing compliance with long-term software maintenance throughout the entire vehicle lifetime requirements through contractual and strategic measures

Key tasks

- Drafting and negotiating contracts, including maintenance, update, and security clauses
- Evaluating and selecting software suppliers (Tier 1/Tier 2)
- Ensuring that requirements such as FOSS compliance are contractually regulated
- Monitoring supplier performance with regard to software quality and availability
- Close cooperation with architecture, quality management, IT security, and legal departments
- Support with audits, escalations, and contract renegotiations

Competence profile

- Contract drafting: Drafting software maintenance, license, and service agreements
- Supplier management: Monitoring adherence to deadlines, maintenance obligations, and quality targets
- FOSS clauses: Integrating compliance requirements into contracts
- Risk management: Assessment and mitigation of potential delivery failures or compliance risks
- Basic technical understanding: Overview of update processes, software components, and security requirements
- Communication and negotiation: Interdisciplinary coordination, contract negotiation, escalation management
- Cooperation with legal/QM: Ensuring technical and legal coverage of delivery obligations

Checklist reference – Responsibilities

1. Contract management: maintenance contracts, time frames, standard documents, access security
2. Vehicle updates: contractual assurance of (F)OTA update capability & long-term maintenance
5. Risk management: Securing update, security, and maintenance obligations
6. Processes and framework conditions: Open source compliance, availability assurance in the supply chain
7. Tier N collaboration: Collaboration models, supplier management, SBOM/CBOM agreements

Profile

Lawyer (Law)

Function of the role

- Legal support for all activities related to software contracts, liability, warranty, and regulatory requirements
- Ensuring that software maintenance, updates, open source, and cybersecurity are legally compliant
- Supporting other departments in the legally compliant implementation of the checklist for long-term software maintenance throughout the entire vehicle lifetime

Key tasks

- Review and drafting of contract clauses on software maintenance, update obligations, and EOL availability
- Advice on liability issues relating to security vulnerabilities, update failures, or incompatibilities
- Assessment and documentation of risks in connection with FOSS, license violations, data protection
- Support in contract negotiations with Tier 1/Tier 2 in the software context
- Close cooperation with purchasing, architecture, IT security, and QM
- Monitoring of regulatory developments, including in specific regions (e.g., UNECE R155/156, product liability EU/DE)

Competence profile

- Software contract law: Drafting and reviewing contracts for updates, maintenance, and availability
- Liability and warranty law: Risk analysis for errors, security vulnerabilities, and incompatibilities
- Open source compliance: License review (e.g., GPL, LGPL), risks associated with FOSS use, SBOM clauses
- Cybersecurity & data protection law: Requirements under ISO 21434, UNECE R155/156, GDPR, IT Security Act
- Regulatory: Review of regulatory differences in regions
- Basic technical understanding: Knowledge of relevant software processes, update cycles, component structure
- Negotiation & consulting: Support in contract negotiations & assistance to specialist departments
- Risk management & escalation: Legal assessment in the event of deviations, safeguards, escalation paths

Checklist reference – Responsibilities

1. Contract management: maintenance contracts, time frames, warranty, liability, standard documents

2. Vehicle updates: securing update obligations and responsibility in the event of errors

5. Risk management: Assessment of legal framework conditions, contingency plans, product liability

6. Processes & framework conditions: Open source compliance, licensing & data protection law

7. Tier N cooperation: FOSS risks in the supply chain

Agenda

AQI Automotive Quality Institute

- Project description of the approach
- **Project contents**
  - Processes
  - Role profiles
  - **Responsibilities**
  - Training modules
- Checklist reference – Timeline and responsibilities

Responsibilities

Objective

AQI Automotive Quality Institute

- **Clarification of roles and responsibilities** within the company and along the supply chain
- Definition of **who is responsible for which aspects of long-term software maintenance throughout the entire vehicle lifetime** (e.g., development, testing, maintenance, supplier management, cybersecurity, compliance)
- Ensuring a **clear communication and decision-making structure** to efficiently manage escalations, risks and security incidents
- **Integrating the long-term software maintenance throughout the entire vehicle lifetime checklist** into the company's **chain of responsibility**

Responsibilities

Overview – RASI

Process / Responsibility	SW-PM	SW-A	TV-Ing	Security	QM	PSM	Law
Contract management - Maintenance contracts	R	(S)	(S)	(S)		I	S
Contract management - Time periods	R	S	S			I	I
Contract management - Warranty & liability	I					R	S
Contract management - Standard documents	S					R/S	(R)/S
Contract management - Access security	R/S	(R/S)				R/S	(S)
Vehicle updates - (F)OTA capability & interfaces	(R)/S	R/(S)					
Vehicle updates - Safety & functional requirements	R/S/I	(R)/S	(R)	(R)/S	I		
Maintenance & testing - Test strategies	(R)/S		R/(S)				
Maintenance & testing - Development & Test Environments	S	S	R				
Maintenance & testing – Availability	(R)/S	(S)	R/(S)				
Maintenance & testing – Knowledge Management	R	S	S	(S)	S	(S)	(S)
Compatibility & Modular Design - Compatibility Strategy	S	R	(S)			S	
Compatibility & Modular Design - Modular Design	S	R					(R)
Processes & Framework Conditions - Open Source Software (FOSS)	(R)/S	R		S	(I)		
Processes & Framework Conditions - A-SPICE / VDA 6.3	R				S		
Processes & Framework Conditions - Cybersecurity	(R)/S	S		R/S			
Risk management - Risk assessment & mitigation	R/(S)	(R)			S		
Risk management - Emergency & crisis management	R	(S)	(S)		S		
Risk management - Legal framework & state of the art	R	(S)		(S)	S		I
Risk management - Malfunction & end customer behavior	(R)/S	R			S		
Collaboration in Tier N supplier structure – collaboration models	R	I	I	I	(S)/I	(S)/I	I
Collaboration in Tier N supplier structure – collaboration with sub-suppliers	R	(S)			S	S	
Collaboration in Tier N supplier structure – SBOM & CBOM management	R	S					

R: Responsible (overall responsibility), (R): Responsibility for individual checkpoints, A: Approval (accountable), S: Support (support) and I: Informed (informed)

Responsibilities

Possible functions and tasks within the company (examples of committees)

Function: Strategic decisions, escalation, and reputation protection
Tasks:
- Approval of fundamental contract and delivery strategies (e.g., maintenance models)
- Decision-making on system-relevant risks (liability, regulatory issues, brand image)
- Resource allocation & strategic decision-making (e.g., "updatability over 15 years")

Function: Technical and functional decision-making authority for all software issues
Tasks:
- Architecture approvals, modularization strategies
- Decisions on platform strategy, variants, updateability
- Escalation of technical conflicts or delivery problems

Function: Overall responsibility for target achievement, resource management, and operational escalations for each project
Tasks:
- Decision-making on measures to be taken in the event of risks or target deviations
- Reconciliation with project schedule and supplier status
- Interface to other control loops and stakeholders

Function: Implementation and coordination of all operational activities to ensure long-term quality for each project
Tasks:
- Checklist integration and cross-departmental coordination
- Review of architecture, testing, security, and contracts
- Documentation, verification, and audit preparation

Responsibilities

Collaboration with external parties: OEM – Tier 1 – Tier 2 – Third-party providers

OEM & Tier-1	▪ OEM defines the requirements for long-term availability, compatibility, and updateability ▪ Tier 1 is responsible for implementation and verification (e.g., SBOM, updateability, testing) ▪ Cooperation takes place through: – Joint architecture coordination – Standardized contract modules (e.g., maintenance agreements, FOSS specifications) – Approvals and reviews (design, testing, security, release)
Tier-1 & Tier-2	▪ Tier 1 must pass on OEM requirements contractually and technically (“flow-down”) ▪ Tier 2 supplies components or software modules, e.g., libraries, middleware, algorithms ▪ Expected: – Disclosure of components (CBOM, SBOM) – Responsiveness to vulnerabilities – Availability beyond the project lifetime
Cooperation with third-party providers/service providers	▪ E.g. for security tools, test systems, OTA platforms, or open source services ▪ Requirements – Contractually secure access protection, compatibility, and auditability – Explicitly define availability and maintenance obligations – Regular security and quality certifications

Agenda

AQI Automotive Quality Institute

- Project description of the approach
- **Project contents**
  - Processes
  - Role profiles
  - Responsibilities
  - **Training modules**
- Checklist reference – Timeline and responsibilities

Role profiles including training concept

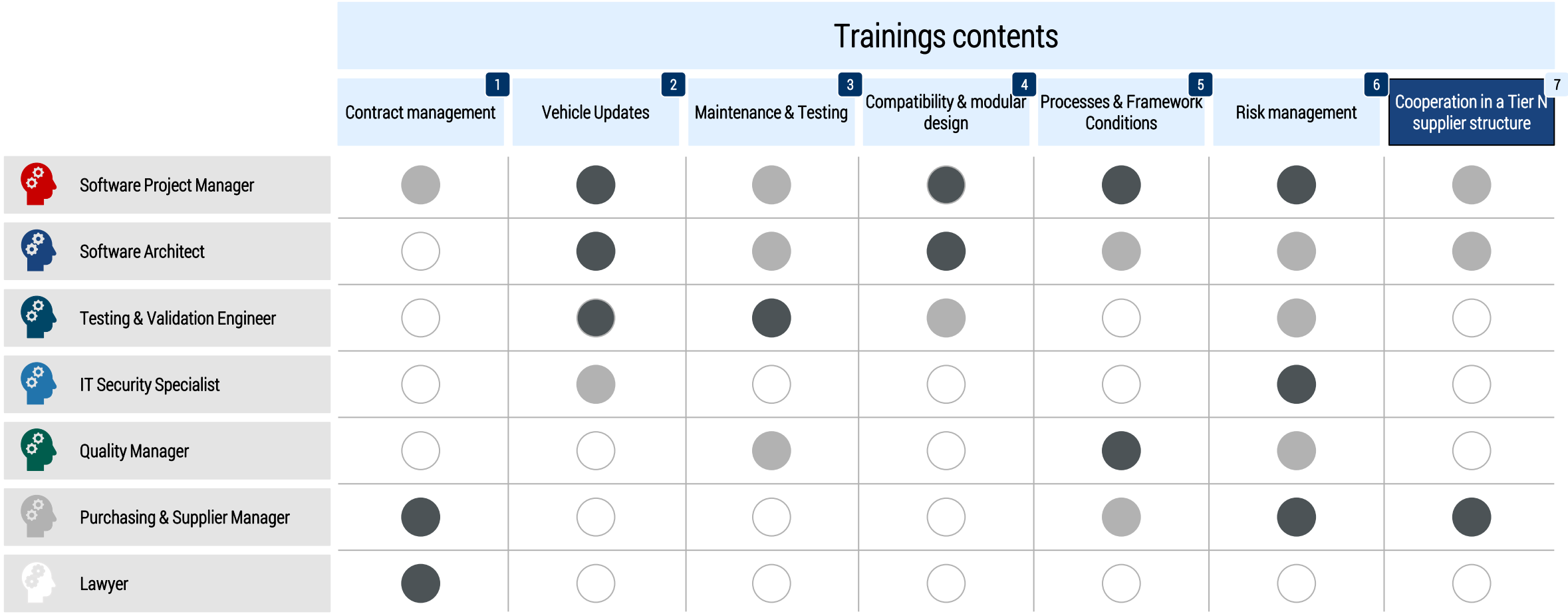
Objective

- Defining the **necessary roles and qualifications** to ensure long-term software maintenance throughout the entire vehicle lifetime
- Assigning the **processes from the checklist** to the corresponding **role profiles**
- Developing a **targeted training concept** to anchor knowledge and skills in the company
- Ensuring that **all relevant departments and stakeholders** have the necessary expertise to implement long-term software maintenance throughout the entire vehicle lifetime in their respective roles

Competence profiles for training concept

Overview: Severity matrix according to checklist categories

AQI | Automotive Quality Institute



Competence/Training module

1 Contract management

- Basics of maintenance and update contracts
- Design of service level agreements (SLA)
- Definition of terms and renewal mechanisms
- Regulation of warranty and liability for software defects
- Flow-down of OEM requirements to suppliers
- Securing long-term access options (e.g., escrow)
- Consideration of FOSS compliance in the contract
- Handling of standard contract clauses (e.g., DIN, VDA, UNECE)
- Coordination of technical requirements with legal/purchasing
- Negotiation techniques & risk distribution in software projects
- Legally compliant contract drafting and handling of performance disruptions in international contracts
- (Standard) documentation of protocols and contracts
- Performance specification - requirements/specifications

Competence/Training module

2 Vehicle Updates

- (F)-OTA architectures
- Concepts relating to SDV (Software Defined Vehicle) High-level architecture
- SOTA vs. FOTA, OTA approaches, update scenarios, update campaigns
- Update strategies and methods for control units
- Management of (F)-OTA updates, UNECE R 156, ISO 24089
- Interfaces, update processes, documentation requirements
- Fail-safe strategies
- Cloud technology and services
- Backend systems
- OTA cybersecurity including data protection (see also category “Processes & Framework Conditions,” cluster “Cybersecurity”)
- Secure bootloaders and managers
- (F)-OTA testing
- Network protocols such as MQTT
- Transport and diagnostic communication protocols such as CAN-TP, UDS, DoIP

Competence/Training module

3 Maintenance & Testing

- Development of test strategies for long-term software maintenance
- Verification measures and techniques
- Validation measures and techniques
- Use of regression tests and compatibility tests
- Setup of long-term maintainable test environments
- Testing of software over the entire vehicle life cycle
- Application of traceability methods (requirement → test → release)
- Use of CI/CD for test automation
- Long-term handling of hardware-in-the-loop (HiL) and simulation
- Version and variant testing (e.g., for different vehicle configurations)
- SBOM management

Competence/Training module

4 Compatibility & modular design

- Concepts and strategies for downward and upward compatibility
- Development of compatibility matrices
- Modularization of software architectures
- Interface management (internal/external APIs)
- Handling platform and hardware variants
- SBOM management
- Strategies for reusing existing modules
- Maintainability of software across multiple generations
- Analyzing dependencies and interoperability
- Integration of security mechanisms into modular architectures
- Evaluating the impact of changes on compatibility

Competence/Training module

5 Processes & Framework Conditions

- Fundamentals of FOSS management and license verification (e.g., FOSS license types and resulting legal framework)
- SBOM management
- Relevant norms and standards (including A-SPICE, ISO 21434, UNECE R155 / R156, etc.)
- Verification and documentation in the product lifecycle
- Traceability and change tracking across software versions
- Process integration of suppliers (e.g., release approvals)
- Tools for configuration and release control
- Role-based process responsibility (e.g., RASI, process owner)

Competence/Training module

6 Risk management

- Introduction to technical and organizational risk types
- Risk strategies for dealing with risks and their implementation
- Application of TARA (total risk assessment = assessment of risks in terms of probability and consequence, focus on probable and consequential risks) in the software context
- Risk assessment for maintenance and update processes
- Dealing with security-critical dependencies (e.g., third-party code)
- Inclusion of legal risks (product liability, update obligations)
- Planning and documentation of emergency measures
- Establishment of an early warning system (technical & organizational)
- Risk analyses in the supply chain (Tier N)Dealing with vulnerability management (CVE, security advisories)
- Integration of risk management in project and product development, including IT systems

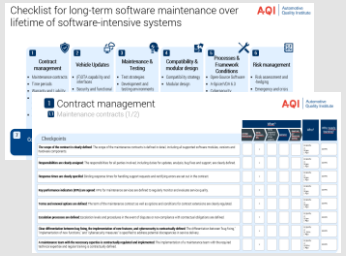
Competence/Training module

7 Cooperation in a Tier N supplier structure

- Establishment of transparent communication structures
- Communication of requirements and SBOM management along the chain
- Contract drafting with suppliers regarding update and maintenance obligations
- Documentation obligations and verification for Tier ½
- Standardization of interfaces and handover documents
- Management of third-party providers and service providers
- Training and awareness among external partners
- Ensuring auditability in the supply chain
- Escalation and reporting chains in the event of errors
- Sharing lessons learned and quality agreements

Summary and conclusion

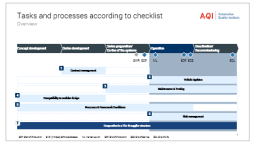
Possible focus and content to ensure "long-term software quality" in companies



Checklist with 7 main categories and a total of 166 checkpoints

All test points evaluated according to responsibility (RASI) and time classification

Processes

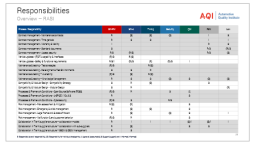


- Derivation of a process landscape to summarize the core tasks/process elements according to the checklist

Role profiles

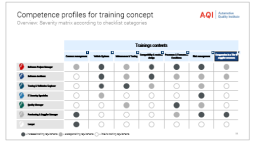
- Definition of a structure and organizational units involved in controlling long-term software maintenance throughout the entire vehicle lifetime

Responsibilities



- RACI matrix for assigning responsibilities across the seven checklist categories

Training modules



- Definition of seven roles, including core tasks and competencies
- Derivation of competency/training modules based on the categories in the checklist

Result

The concept for long-term software maintenance throughout the entire vehicle lifetime includes role-based anchoring, defined processes in line with regulatory requirements, binding responsibilities, and role-based training modules to ensure sustainable competence.

Guidance for companies on individual implementation

Agenda

AQI Automotive Quality Institute

Project description of the approach

Project contents

Checklist reference – Timeline and responsibilities

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)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
Responsibilities are clearly assigned: The responsibilities for all parties involved, including duties for updates, analysis, bug fixes and support, are clearly defined.		x				R: SW-PM A: S: Law I: PSM	SW-PM
Response times are clearly specifed: Binding response times for handling support requests and rectifying errors are set out in the contract.		x				R: SW-PM A: S: Law I: PSM	SW-PM
Key performance indicators (KPIs) are agreed: KPIs for maintenance services are defined to regularly monitor and evaluate service quality.		x				R: SW-PM A: S: Law I: PSM	SW-PM
Terms and renewal options are defined: The term of the maintenance contract as well as options and conditions for contract extensions are clearly regulated.		x				R: SW-PM A: S: Law I: PSM	SW-PM
Escalation processes are defined: Escalation levels and procedures in the event of disputes or non-compliance with contractual obligations are defined.		x				R: SW-PM A: S: Law I: PSM	SW-PM
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.		x				R: SW-PM A: S: : SW-A I: PSM	SW-PM
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.		x				R: SW-PM A: S: SW-A I: PSM	SW-PM

1 Contract management

1.1 Maintenance contracts (2/2)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
Cost structure is transparent: A transparent and comprehensible cost structure for all maintenance services, including regular updates and adjustments, has been created.		x				R: PSM A: SW-PM S: TV-Ing I:	PSM
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
Binding documentation requirements are defined: Binding requirements are defined to ensure traceability and transparency in the documentation of all maintenance work and changes		x				R: SW-PM A: S: TV-Ing I: PSM	SW-PM
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.		x				R: SW-PM A: S: TV-Ing I: Law	SW-PM

1 Contract management

1.2 Time periods

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
Liability periods are regulated across the entire supply chain: The liability periods are transparent, clearly regulated and contractually stipulated throughout the entire supply chain.		x				R: SW-PM A: S: Law I: PSM	SW-PM
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
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.		x				R: SW-PM A: S: : SW-A I: PSM	SW-PM

1 Contract management

1.3 Warranty and liability

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: Law I: PSM	PSM
Liability risks have been comprehensively analysed: All potential liability risks have been identified and considered in the contract to minimize unexpected costs.		x				R: PSM A: S: Law, SW-E I:SW-PM	PSM
Contractual penalties for non-performance are defined: Contractual penalties are provided for if the contractually stipulated guarantee or liability conditions are not met.		x				R: PSM A: Law S: I: SW-PM	PSM
Liability limits are coordinated with suppliers: The defined liability limits are consistent across the entire supply chain and harmonised with the suppliers.		x				R: PSM A: S: Law I: SW-PM	PSM
Recourse claims are clearly regulated: The conditions for recourse claims in the event of defects or damages are clearly defined and contractually stipulated.		x				R: Law A: S: SW-PM I: PSM	Law
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.		x				R: SW-PM, PSM A: S: PSM I:	SW-PM, PSM
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM

1 Contract management

1.4 Standard documents

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
Ensuring the use of standardised contract templates: All contracts and agreements are based on coherent, standardised document templates to ensure consistency and legal certainty.		x				R: Law A: S: PSM I: SW-PM	Law
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.		x				R: PSM, SW-PM A: S: I: Law	PSM, SW-PM
Consistency across the supply chain is ensured: The use of standard documents is enforced across the supply chain to ensure consistent terms and procedures.		x				R: PSM A: S: I: Law	PSM
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.		x				R: Law A: S: PSM I: SW-PM	Law
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.		x				R: PSM A: S: SW-PM I: Law	PSM
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.		x				R: PSM A: S: SW-PM I: Law	PSM

1 Contract management

1.5 Access protection (1/2)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: Law I: PSM	SW-PM
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.		x				R: PSM A: S: SW-PM I:	PSM
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.		x				R: PSM A: S: SW-PM I:	PSM
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.		x				R: SW-A A: S: SW-PM I:	SW-A
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.		x				R: SW-PM A: S: SW-A I: PSM	SW-PM
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.		x				R: PSM A: S: SW-PM I:	PSM
Regular reviews of escrow agreements is implemented: Escrow agreements are regularly reviewed and adjusted as necessary to ensure that they meet current requirements.		x				R: PSM A: S: Law I:	PSM
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.		x				R: SW-PM A: S: PSM, SW-A I:	SW-PM

1 Contract management

1.5 Access protection (2/2)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: SW-A I: PSM	SW-PM

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)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: LawPSM I:	SW-PM
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Interfaces are standardized: The interfaces for (F)OTA updates are coherent and standardised across projects for both the OEM and the supplier.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.		x	x			R: SW-PM A: S: SW-A I:	SW-PM
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.		x	x	x		R: SW-A A: S: SW-PM I:	SW-A
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.		x	x			R: SW-PM A: S: SW-A I:	SW-PM

2 Vehicle Updates

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

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.	x	x				R: SW-A A: S: I: SW-PM	SW-A
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.		x	x			R: TV-Ing A: S: SW-A I: SW-PM	TV-Ing

2 Vehicle Updates

2.2 Security and functional requirements (1/2)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.	x	x				R: SW-A A: S: Security I: SW-PM	SW-A
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.		x	x	x		R: Security A: S: SW-A I: SW-PM	Security
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.		x	x	x		R: SW-A A: S: SW-PM I:	SW-A
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.		x	x	x		R: TV-Ing A: S: SW-A I: SW-PM	TV-Ing
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.		x	x	x		R: Security A: S: SW-PM I:	Security
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.		x	x	x		R: Security A: S: SW-PM I:	Security
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.	x	x				R: SW-A A:Security S: SW-PM I: QM	SW-A
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.		x	x	x		R: Security A: S: SW-A I: QM	Security

2 Vehicle Updates

2.2 Security and functional requirements (2/2)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
Security protocols are continuously monitored: All security-relevant protocols and logs are continuously monitored in order to detect anomalies or security-critical events immediately.		x	x			R: SW-PM A: S: Security I:	SW-PM
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.	x	x	x	x		R: Security A: S: SW-PM, SW-A I: QM	Security

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)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x	x			R: TV-Ing A: S: I: SW-PM	TV-Ing
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.		x				R: SW-PM, PSM A: S: TV-Ing I:	SW-PM, PSM
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.			x			R: TV-Ing A: S: I: SW-PM	TV-Ing
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.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
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.			x	x		R: SW-PM A: S: TV-Ing I:	SW-PM
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.		x				R: SW-PM A: S: TV-Ing I:	SW-PM
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.		x	x	x		R: TV-Ing A: S: I: SW-PM	TV-Ing
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.			x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Maintenance & Testing

3.1 Test strategies (2/2)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.				x		R: TV-Ing A: S: SW-PM I:	TV-Ing
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.				x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Maintenance & Testing

3.2 Development and testing environments

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.	x	x	x	x		R: TV-Ing A: S: SW-A, SW-PM I:	TV-Ing
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.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
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.	x	x	x	x		R: TV-Ing A: S: SW-A, SW-PM I:	TV-Ing
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.		x	x	x		R: SW-PM A: S: TV-Ing I:	SW-PM
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.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
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.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Maintenance & Testing

3.3 Availabilities

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
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.	x	x	x	x		R: TV-Ing A: S: SW-PM, SW-A I:	TV-Ing
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.		x	x	x		R: SW-PM A: S: TV-Ing I:	SW-PM
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).		x	x			R: SW-PM A: S: TV-Ing I:	SW-PM
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.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Maintenance & Testing

3.4 Knowledge management

Automotive Quality Institute

Checkpoints

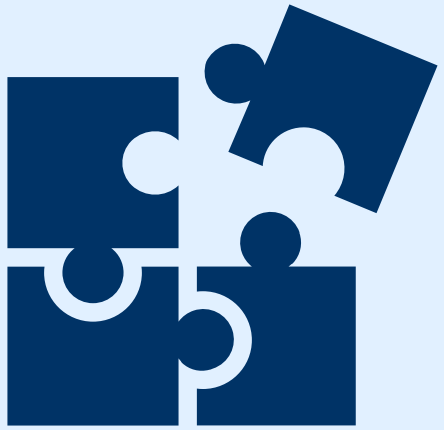
	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
Systematic documentation is implemented: All relevant information, processes and experiences are systematically documented and stored in a central knowledge management system to ensure access for everyone involved.		x	x	x		R: SW-PM A: S: SW-A I: Alle	SW-PM
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.		x	x	x		R: SW-PM A: S: SW-A I: Alle	SW-PM
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.	x	x	x	x	x	R: SW-PM A: S: Alle I: QM	SW-PM, R: Alle
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.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x		R: SW-PM A: S: Alle I:	SW-PM
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.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x		R: SW-PM A: S: TV-Ing I: QM	SW-PM

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

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.	x					R: SW-A A: S: SW-PM I:	SW-A
Backwards compatibility is ensured: Backward compatibility of software and hardware is strategically considered and implemented ensuring that new components remain compatible with older system.	x					R: SW-A A: S: SW-PM I:	vorgeschriebener Prozess
Forward compatibility of hardware is planned: The hardware forward compatibility strategy considers future requirements and includes measures to oversize hardware to facilitate future upgrades.	x					R: SW-A A: S: SW-PM I:	vorgeschriebener Prozess
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.	x	x				R: SW-A A: S: SW-PM, PSM I:	vorgeschriebener Prozess
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.		x	x	x	x	R: SW-PM A: S: TV-Ing I:	SW-PM
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.		x				R: SW-PM A: S: PSM I:	SW-PM
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.	x	x	x	x	x	R: SW-A A: S: SW-PM I:	SW-A
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.	x	x				R: SW-A A: S: SW-PM, PSM I:	SW-A

4 Kompatibilität & Modulare Bauweise

4.2 Modular design

AQI Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
"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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.		x	x	x	x	R: SW-PM A: S: SW- A I:	SW-PM
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.	x	x				R: Law A: S: SW-PM, SW-A I:	Law

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)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.	x	x				R: SW-A A: S: Law I: SW-PM	SW-A
FOSS components are documented and traceable: All FOSS components used are fully documented and versions are clearly traceable to ensure consistent maintenance and updates.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.		x	x	x	x	R: SW-PM A: S: Security I:	SW-A
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.		x	x			R: SW-PM A: S: SW-A I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
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.	x	x				R: SW-A A: S: SW-PM, Security I: QM	SW-A
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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".	x	x	x	x	x	R: SW-A A: S: SW-PM, Security I:	SW-A

5 Processes & Framework Conditions

5.2 A-Spice/VDA 6.3

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: QM I:	SW-PM
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.		x				R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

5 Processes & Framework Conditions

5.3 Cybersecurity

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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]	x	x				R: Security A: S: SW-A, SW-PM I:	Security
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.		x	x	x	x	R: SW-PM A: S: Security I:	SW-PM

[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

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
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.	x	x				R: SW-A A: S: SW-PM, QM I:	SW-A
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Responsibilities for risk management are defined: Clear responsibilities are defined for monitoring, assessing and managing risks throughout the entire product lifecycle.		x				R: SW-PM A: S: QM I:	SW-PM
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.		x				R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

6 Risk management

6.2 Emergency and crisis management

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x				R: SW-PM A: S: SW-A, QM I:	SW-PM
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.		x				R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: TV-Ing, QM I:	SW-PM
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.		x				R: SW-PM A: S: QM I:	SW-PM
Crisis management strategies are documented: Detailed crisis management strategies, including escalation levels and decision paths, are documented and regularly updated.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: SW-A I: QM	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

6 Risk management

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

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x	x	x	x	R: SW-PM A: S: QM I: Law	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I: Law	SW-PM
Resposibility for legislative changes is defined: The responsibilities within the supply chain for updating software components due to legal changes are clearly defined.		x				R: SW-PM A: S: QM I: Law	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I: Law	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
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.		x				R: SW-PM A: S: QM I:	SW-PM
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.		x				R: SW-PM A: S: QM I:	SW-PM

6 Risk management

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

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x	x	x	x	R: SW-PM A: S: Security, QM I:	SW-PM

6 Risk management

6.4 Disruptions and end-customer behavior

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.	x	x				R: SW-A A: S: SW-PM I:	SW-A
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.				x		R: SW-PM A: S: QM I:	SW-PM
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.	x			x		R: SW-PM A: S: QM I:	SW-PM

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 Cooperation in a Tier N supplier structure

7.1 Collaboration models

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.	x					R: SW-PM A: S: PSM I:	SW-PM
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.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
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.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
Responsibilities and competencies are documented: All responsibilities and accountabilities within the collaboration models are clearly documented and assigned to the respective parties.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
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.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
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.		x	x	x		R: SW-PM A: S: QM I: Alle	SW-PM
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.		x	x	x		R: SW-PM A: S: I: Alle	SW-PM

7 Cooperation in a Tier N supplier structure

7.2 Cooperation with subcontractors

AQI Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
Distribution of responsibilities is clearly defined: The distribution of competencies between OEMs, suppliers and subcontractors is clearly regulated and documented to ensure smooth cooperation.	x	x	x	x	x	R: SW-PM A: S: SW-A, QM I:	SW-PM
Documentation is transparent and accessible: All relevant documentation, including technical specifications and process descriptions, is accessible to all partners and is updated regularly.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
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.	x	x				R: SW-A A: S: SW-PM I:	SW-PM
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.		x	x	x		R: SW-PM A: S: SW-A I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: PSM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: PSM I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

7 Cooperation in a Tier N supplier structure

7.3 Documentation (SBOM, CBOM)

Automotive Quality Institute

Checkpoints

	When?					Who?	Who needs training?
	Concept development	Series develop-ment	Series preparation/ Go-live of the systems	Operation	Dectivation/ Decommissioning		
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]		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
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.		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
Standardised implementation in the supply chain: The handling of SBOMs and CBOMs is standardised for the entire supply chain.		x				R: SW-PM A: S: SW-A I:	SW-PM

[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