AQI Automotive Quality Institute

Schulungsinhalte Software-Langzeitqualität

Detaillierter Projekt-Überblick

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

Agenda

AQI Automotive Quality Institute

- Projektbeschreibung der Vorgehensweise
- Projektinhalte
- Checklistenbezug – Zeitliche Einordnung und Verantwortlichkeiten

Schulungsinhalte Software-Langzeitqualität

Folgeprojekt 2025

AQI Automotive Quality Institute

Ist-Situation und Problembeschreibung

- Im Rahmen eines Digitalen Lifecycle Managements sind die Produkte über den **gesamten Nutzungszeitraum aktuell zu halten** und darüber hinaus mit weiteren **Funktionalitäten zu erweitern**. Dies hat Auswirkungen u. a. auf: **Verträge/Zusammenarbeit im Kunden-Lieferanten-Verhältnis** als auch auf **Organisationen und Prozesse** bei OEM und Lieferanten.
- Vom AQI wurden im Projekt 2023 ein **10-Punkte-Plan** und im Projekt 2024 eine umfangreiche **Checkliste** erarbeitet, die in den Unternehmen sofort genutzt werden können. Diese Ergebnisse helfen, die Herausforderungen zu erfüllen, um die **Langzeitqualität von Software** gewährleisten zu können.
- Um die Umsetzung in den Unternehmen weiter zu unterstützen, sollen im aktuellen Projekt aus diesen Materialien und den weiteren Projektergebnissen **Schulungsinhalte** entwickelt werden. Dazu ist es notwendig, zu den in den beiden bisherigen Projekten entwickelten **technischen Anforderungen** die **bei Mitarbeitern notwendigen Kompetenzen/Wissen** zu erarbeiten und ein **Mapping** zwischen technischen Anforderungen und benötigte Kompetenzen/Wissen der Mitarbeiter herzustellen.
- Die Schulungsinhalte sollen ggf. in zwei Stufen entwickelt werden: als **Selbstlernprogramm** und als **Schulungsangebot**

Ziel und Nutzen

- **Ziel**: Absicherung der Softwarequalität im Kunden-Lieferanten-Verhältnis in der Serien-/Wartungsphase
- **Nutzen**: Notwendige Elemente für Schulung zur Software-Langzeitqualität in der Automobilindustrie sind erarbeitet

Lösungsweg

- Die in den AQI-Projekten zur Software-Langzeitqualität in den Jahren 2023 und 2024 gewonnenen Erkenntnisse werden genutzt, um die Schulungsinhalte auszuarbeiten.
- Die Erfahrungen aus weiteren AQI-Projekten (z. B. Schulung Digitaler Q-Manager) werden zusätzlich im Projekt genutzt.

Projektergebnisse

- Ausgearbeitete Schulungsinhalte zum Thema Software-Langzeitqualität (ggf. in zwei Stufen: Selbstlernprogramm und Schulungsangebot)
- Adressat der Schulungen: Mitarbeiter in den Unternehmen, die für die Umsetzung verantwortlich sind (z. B. auch in Softwareentwicklungsunternehmen, die nicht ausschließlich für die Automobilindustrie tätig sind → Sensibilisierung Langzeitqualität).
- Input für VDA 2 und AK13 (A-SPICE)

Projektlaufzeit und Dauer

01.01.2025 - 31.12.2025 (12 Monate)

AQI-Projektleiter und Team

- PL: Dr. Björn Schünemann
- Projektpate (Bosch): Axel Böringer
- Projektpartner (Automotive Quality Consulting GmbH): Christof Lorenz

Vorschlag / Abfrage von

- Empfehlung AQI-Fortsetzungsprojekt

Überblick

Projekt „Schulungsinhalte Software-Langzeitqualität“

Ziel des Projekts	Anwendbarkeit und **Umsetzung der Checklisten-Inhalte** in den Unternehmen unterstützen und Erarbeitung der dafür **notwendigen Elemente zur Schulung von Software-Langzeitqualität** → Die **technischen Anforderungen** der Checkliste sollen dazu auf **Unternehmensorganisation & -prozesse, Verantwortlichkeiten und Rollen/Mitarbeiterprofile** abgebildet werden
Geplante Projektergebnisse	**Umsetzungskonzept von Software-Langzeitqualität** in Unternehmen („Schulung“) → **Adressat:** Führungskräfte und Mitarbeiter, die für die **Erfüllung (von Teilen) der Checkliste** verantwortlich sind
Hinweis	Im Rahmen dieses Projekts werden **keine didaktischen Konzepte** entwickelt, um die erarbeiteten Inhalte in Schulungen zu vermitteln. Die Art der Wissensvermittlung ist nicht Bestandteil des Projekts.

Projektinhalte

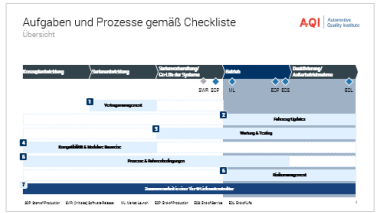
Bewertung gemäß Checkliste

Checkliste mit
7 Hauptkategorien und
insgesamt 38 Seiten

Alle Prüfpunkt nach Verantwortlichkeit (RASI) und zeitlicher Einordnung bewertet

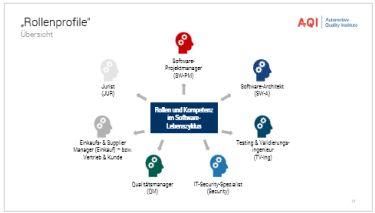
„Schulungsinhalte Software-Langzeitqualität" bzw. Umsetzungskonzept

Prozesse



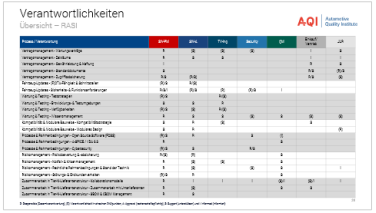
Besteht die Notwendigkeit neue oder angepasste Prozesse im Unternehmen zu etablieren?

Rollenprofile



Welche Rollen sind involviert? Wo könnten welche Aufgaben bestmöglich verankert sein?

Verantwortlichkeiten



Welche Verantwortlichkeiten gibt es für einzelne Aufgaben (Bewertung z.B. mit RASI-Matrix)?

Schulungsmodule

Welche Schulungsmodule werden mit welcher Kompetenz benötigt?

Ergebnis

Umsetzungskonzept
(diese Unterlage)

Befähigung der Unternehmen zur Erfüllung der Checkliste bzw. zur Sicherstellung der Langzeitqualität

„Prozesse"

„Rollenprofile"

„Verantwortlichkeiten"

und Schulungsmodule

Agenda

AQI Automotive Quality Institute

- Projektbeschreibung der Vorgehensweise
- **Projektinhalte**
  - **Prozesse**
  - Rollenprofile
  - Verantwortlichkeiten
  - Schulungsmodule
- Checklistenbezug – Zeitliche Einordnung und Verantwortlichkeiten

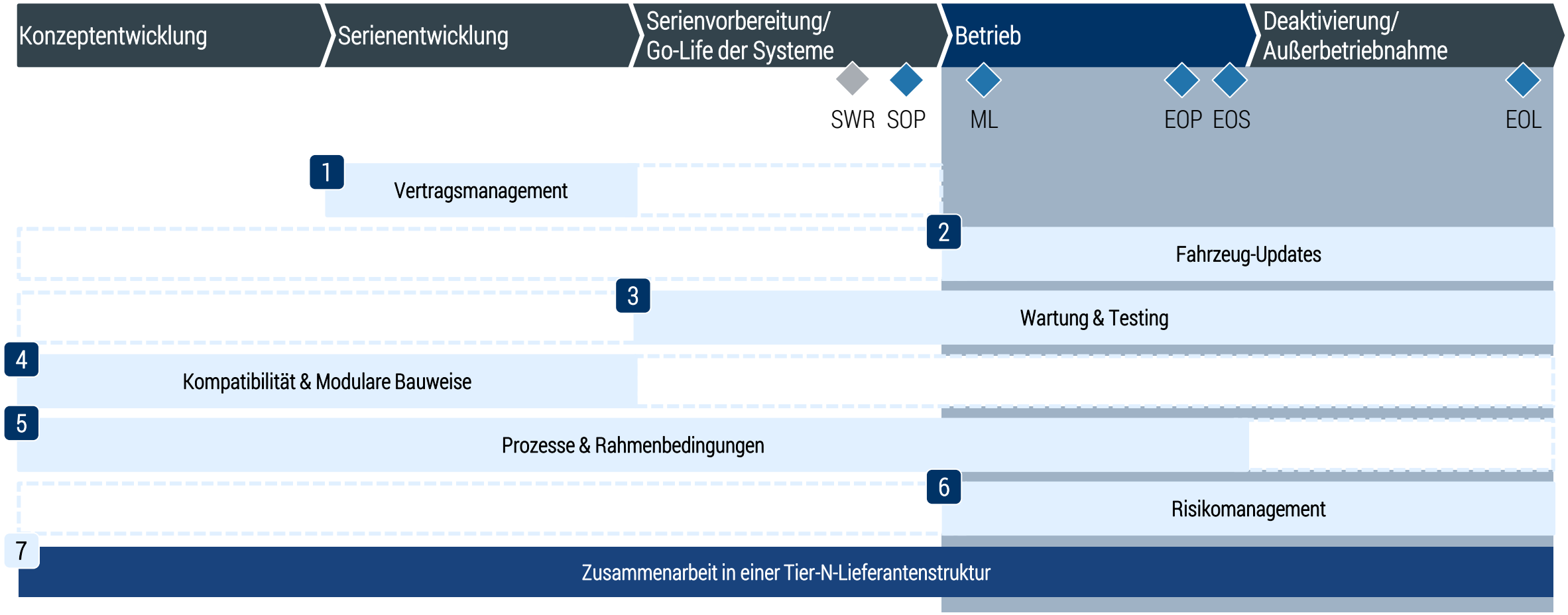
Prozesse

Zielsetzung

- Identifikation und Definition der **relevanten Prozesse**, die zur Sicherstellung der Software-Langzeitqualität erforderlich sind
- Sicherstellung, dass alle notwendigen **technischen, organisatorischen und regulatorischen Prozesse** vorhanden sind
- Anpassung bestehender und Implementierung neuer **Prozesse für Software-Wartung, Updates, Testing und Cybersecurity**
- Integration der **Checkliste zur Software-Langzeitqualität**
- Vermeidung von Risiken durch **klare Prozessabläufe für z.B. (F)OTA-Updates und Risikomanagement**

Aufgaben und Prozesse gemäß Checkliste

Übersicht



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

Kernaufgaben/Prozesselemente gemäß Checkliste

1. Vertragsmanagement

1.1 Wartungsverträge

- **Anforderungsdefinition:** Sammlung von Anforderungen aus Entwicklung, Testing, After-Sales
- **Vertragserstellung:** Aufsetzen der Wartungsverträge (inkl. Updateumfang, Reaktionszeiten, KPIs)
- **Verhandlung & Abschluss:** Abstimmung mit Tier-1, Rechtswesen, Einkauf
- **Review & Freigabe:** Juristische Prüfung und QM-Freigabe
- **Implementierung:** Verankerung in Projekt- und Lieferantenstruktur
- **Regelmäßige Überprüfung:** Turnusmäßige Aktualisierung nach techn./regulatorischem Stand

1.2 Zeiträume

- **Lebenszyklusmodell definieren:** SOP, EOP, EOS, EOL
- **Supportzeiträume festlegen:** Mindestlaufzeiten für Wartung und Sicherheitsupdates
- **Vertragliche Verankerung:** Fixierung der Zeiträume im Vertrag
- **Pflegezyklen & Verlängerungen planen:** Optionsklauseln & Änderungsmanagement
- **Lifecycle-Dokumentation etablieren:** Einbindung in Projekt- und QMS-Struktur

1.3 Gewährleistung & Haftung

- **Haftungsrisiken analysieren:** Juristische & technische Szenarien
- **Haftungsrahmen regeln:** Caps, Rückgriff, Gewährleistung
- **Verantwortlichkeiten klären:** Technisch und juristisch entlang der Lieferkette
- **Fallbacks definieren:** Absicherung durch Escrow, SLAs, Versicherung
- **Kommunikation & Awareness schaffen:** Klare Darstellung intern und extern

1.4 Standarddokumente

- **Vertragsvorlagen identifizieren:** Auswahl relevanter Muster (AGB, SLA, MSA)
- **Anpassung an Softwarekontext:** Einbindung von Checklisten-anforderungen
- **Zentrale Verwaltung:** Nutzung eines Vertragsmanagementsystems
- **Versionskontrolle & Reviewprozesse etablieren:** Aktualität & Compliance sicherstellen

1.5 Zugriffsabsicherung

- **Kritikalitätsbewertung durchführen:** Code, Zertifikate, Schlüssel, Dokumentation
- **Vertragsklauseln formulieren:** Zugriffsrechte, Escrow, Offenlegungspflichten
- **Zugriffswege dokumentieren:** Wer darf was, wann, wie?
- **Krisenmechanismen vorbereiten:** Für Insolvenz, Technikausfall, Lieferantenausstieg

Kernaufgaben/Prozesselemente gemäß Checkliste

2. Fahrzeug-Updates

2.1 (F)OTA-Fähigkeit & Schnittstellen	2.2 Sicherheits- & Funktionsanforderungen	Updateprozess-Management	Verantwortungsverteilung & Lieferantenintegration
▪ **Updatefähigkeit definieren:** Technische Anforderungen für (F)OTA identifizieren (Speicher, Bandbreite, Steuergeräte) ▪ **Systemarchitektur anpassen:** Integration von Updatekomponenten & modularen Softwarecontainern ▪ **Schnittstellen standardisieren:** Kommunikationsschnittstellen zwischen Backend, Gateway & Steuergeräten definieren ▪ **Technische Freigabeprozesse etablieren:** Release-Management für OTA-fähige Komponenten und Systeme ▪ **Testing & Validierung integrieren:** Rückfallmechanismen, Testumgebungen & Sicherheitsprüfungen aufbauen	▪ **Sicherheitsanforderungen definieren:** Absicherung der Kommunikation ▪ **Updateinhalte verifizieren:** Strukturierte Prüfung auf Integrität, Authentizität, Kompatibilität ▪ **Rollen & Verantwortlichkeiten klären:** Wer darf Releases signieren, freigeben, verteilen? ▪ **Update-Policies entwickeln:** Welche Updates werden wann und wie ausgerollt? ▪ **Regulatorische Anforderungen einbinden:** UNECE R156-konforme Updatefreigaben & Änderungsnachweise	▪ **Updatezyklen definieren:** Strategische Planung (z. B. monatlich, quartalsweise, eventbasiert) ▪ **Rollout planen & umsetzen:** Systematische Ausbringung nach Regionen, Baureihen oder Sicherheitsstufen ▪ **Kompatibilität sicherstellen:** Rückwärts-/Vorwärtskompatibilität durch Test- und Migrationsstrategien absichern ▪ **Dokumentation & Reporting:** Wer hat wann welche Version auf welchem Fahrzeug? ▪ **Feedbackmechanismen etablieren:** Erkennung von Fehlern im Feld & Rückverfolgbarkeit zur Fehlerquelle	▪ **Verantwortlichkeiten regeln:** OEM/Tier-1/Tier-2 Zuständigkeiten für Update-Bereitstellung, -Absicherung, -Support ▪ **Vertragsklauseln ergänzen:** Verbindliche Zusagen zur Langzeit-Updatefähigkeit & Wartung ▪ **Sicherheitsverpflichtungen fordern:** Verpflichtung zu regelmäßigen Security Patches und Reaktionszeiten ▪ **Update-Dokumentation verlangen:** Standardisierte Protokolle über ausgelieferte Softwarestände und Freigaben ▪ **Auditierbarkeit sicherstellen:** Prozesse, Tools & Nachweise für Audit und Behördenzugriff vorbereiten

Kernaufgaben/Prozesselemente gemäß Checkliste

3. Wartung & Testing

3.1 Teststrategien

- **Testkonzepte entwickeln:** Ableitung aus Architektur, Sicherheits-anforderungen & Updatezyklen
- **Testarten definieren:** Regressionstests, Kompatibilitätstests, Lebensdauertests
- **Automatisierungsgrad planen:** Toolgestützte Tests & „Continuous Integration / Continuous Delivery“
- **Abdeckung und Tiefe festlegen:** Welche Komponenten, Varianten, Releases werden wie getestet?
- **Verzahnung mit Release- & Updateprozess:** Tests als Freigabekriterium und Rückfallstrategie

3.2 Entwicklungs- & Testumgebungen

- **Testumgebungen spezifizieren:** Anforderungen an Hardware, Virtualisierung, Datenbanken
- **Verfügbarkeit sicherstellen:** Infrastruktur über die gesamte Projekt- und Wartungszeit
- **Zugriffs- & Nutzerkonzepte definieren:** Rechte, Protokollierung, Freigaben
- **Synchronisation mit Entwicklung:** Umgebungspflege parallel zur Produktreife
- **Archivierungs- & Reproduzierbarkeitsstrategien:** Wiederherstellung von Testumgebungen auch Jahre später

3.3 Verfügbarkeiten

- **Verfügbarkeitsstrategien planen:** Sicherstellen von Tools, Plattformen, Ressourcen
- **Verfügbarkeiten vertraglich absichern:** Lieferantenseitig garantierte Testinfrastruktur und Support
- **Redundanz & Backup-Systeme aufbauen:** Minimierung von Testausfällen
- **Langzeitfähige Testdaten erzeugen & pflegen:** z. B. anonymisierte Feldrückmeldungen
- **Monitoring & KPIs implementieren:** Nutzungs- und Reifegradmessung der Testinfrastruktur

3.4 Wissensmanagement

- **Wissensspeicher aufbauen:** Testfälle, Abdeckungsstrategien, Lessons Learned dokumentieren
- **Rollenbasiertes Training ermöglichen:** Schulungspläne für Tester, DevOps, Qualität
- **Versionierung & Historie erhalten:** Dokumentationspflichten & Reproduzierbarkeit sichern
- **Übergaben strukturieren:** Wissenstransfer bei Teamwechsel oder EOL-Übergängen
- **Tool- & Prozessdokumentation pflegen:** Verständlichkeit und Anwendbarkeit langfristig sichern

Kernaufgaben/Prozesselemente gemäß Checkliste

4. Kompatibilität & Modulare Bauweise

4.1 Kompatibilitätsstrategie

- **Kompatibilitätsziele definieren:** Rückwärts-/Vorwärtskompatibilität, Plattformstrategie
- **Abhängigkeiten analysieren:** Identifikation kritischer Komponenten & Schnittstellen
- **Verträglichkeitsmatrix aufbauen:** Welche Kombinationen sind getestet und freigegeben?
- **Testkonzepte entwickeln:** Spezielle Tests für Kompatibilität & Migrationsszenarien
- **Pflege über Lebenszyklus sicherstellen:** Nachverfolgung von Varianten & Updates

4.2 Modulares Design

- **Modularisierung planen:** Aufteilung in klar abgegrenzte, wartbare Softwaremodule
- **Schnittstellenstandardisierung etablieren:** Saubere, dokumentierte APIs mit stabilen Verträgen
- **Versionierung & Abhängigkeiten managen:** Strukturierter Umgang mit Release-Ständen & Komponentenzuordnung
- **Wartbarkeit im Design absichern:** Kapselung, Austauschbarkeit und Wiederverwendbarkeit früh berücksichtigen
- **Dokumentation & Reviewprozesse einführen:** Architekturfreigaben & Änderungsmanagement

Wiederverwendung & Variantenmanagement

- **„Reuse-Strategien“ (Wiederverwendung) definieren:** Wiederverwendbare Module über Projekte und Baureihen hinweg
- **Konfigurationsmanagement etablieren:** Variantenlogik, Feature-Sets & Parameterisierung
- **Tool-gestützte Rückverfolgbarkeit einführen:** Varianten & Releasestände systematisch abbilden
- **Standardisierung fördern:** Reduktion von Sonderlösungen zur Vereinfachung von Wartung & Updates
- **Organisatorische Verantwortlichkeiten klären:** Wer pflegt, wer entscheidet, wer freigibt?

Kernaufgaben/Prozesselemente gemäß Checkliste

5. Risikomanagement

5.1 Risikobewertung & -absicherung

- **Risikokategorien definieren:** Funktional, technisch, betrieblich, rechtlich, organisatorisch
- **Risikoidentifikation durchführen:** z. B. mittels FMEA, TARA, Experten-Workshops
- **Bewertung & Priorisierung:** Eintrittswahrscheinlichkeit × Auswirkung, Reifegrad, Risikoindikatoren
- **Absicherungsmaßnahmen ableiten:** Redundanzen, Tests, Vertragsklauseln, Monitoring
- **Risikoreview & Freigabeprozesse etablieren:** Regelmäßige Neubewertung & Statusüberprüfung

5.2 Notfall- & Krisenmanagement

- **Notfallprozesse definieren:** Vorgehen bei Sicherheitslücken, Updatefehlern, Inkompatibilität
- **Rollen & Eskalationsketten festlegen:** Wer entscheidet, wer informiert, wer handelt?
- **Kommunikationspläne vorbereiten:** Intern, Zulieferer, Kunden, Behörden
- **Krisensimulationen durchführen:** Vorbereitung auf Zero-Day, OTA-Failure, Massenrückrufe
- **Lessons Learned verankern:** Ableitung systematischer Verbesserungen nach Vorfällen

5.3 Rechtliche Rahmenbedingungen & Stand der Technik

- **Rechtliche Mindestanforderungen identifizieren:** Produktsicherheitsrecht, Produkthaftung, ISO 21434, UNECE R155/R156
- **„Stand der Technik" definieren & beobachten:** Branchen- und Technologiestand im jeweiligen Zeitpunkt
- **Regelmäßige juristische Bewertung & Dokumentation:** Interne Abstimmung mit Rechtswesen, QM, Security
- **Integration in Entwicklung & Verträge:** Anforderungen operationalisieren & absichern
- **Auditfähigkeit sicherstellen:** Nachweise, Risikodokumentation, Änderungsprotokolle

5.4 Infrastruktur & Endkundenverhalten

- **Externe Faktoren analysieren:** Netzverfügbarkeit, Kundennutzung, Regionale Vorschriften
- **Endkundenszenarien simulieren:** Update-Abbrüche, Fehlbedienungen, verspätete Nutzung
- **Risikopuffer & Fallbacks einplanen:** Retry-Strategien, Servicekonzepte
- **Kommunikationsstrategien entwickeln:** Transparenz gegenüber Kunden bei sicherheitsrelevanten Änderungen
- **Monitoring im Feld etablieren:** Früherkennung & Reaktion auf Muster in der Nutzung

Kernaufgaben/Prozesselemente gemäß Checkliste

6. Prozesse & Rahmenbedingungen

6.1 Open Source Software (FOSS)

- **FOSS-Strategie definieren:** Welche OSS-Komponenten dürfen wie eingesetzt werden?
- **Lizenzprüfung & Freigabeprozess etablieren:** Lizenzkompatibilität, Verbote, Pflichten
- **SBOM-Dokumentation führen:** Komponentenverzeichnis, Herkunft, Version, Lizenz
- **Compliance-Toolchain integrieren:** z. B. OSS Review Toolkit
- **Verpflichtungen in Verträge aufnehmen:** Offenlegungspflichten, Support, Updates, Auditrechte
- **Schulung & Awareness-Maßnahmen durchführen:** Technisch & rechtlich für Entwickler & Einkauf

6.2 A-SPICE / VDA 6.3

- **Prozesse gemäß A-SPICE einführen:** Planung, Entwicklung, Testing, Freigabe & Support
- **Reifegradmodell anwenden:** Level 1–5 zur kontinuierlichen Prozessverbesserung
- **Auditoren & Rollen definieren:** Projekt-QM, Prozessowner, Lieferantenschnittstelle
- **Lieferantenaudits durchführen:** Bewertung von Software-Entwicklungsqualität bei Tier-1/Tier-2
- **Verknüpfung mit anderen Normen sicherstellen:** ISO 26262, ISO 21434, UNECE etc.

6.3 Cybersecurity

- **Sicherheitsanforderungen definieren & verfolgen:** Aus Architektur, TARA, Risikoanalyse
- **Security by Design verankern:** Frühzeitige Einbindung in Konzept & Entwicklung
- **Cybersecurity Management System (CSMS) betreiben:** UNECE R155-konform
- **Sicherheitsnachweise dokumentieren:** Freigaben, Patches, Schwachstellenmanagement
- **Incident Response-Prozesse etablieren:** Erkennung, Reaktion, Reporting

Kernaufgaben/Prozesselemente gemäß Checkliste

7. Zusammenarbeit in der Tier-N-Lieferantenstruktur

7.1 Kollaborationsmodelle

- **Zusammenarbeitsmodelle definieren:** Direktsteuerung vs. Kaskadenmodell, Verantwortungsabgrenzung
- **Kommunikationsschnittstellen etablieren:** Technische & organisatorische Ansprechpartner je Tier
- **Anforderungen entlang der Kette durchreichen:** Transparenz sicherstellen – keine Informationsverluste
- **Synchronisationsroutinen einführen:** Regeltermine, gemeinsame Review- & Abstimmungsformate
- **Tool- & Datenkompatibilität abstimmen:** Kompatible Systeme & Formate (z. B. SBOM, Testberichte)

7.2 Zusammenarbeit mit Unterlieferanten

- **Vertragliche Absicherung über Tier-1 hinaus:** „Durchreichungsklauseln", Transparenzpflichten
- **Verantwortlichkeiten klären:** Wer ist für was in der Lieferkette verantwortlich (RASI)?
- **Risikoanalyse in der Kette durchführen:** Bewertung technischer & organisatorischer Risiken durch Sub-Lieferanten
- **Freigabekriterien je Tier definieren:** Technische und formale Anforderungen dokumentieren & auditieren
- **Lieferkettenüberwachung betreiben:** Monitoring, Eskalationswege & Eskalationsstufen

7.3 SBOM & CBOM Management

- **SBOM/CBOM-Anforderungen festlegen:** Struktur, Inhalt, Format
- **Pflichten zur Erstellung & Pflege vertraglich regeln:** Frequenz, Aktualität, Zugriffsrechte
- **Validierungsprozesse einführen:** Prüfung auf Vollständigkeit, Aktualität, FOSS-Compliance
- **SBOM entlang der Lieferkette weitergeben:** OEM vs. Tier-1 vs. Tier-2 vs. Zulieferer
- **Sicherheitsupdates & Lizenznachweise rückverfolgen:** Unterstützung bei Schwachstellenmanagement

Auditfähigkeit & Nachweisführung

- **Auditpflichten definieren:** Wer muss wann welche Nachweise liefern?
- **Auditdokumentation vorbereiten:** Checklisten, Templates, Belege für Zusammenarbeit & Qualität
- **Behördliche Anforderungen integrieren:** UNECE R155/R156, Produkthaftung, IT-Sicherheitsgesetz
- **Reviewmechanismen entlang der Kette einführen:** Reifegradbewertung, QS-Maßnahmen
- **Schulungs- & Awarenessmaßnahmen in der Lieferkette etablieren:** Auch bei Tier-2/Tier-3

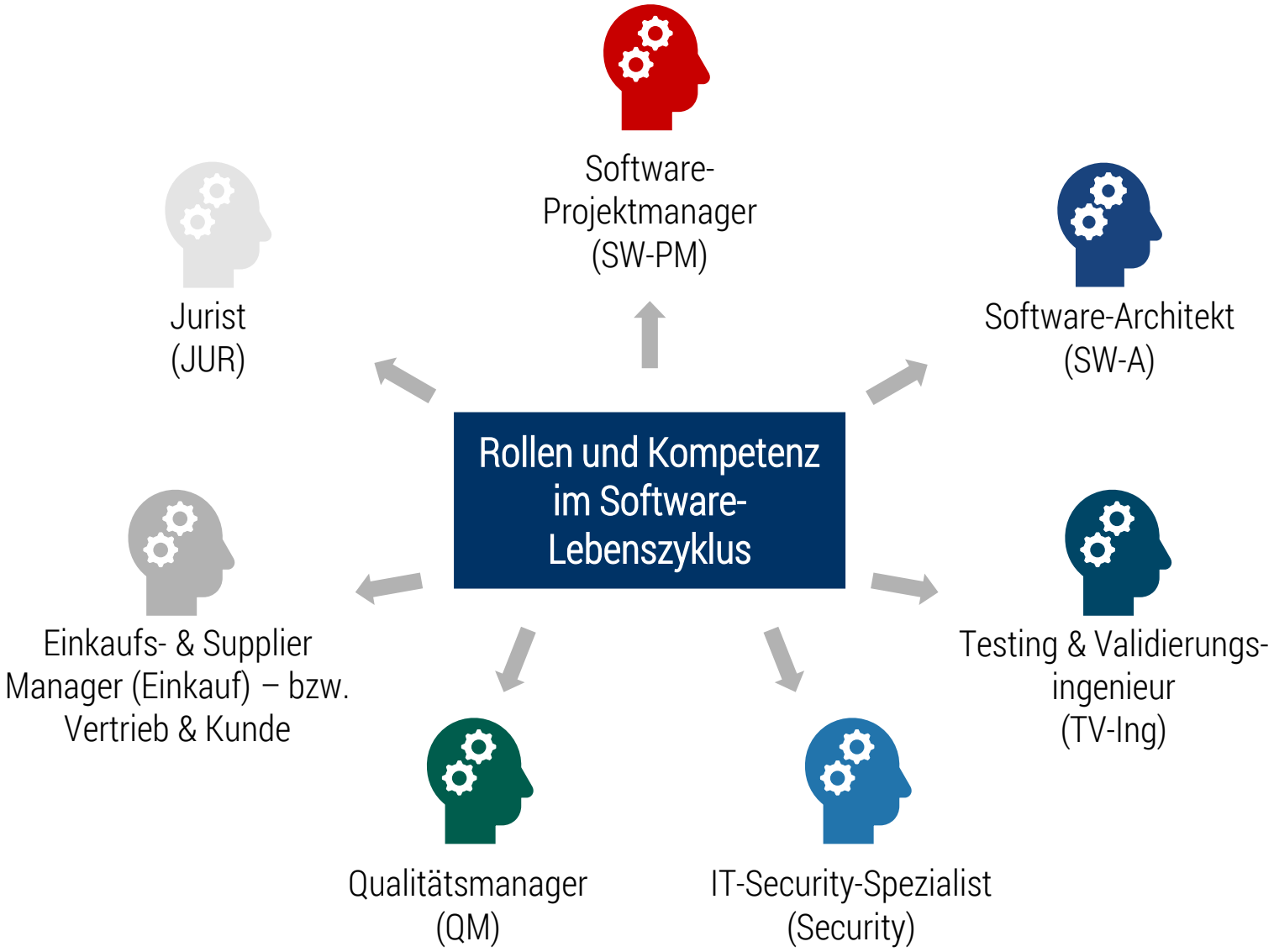
Agenda

AQI Automotive Quality Institute

- Projektbeschreibung der Vorgehensweise
- **Projektinhalte**
  - Prozesse
  - **Rollenprofile**
  - Verantwortlichkeiten
  - Schulungsmodule
- Checklistenbezug – Zeitliche Einordnung und Verantwortlichkeiten

„Rollenprofile“

Übersicht



„Rollenprofile“

Inhalte – Relevante Rollenprofile & Verantwortlichkeiten

AQI Automotive Quality Institute

- **Software-Projektmanager:** Verantwortet die projektseitige Koordination aller Langzeitqualitätsmaßnahmen, Integration von Langzeitqualitätszielen & der Checkliste, stellt Termine, Nachweise und abteilungsübergreifende Umsetzung sicher
- **Software-Architekt:** Verantwortlich für eine modulare, wartbare Architektur und die langfristige Kompatibilität von Softwarekomponenten und Schnittstellen für Langzeitqualität
- **Testing & Validierungs-Ingenieur:** Plant und führt Teststrategien für Kompatibilität, Regression und Lebensdauer durch und stellt die Wiederverwendbarkeit von Testfällen sicher (inkl. Langzeitteststrategien)
- **IT-Security-Spezialist:** Bewertet Cybersecurity-Risiken (TARA), Update-Absicherung, Patch-Management und Auditfähigkeit nach ISO 21434 / UNECE R155, Schwachstellenmanagement und berät zu sicherer Architektur
- **Qualitätsmanager:** Sichert die Einhaltung von Qualitätsstandards, verantwortet Auditfähigkeit und Qualitätsnachweise entlang der Lieferkette (Lieferantenbewertung & Qualitätssicherung in Softwareprojekten)
- **Einkaufs- & Supplier Manager/Vertrieb:** Gestaltet und verhandelt Verträge zu Wartung, FOSS, steuert Tier-1/Tier-2 bzgl. Softwarequalität & Vertrags-Compliance, Supplier-Absicherung bzgl. Wartung, Update, FOSS
- **Jurist:** Prüft und gestaltet Verträge mit Fokus auf Updatepflicht, Verfügbarkeit, Haftung, Open Source Compliance und regulatorische Anforderungen (z.B. UNECE), Regulatorik in Regionen

„Rollenprofile“

Übersicht und Beschreibung der Aufgaben

AQI Automotive Quality Institute

Software-Projektmanager	Verantwortlich für die projektseitige Planung, Steuerung und Koordination aller Aktivitäten rund um softwarebezogene Langzeitqualität: ▪ Integration der Checkliste und aller Langzeitqualitätsziele in die Projektstruktur und Meilensteine ▪ Koordination von Entwicklungs-, Test-, Sicherheits- und Lieferantenaktivitäten ▪ Risikomanagement, Dokumentation und Fortschrittsüberwachung ▪ Abstimmung mit Einkauf, Architektur, Testing, Security, QM, Rechtswesen ▪ Eskalations- und Kommunikationsschnittstelle zur Gesamtprojektleitung
Software-Architekt	Verantwortlich für das Design, die Dokumentation und die strategische Weiterentwicklung der Softwarearchitektur mit Fokus auf Modularität, Kompatibilität und Updatefähigkeit: ▪ Entwicklung modularer, wartbarer Architekturen mit Fokus auf Updatefähigkeit & Kompatibilität ▪ Definition stabiler Schnittstellen (APIs) und Rückwärts-/Vorwärtskompatibilität ▪ Integration von (F)OTA-Fähigkeit, Sicherheitsmechanismen und Versionierung ins Architekturdesign ▪ Dokumentation von Architekturentscheidungen, Release-Ständen und Varianten ▪ Enge Abstimmung mit Entwicklung, Testing, Security, Einkauf und Projektmanagement
Testing & Validierungs-Ingenieur	Zuständig für die Planung, Umsetzung und Pflege von Teststrategien, die Langzeitqualität messbar und nachweisbar machen: ▪ Entwicklung und Durchführung von Regressions- und Kompatibilitätstests ▪ Aufbau von testbaren (F)OTA-Szenarien und Rückfallstrategien ▪ Pflege langfristig verfügbarer Testumgebungen und Tools ▪ Sicherstellung der Rückverfolgbarkeit (Traceability) von Anforderungen bis Testergebnissen ▪ Unterstützung bei Audits, Freigaben und Feldrückmeldungen
IT-Security-Spezialist	Verantwortlich für die langfristige Absicherung von Softwarelösungen, Updateprozessen und Zuliefererketten: ▪ Durchführung von TARA (Threat and Risk Assessment) für neue Softwarekomponenten ▪ Verankerung von Sicherheitsanforderungen in Architektur, Wartung & Testing ▪ Aufbau & Pflege von Methodiken zur Sicherstellung der IT-Security ▪ Reaktion auf Schwachstellen im Feld (Incident Response) ▪ Unterstützung bei Sicherheits-Audits, Nachweispflichten & Reporting

Qualitätsmanager	Steuert und überwacht die Prozess- und Qualitätsabsicherung entlang des gesamten Softwarelebenszyklus: ▪ Umsetzung und Überwachung von Qualitätsstandards ▪ Bewertung von Lieferanten hinsichtlich Softwarequalität & Compliance ▪ Prozessfreigaben, Review von Reifegraden & Eskalationsfähigkeit ▪ Sicherstellung der Dokumentationspflichten (Checklisten, Nachweise, Auditdokumentation) ▪ Koordination des internen „Langzeit-Qualitätsboards“
Einkaufs- & Supplier Manager/ Vertrieb	Zentrale Schnittstelle für die Vertragliche und prozessuale Absicherung von Anforderungen entlang der Lieferkette: ▪ Gestaltung und Verhandlung von Verträgen bzgl. Updatepflicht, Wartung, Support ▪ Verankerung von FOSS-/Open-Source-Compliance-Klauseln in Lieferantenverträgen ▪ Steuerung und Bewertung von Tier-1 / Tier-2 bzgl. Software-Langzeitqualität ▪ Durchführung von Lieferantenaudits und Nachweisprüfungen ▪ Zusammenarbeit mit Rechtswesen, Architektur, QM und Security bei Lieferantenauswahl
Jurist	Juristisch verantwortlich für die rechtssichere Ausgestaltung und Absicherung aller Langzeitqualitäts-relevanten Verpflichtungen: ▪ Prüfung und Mitgestaltung von Verträgen zu Wartung, Updates, Verfügbarkeiten ▪ Einbindung regulatorischer Anforderungen wie UNECE R155/R156, ISO 21434 und regionale Unterschiede ▪ Bewertung von Lizenzrisiken (z. B. Open Source GPL), Produkthaftung & Regressszenarien ▪ Unterstützung bei Eskalationen und im Krisen-/Vorfallmanagement ▪ Zusammenarbeit mit Einkauf, QM, Architektur, PM und IT-Security

Steckbrief

Software-Projektmanager (SW-PM)

AQI Automotive Quality Institute

Funktion der Rolle

- Verantwortlich für Planung, Steuerung & Umsetzung softwareintensiver Projekte.
- Zentrale Schnittstelle zwischen Technik, Einkauf, Rechtswesen, Qualität & externen Partnern.
- Sicherstellung der Integration von Langzeitqualitätsaspekten über den gesamten Projektlebenszyklus.

Kernaufgaben

- Projektplanung, Milestones, Ressourcenmanagement
- Einbindung der Langzeitqualitäts-Checkliste in alle Projektphasen
- Steuerung von Updates, Risiko- und Änderungsmanagement
- Kommunikationsschnittstelle & Eskalationskoordination
- Schnittstelle zu Einkauf, IT-Security, Testing, Rechtswesen & After-Sales

Kompetenzprofil

- Projektmanagement: Klassisches & agiles PM, Ressourcenplanung, Milestone-Verfolgung
- Technisches Verständnis: Architektur, Modularisierung, (F)OTA-Fähigkeit, Testing-Grundverständnis
- Kommunikation & Führung: Stakeholderkoordination, Moderation, Reporting
- Regulatorik & Normen: A-SPICE, ISO 21434, UNECE R155/156
- Risikomanagement: Bewertung & Steuerung technischer und organisatorischer Risiken
- Vertragsverständnis: Grundlagen zu Wartungsverträgen, Gewährleistung, Lieferverpflichtungen
- Change & Configuration: Handhabung von Softwareänderungen, Releasemanagement
- Qualitätsverständnis: Verankerung qualitätssichernder Maßnahmen im Projekt

Checklistenbezug – Verantwortlichkeiten

1. Vertragsmanagement: Wartungsverträge, Zeiträume, Standarddokumente
2. Fahrzeug-Updates: (F)OTA-Fähigkeit, Sicherheitsanforderungen
3. Wartung & Testing: Entwicklungsumgebungen, Verfügbarkeiten, Teststrategien
4. Kompatibilität & Modulare Bauweise: Kompatibilitätsstrategie
5. Risikomanagement: Krisenmanagement, rechtliche Rahmenbedingungen
6. Prozesse & Rahmenbedingungen: A-SPICE, FOSS, Cybersecurity
7. Zusammenarbeit Tier-N-Struktur: Kollaborationsmodelle, SBOM-Management

Steckbrief

Software-Architekt (SW-PM)

AQI Automotive Quality Institute

Funktion der Rolle

- Konzeption und Design modularer, wartbarer Softwarearchitekturen
- Sicherstellung von Kompatibilität, Updatefähigkeit und Wartbarkeit über den gesamten Lebenszyklus
- Integration technischer Anforderungen der Software-Langzeitqualität in die Architekturstrategie

Kernaufgaben

- Architekturentscheidungen, Technologiewahl, Schnittstellendefinition
- Technische Abstimmung mit Entwicklung, Testing, IT-Security und Projektleitung
- Dokumentation & Pflege der Architektur über den Lebenszyklus
- Einhaltung von Sicherheits-, Wartungs- & EOL-Anforderungen in der Architektur

Kompetenzprofil

- Softwarearchitektur: Modularisierung, Entwurfsmuster, Architekturstandards
- Kompatibilitätsmanagement: Strategien zur Rückwärts-/Vorwärtskompatibilität
- API- und Schnittstellendesign: Gestaltung wartungsfreundlicher, klar dokumentierter Schnittstellen
- Update- & Lifecycle-Strategie: Berücksichtigung von EOL, (F)OTA & Versionierung in der Architektur
- Cybersecurity-Integratio: Sicherheitsarchitektur, Threat-Modelling, ISO 21434
- Open Source & Compliance: Berücksichtigung von FOSS, SBOM, Lizenzpflichten
- Dokumentation & Modellierung: Verwendung von Tools & Standards zur strukturierten Architekturpflege
- Kommunikation & Moderation: Zusammenarbeit mit technischen und nicht-technischen Stakeholdern

Checklistenbezug – Verantwortlichkeiten

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

Steckbrief

Testing & Validierungs-ingenieur (TV-Ing)

AQI Automotive Quality Institute

Funktion der Rolle

- Planung, Durchführung und Bewertung von Softwaretests zur Sicherstellung der langfristigen Qualität
- Verantwortung für die Testabdeckung von Updatefähigkeit, Kompatibilität, Wartbarkeit und Sicherheitsanforderungen
- Enge Zusammenarbeit mit Entwicklung, Architektur und Qualitätsmanagement zur spezifikations- und anforderungsgerechten Verifikation

Kernaufgaben

- Entwicklung von Testkonzepten und -strategien inkl. Langzeitaspekte
- Aufbau und Pflege von Testumgebungen, Regressionstestketten und Absicherungstools
- Validierung von (F)OTA-Funktionalitäten, Kompatibilität, Rückwärts-/Vorwärtsintegration
- Fehlerdokumentation, Rückverfolgbarkeit & Testreporting
- Unterstützung bei Audits und Freigabeentscheidungen (z. B. SOP, Releases, Wartungsupdates)

Kompetenzprofil

- Teststrategie & -planung: Entwicklung zielgerichteter Strategien für verschiedene Testarten
- Testautomatisierung: Kenntnisse in Testframeworks, Skripting und Tools
- Kompatibilitätstests: Planung von Cross-Version-, Cross-Plattform-, Cross-Komponenten-Tests
- (F)OTA-Testmethodik: Updatezyklen testen, Rückfallmechanismen, Validierung von Sicherheitspatches
- Rückverfolgbarkeit & Dokumentation: Sicherstellung von Traceability zu Anforderungen & Testfällen
- Langzeittest & EOL-Verifikation: Wartbarkeit, Performance über Lebensdauer testen
- Tool-Know-how: z. B. Jenkins, Python, Vector Tools, CANoe, Git
- Kommunikation: Abstimmung mit Entwicklung, Architektur, Qualität und Projektleitung

Checklistenbezug – Verantwortlichkeiten

2. Fahrzeug-Updates: Validierung von Updatefähigkeit, Sicherheits- und Funktionsprüfung

3. Wartung & Testing: Teststrategien, Testumgebungen, Verfügbarkeiten

4. Kompatibilität & Modulare Bauweise: Rückwärts-/ Vorwärtskompatibilitätstests

5. Risikomanagement: Fehleranalyse, Testabdeckung kritischer Funktionen

6. Prozesse & Rahmenbedingungen: Nachweise für A-SPICE, Auditvorbereitung, Absicherung von SBOM

Steckbrief

IT-Security-Spezialist (Security)

AQI Automotive Quality Institute

Funktion der Rolle

- Verantwortung für die Cybersicherheit von softwareintensiven Systemen über den gesamten Produktlebenszyklus
- Bewertung und Umsetzung von Sicherheitsanforderungen (z. B. nach ISO 21434, UNECE R155/156)
- Unterstützung bei der Sicherstellung von Schutzmaßnahmen, die auch bei Updates, in der Wartung und im EOL-Zustand greifen

Kernaufgaben

- Bedrohungs- & Risikoanalysen (TARA) durchführen/pflegen
- Entwicklung und Validierung von Sicherheitskonzepten & -architekturen
- Definition von Anforderungen an kryptographische Komponenten, Secure Boot, Secure Updates
- Überprüfung und Dokumentation sicherheitsrelevanter Funktionen & Absicherungen
- Beratung anderer Fachbereiche (Architektur, Testing, Einkauf, Rechtswesen) bei Sicherheitsfragen
- Unterstützung bei Sicherheitsvorfällen & Incident-Management

Kompetenzprofil

- Cybersecurity-Standards: ISO 21434, UNECE R155/156, NIST, BSI Grundschutz
- TARA-Methodik: Durchführung und Pflege von Threat & Risk Assessments
- Security-by-Design: Integration von Sicherheitsaspekten in Architektur und Entwicklungsprozess
- Update-Sicherheit: Kryptographisch abgesicherte (F)OTA-Prozesse, Schlüssel- und Zertifikatsmanagement
- Incident Response: Analyse, Koordination & Eskalation bei Sicherheitsvorfällen
- Tool-Know-how: z. B. Security Analyzer, TARA Tools, Penetrationstest-Tools
- Beratung & Schnittstellenarbeit: Kommunikation mit PM, Testing, Rechtswesen, Architektur, Einkauf

Checklistenbezug – Verantwortlichkeiten

1. Vertragsmanagement: Anforderungen an Zugriffssicherheit und Sicherheitsklauseln im Vertrag
2. Fahrzeug-Updates: Sicherheitsanforderungen, Secure Update, Zertifikatmanagement
3. Wartung & Testing: Absicherung von Wartungszugängen, Sicherheitsvalidierung
5. Risikomanagement: Bedrohungsanalysen, Incident-Handling, Notfallmanagement
6. Prozesse & Rahmenbedingungen: Cybersecurity-Vorgaben (ISO 21434, UNECE R155), Sicherheitskonzepte
7. Tier-N-Zusammenarbeit: Absicherung von Drittsoftware, Risikoanalyse in der Lieferkette

Steckbrief

Qualitätsmanager (QM)

AQI Automotive Quality Institute

Funktion der Rolle

- Sicherstellung der Einhaltung aller qualitäts-relevanten Prozesse, Normen und Standards im Lebenszyklus softwareintensiver Systeme
- Verantwortung für die Implementierung und Überwachung qualitätssichernder Maßnahmen mit Fokus auf Langzeitverfügbarkeit und Wartbarkeit
- Begleitung interner und externer Audits sowie kontinuierliche Verbesserung qualitätsbezogener Abläufe

Kernaufgaben

- Entwicklung, Pflege und Überwachung qualitätsrelevanter Prozesse (z. B. A-SPICE, VDA 6.3)
- Unterstützung der Fachabteilungen bei der korrekten Umsetzung von Qualitätsanforderungen
- Nachverfolgbarkeit und Konsistenz von Software-Qualitätsnachweisen (z. B. Testing, Review, Audit)
- Auditierung von Lieferanten im Hinblick auf Softwarequalität und Langzeitfähigkeit
- Schulung von Teams in Qualitätsstandards & -prozessen
- Fehleranalysen und Ableitung syst. Verbesserungsmaßnahmen

Kompetenzprofil

- Qualitätsstandards & Normen: A-SPICE, ISO 9001, VDA 6.3, ggf. ISO 26262, ISO 21434
- Prozessmanagement: Definition, Monitoring & Verbesserung von Qualitätssicherungs-prozessen
- Auditkompetenz: Durchführung interner & externer Audits, Lieferantenaudits
- Langzeitqualitätsbewertung: Analyse von Wartungsfähigkeit, Kompatibilität & EOL-Konzepten
- Softwarequalitätsverständnis: Bewertung technischer Maßnahmen, Testabdeckungen, Updatefähigkeit
- Kommunikation & Durchsetzungsstärk: Vermittlung zwischen Technik, Management und Lieferanten
- Tool-Know-how: z. B. QMS-Systeme, DOORS, APIS IQ, Auditsoftware

Checklistenbezug – Verantwortlichkeiten

1. Vertragsmanagement: Sicherstellung qualitätsrelevanter Vertragsbestandteile
2. Fahrzeug-Updates: Nachweisführung zu Updatefähigkeit
3. Wartung & Testing: Wissensmanagement, Teststrategien, Dokumentation
4. Kompatibilität & Modulare Bauweise: Test- und Regressionsabdeckung
5. Risikomanagement: Qualitätssicherung von Eskalations- und Notfallmanagement
6. Prozesse & Rahmenbedingungen: A-SPICE, VDA 6.3, Qualitätsprozesse und Prozessstandards
7. Tier-N-Zusammenarbeit: Review von SBOM/CBOM, Lieferantenaudits

Steckbrief

Einkaufs- & Supplier Manager (Einkauf) – bzw. Vetrieb & Kunde

Funktion der Rolle

- Verantwortung für die Vertragsgestaltung und Lieferantensteuerung im Bereich softwareintensiver Systeme
- Absicherung, dass Lieferanten ihre Verpflichtungen hinsichtlich Software-Wartung, Updates, Kompatibilität und Cybersecurity erfüllen
- Steuerung der Einhaltung von Langzeitqualitätsanforderungen durch vertragliche und strategische Maßnahmen

Kernaufgaben

- Erstellung und Verhandlung von Verträgen inkl. Wartungs-, Update- und Sicherheitsklauseln
- Bewertung und Auswahl Softwarelieferanten (Tier-1/Tier-2)
- Sicherstellung, dass Anforderungen wie FOSS-Compliance vertraglich geregelt sind
- Überwachung der Lieferantenperformance im Hinblick auf Softwarequalität und -verfügbarkeit
- Enge Zusammenarbeit mit Architektur, Qualitätsmanagement, IT-Security und Rechtswesen
- Unterstützung bei Audits, Eskalationen & Vertragsnachverhandl.

Kompetenzprofil

- Vertragsgestaltung: Gestaltung von Software-Wartungs-, Lizenz- & Serviceverträgen
- Lieferantensteuerung: Monitoring von Termintreue, Wartungsverpflichtungen & Qualitätszielen
- FOSS-Klauseln: Integration von Compliance-Anforderungen in Verträge
- Risikomanagement: Einschätzung & Absicherung potenzieller Lieferausfälle oder Compliance-Risiken
- Technisches Grundverständnis: Überblick über Updateprozesse, Softwarekomponenten & Sicherheitsanforderungen
- Kommunikation & Verhandlung: Interdisziplinäre Abstimmung, Vertragsverhandlung, Eskalationsmanagement
- Zusammenarbeit mit Rechtswesen/QM: Sicherstellung der technischen & rechtlichen Absicherung von Lieferverpflichtungen

Checklistenbezug – Verantwortlichkeiten

1. Vertragsmanagement: Wartungsverträge, Zeiträume, Standarddokumente, Zugriffsabsicherung

2. Fahrzeug-Updates: Vertragliche Sicherstellung von (F)OTA-Updatefähigkeit & Langzeitpflege

5. Risikomanagement: Absicherung von Update-, Security- & Wartungsverpflichtungen

6. Prozesse & Rahmenbedingungen: Open Source Compliance, Verfügbarkeitsabsicherung in der Lieferkette

7. Tier-N-Zusammenarbeit: Kollaborationsmodelle, Lieferantensteuerung, SBOM/CBOM-Vereinbarungen

Steckbrief

Jurist (Jur)

AQI Automotive Quality Institute

Funktion der Rolle

- Juristische Begleitung aller Aktivitäten rund um Softwareverträge, Haftung, Gewährleistung und regulatorische Vorgaben
- Absicherung, dass Software-Wartung, Updates, Open Source und Cybersicherheit rechtlich korrekt geregelt sind
- Unterstützung anderer Fachabteilungen bei der rechtssicheren Umsetzung der Checkliste zur Langzeitqualität

Kernaufgaben

- Prüfung und Erstellung von Vertragsklauseln zu Softwarepflege, Updatepflichten und EOL-Verfügbarkeit
- Beratung bei Haftungsfragen rund um Sicherheitslücken, Updateversäumnisse oder Inkompatibilitäten
- Bewertung & Dokumentation von Risiken im Zusammen-hang mit FOSS, Lizenzverletzungen, Datenschutz
- Unterstützung bei Vertragsverhandlungen mit Tier-1/Tier-2 im Softwarekontext
- Enge Zusammenarbeit mit Einkauf, Architektur, IT-Security, QM
- Beobachtung regulatorischer Entwicklungen auch in Regionen (z. B. UNECE R155/156, Produkthaftung EU/DE)

Kompetenzprofil

- Software-Vertragsrecht: Gestaltung & Prüfung von Verträgen zu Updates, Wartung, Verfügbarkeit
- Haftungs- & Gewährleistungsrecht: Risikoanalyse bei Fehlern, Sicherheitslücken, Inkompatibilitäten
- Open Source Compliance: Lizenzprüfung (z. B. GPL, LGPL), Risiken bei FOSS-Nutzung, SBOM-Klauseln
- Cybersecurity & Datenschutzrecht: Anforderungen aus ISO 21434, UNECE R155/156, DSGVO, IT-Sicherheitsgesetz
- Regulatorik: Prüfung regulatorischer Unterschiede in Regionen
- Technisches Grundverständnis: Kenntnis der relevanten Softwareprozesse, Updatezyklen, Komponentenstruktur
- Verhandlung & Beratung: Begleitung von Vertragsverhandlungen & Unterstützung der Fachabteilungen
- Risikomanagement & Eskalation: Juristische Einschätzung bei Abweichungen, Absicherungen, Eskalationswegen

Checklistenbezug – Verantwortlichkeiten

1. Vertragsmanagement: Wartungsverträge, Zeiträume, Gewährleistung, Haftung, Standarddokumente
2. Fahrzeug-Updates: Absicherung von Updateverpflichtungen und Verantwortung im Fehlerfall
5. Risikomanagement: Bewertung rechtlicher Rahmenbedingungen, Notfallpläne, Produkthaftung
6. Prozesse & Rahmenbedingungen: Open Source Compliance, Lizenz- & Datenschutzrecht
7. Tier-N-Zusammenarbeit: FOSS-Risiken in der Lieferkette

Agenda

AQI Automotive Quality Institute

- Projektbeschreibung der Vorgehensweise
- **Projektinhalte**
  - Prozesse
  - Rollenprofile
  - **Verantwortlichkeiten**
  - Schulungsmodule
- Checklistenbezug – Zeitliche Einordnung und Verantwortlichkeiten

Verantwortlichkeiten

Zielsetzung

AQI | Automotive Quality Institute

- **Klärung der Rollen und Zuständigkeiten** innerhalb des Unternehmens und entlang der Lieferkette
- Definition, **wer für welche Aspekte der Software-Langzeitqualität verantwortlich ist** (z. B. Entwicklung, Testing, Wartung, Zulieferermanagement, Cybersecurity, Compliance)
- Sicherstellung einer **klaren Kommunikations- und Entscheidungsstruktur**, um Eskalationen, Risiken und Sicherheitsvorfälle effizient zu managen
- **Integration der Checkliste zur Software-Langzeitqualität in die Verantwortungskette** des Unternehmens

Verantwortlichkeiten

Übersicht – RASI

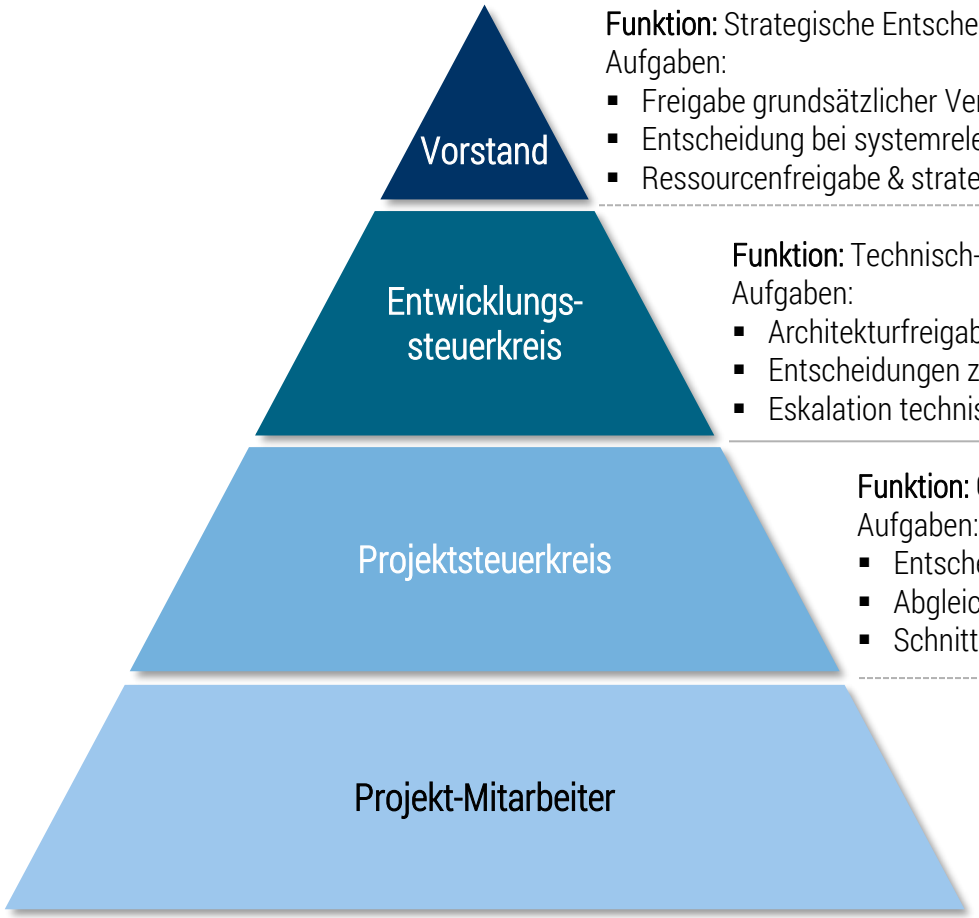
AQI Automotive Quality Institute

Prozess / Verantwortung	SW-PM	SW-A	TV-Ing	Security	QM	Einkauf/ Vertrieb	JUR
Vertragsmanagement - Wartungsverträge	R	(S)	(S)	(S)		I	S
Vertragsmanagement - Zeiträume	R	S	S			I	I
Vertragsmanagement - Gewährleistung & Haftung	I					R	S
Vertragsmanagement - Standarddokumente	S					R/S	(R)/S
Vertragsmanagement - Zugriffsabsicherung	R/S	(R/S)				R/S	(S)
Fahrzeug-Updates - (F)OTA-Fähigkeit & Schnittstellen	(R)/S	R/(S)					
Fahrzeug-Updates - Sicherheits- & Funktionsanforderungen	R/S/I	(R)/S	(R)	(R)/S	I		
Wartung & Testing - Teststrategien	(R)/S		R/(S)				
Wartung & Testing - Entwicklungs- & Testumgebungen	S	S	R				
Wartung & Testing - Verfügbarkeiten	(R)/S	(S)	R/(S)				
Wartung & Testing - Wissensmanagement	R	S	S	(S)	S	(S)	(S)
Kompatibilität & Modulare Bauweise - Kompatibilitätsstrategie	S	R	(S)			S	
Kompatibilität & Modulare Bauweise - Modulares Design	S	R					(R)
Prozesse & Rahmenbedingungen - Open Source Software (FOSS)	(R)/S	R		S	(I)		
Prozesse & Rahmenbedingungen - A-SPICE / VDA 6.3	R				S		
Prozesse & Rahmenbedingungen - Cybersecurity	(R)/S	S		R/S			
Risikomanagement - Risikobewertung & -absicherung	R/(S)	(R)			S		
Risikomanagement - Notfall- & Krisenmanagement	R	(S)	(S)		S		
Risikomanagement - Rechtliche Rahmenbedingungen & Stand der Technik	R	(S)		(S)	S		I
Risikomanagement - Störungs- & Endkundenverhalten	(R)/S	R			S		
Zusammenarbeit in Tier-N-Lieferantenstruktur - Kollaborationsmodelle	R	I	I	I	(S)/I	(S)/I	I
Zusammenarbeit in Tier-N-Lieferantenstruktur - Zusammenarbeit mit Unterlieferanten	R	(S)			S	S	
Zusammenarbeit in Tier-N-Lieferantenstruktur - SBOM & CBOM Management	R	S					

R: Responsible (Gesamtverantwortung), (R): Verantwortlichkeit in einzelnen Prüfpunkten, A: Approval (rechenschaftspflichtig), S: Support (unterstützen) und I: Informed (informiert)

Verantwortlichkeiten

Mögliche Funktion und Aufgaben im Unternehmen (exemplarische Gremien)



Funktion: Strategische Entscheidungen, Eskalation & Reputationsschutz
Aufgaben:
- Freigabe grundsätzlicher Vertrags- & Lieferstrategien (z. B. Wartungsmodelle)
- Entscheidung bei systemrelevanten Risiken (Haftung, Regulatorik, Markenimage)
- Ressourcenfreigabe & strategische Weichenstellung (z. B. „Updatefähigkeit über 15 Jahre“)

Funktion: Technisch-funktionale Entscheidungshoheit für alle Softwarethemen
Aufgaben:
- Architekturfreigaben, Modularisierungsstrategien
- Entscheidungen zu Plattformstrategie, Varianten, Updatefähigkeit
- Eskalation technischer Zielkonflikte oder Lieferprobleme

Funktion: Gesamtverantwortung für Zielerreichung, Ressourcensteuerung & operative Eskalationen je Projekt
Aufgaben:
- Entscheidung über Maßnahmen bei Risiken, Zielabweichungen
- Abgleich mit Projektzeitplan & Lieferantenstatus
- Schnittstelle zu anderen Steuerkreisen & Stakeholdern

Funktion: Umsetzung & Koordination aller operativen Aktivitäten zur Sicherstellung der Langzeitqualität je Projekt
Aufgaben:
- Checklisten-Integration & abteilungsübergreifende Abstimmung
- Review von Architektur, Test, Security, Verträgen
- Dokumentation, Nachweise & Auditvorbereitung

Verantwortlichkeiten

Zusammenarbeit mit Externen: OEM – Tier-1 – Tier-2 – Drittanbieter

OEM & Tier-1	▪ OEM definiert die Anforderungen zur Langzeitverfügbarkeit, Kompatibilität, Updatefähigkeit ▪ Tier-1 ist verantwortlich für Umsetzung & Nachweise (z. B. SBOM, Updatefähigkeit, Tests) ▪ Zusammenarbeit erfolgt durch: – Gemeinsame Architekturabstimmungen – Standardisierte Vertragsmodule (z. B. Wartungsvereinbarungen, FOSS-Vorgaben) – Freigaben & Reviews (Design, Test, Security, Release)
Tier-1 & Tier-2	▪ Tier-1 muss Anforderungen des OEM vertraglich und technisch weitergeben („Flow-down“) ▪ Tier-2 liefert Komponenten oder Softwaremodule, z. B. Libraries, Middleware, Algorithmen ▪ Erwartet wird: – Dokumentation von Komponenten (CBOM, SBOM) – Reaktionsfähigkeit bei Schwachstellen – Verfügbarkeit über Projektlaufzeit hinaus
Zusammenarbeit mit Drittanbietern/ Dienstleistern	▪ Z. B. für Security-Tools, Testsysteme, OTA-Plattformen oder Open-Source-Services ▪ Anforderungen: – Zugriffsschutz, Kompatibilität & Auditfähigkeit vertraglich absichern – Verfügbarkeiten & Wartungspflichten explizit festlegen – Regelmäßige Sicherheits- & Qualitätsnachweise

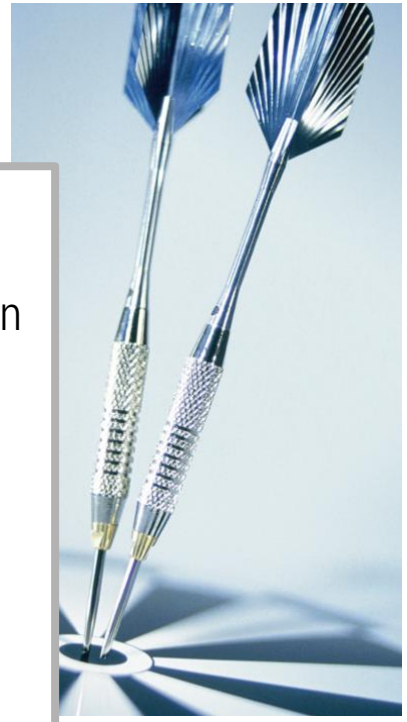
Agenda

AQI Automotive Quality Institute

- Projektbeschreibung der Vorgehensweise
- **Projektinhalte**
  - Prozesse
  - Rollenprofile
  - Verantwortlichkeiten
  - **Schulungsmodule**
- Checklistenbezug – Zeitliche Einordnung und Verantwortlichkeiten

„Rollenprofile“ inkl. Schulungskonzept

Zielsetzung



- Definition der **notwendigen Rollen und Qualifikationen**, um die Software-Langzeitqualität sicherzustellen
- Zuordnung der **Prozesse aus der Checkliste** zu den entsprechenden **Rollenprofilen**
- Entwicklung eines **zielgerichteten Schulungskonzepts**, um Wissen und Kompetenzen langfristig im Unternehmen zu verankern
- Sicherstellung, dass **alle relevanten Abteilungen und Stakeholder** das notwendige Fachwissen haben, um Software-Langzeitqualität in ihrer jeweiligen Funktion umzusetzen

Kompetenzprofile für Schulungskonzept

Übersicht: Ausprägungsmatrix nach Kategorien der Checkliste

AQI | Automotive Quality Institute

	Schulungsmodule						
	1 Vertragsmanagement	2 Fahrzeug-Updates	3 Wartung & Testing	4 Kompatibilität & Modulare Bauweise	5 Prozesse & Rahmenbedingungen	6 Risikomanagement	7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur
Software-Projektmanager	●	◉	●	◉	◉	◉	●
Software-Architekt	○	◉	●	◉	●	●	●
Testing & Validierungs-Ingenieur	○	◉	◉	●	○	●	○
IT-Security-Spezialist	○	●	○	○	○	◉	○
Qualitätsmanager	○	○	●	○	◉	●	○
Einkaufs- & Supplier Manager	◉	○	○	○	●	◉	◉
Jurist	◉	○	○	○	○	○	○

◉ = Erhöhter Schulungsbedarf ● = Mittlerer Schulungsbedarf ○ = Geringer/kein Schulungsbedarf

Kompetenz-/Schulungsmodul

1 Vertragsmanagement

- Grundlagen zu Wartungs- und Updateverträgen
- Gestaltung von Service-Level-Agreements (SLA)
- Definition von Laufzeiten und Verlängerungsmechanismen
- Regelung von Gewährleistung und Haftung bei Softwaremängeln
- Flow-down von OEM-Anforderungen an Lieferanten
- Absicherung langfristiger Zugriffsmöglichkeiten (z. B. Escrow)
- Berücksichtigung von FOSS-Compliance im Vertrag
- Umgang mit Standardvertragsklauseln (z. B. DIN, VDA, UNECE)
- Abstimmung technischer Anforderungen mit Legal / Einkauf
- Verhandlungstechniken & Risikoverteilung bei Softwareprojekten
- Rechtssichere Vertragsgestaltung und Umgang mit Leistungsstörungen bei internationalen Verträgen
- (Standard)Dokumentation von Protokollen und Verträgen
- Leistungsspezifikation - Pflichten-/Lastenheft

Kompetenz-/Schulungsmodul

2 Fahrzeug-Updates

- (F)-OTA-Architekturen
- Konzepte bezüglich SDV (Software Defined Vehicle) High level architecture
- SOTA vs. FOTA, OTA-Ansätze, Update-Szenarien, Update-Kampagnen
- Update-Strategien und -Methoden für Steuergeräte
- Management von (F)-OTA-Updates, UNECE R 156, ISO 24089
- Schnittstellen, Aktualisierungsprozesse, Dokumentationsanforderungen
- Fail-Safe-Strategien
- Cloud-Technologie und -dienste
- Backend-Systeme
- OTA-Cybersecurity inklusive Datenschutz (siehe auch Kategorie „Prozesse & Rahmenbedingungen“, Cluster „Cybersecurity“)
- Sichere Bootloader und -manager
- (F)-OTA-Testing
- Netzwerkprotokolle wie MQTT
- Transport- und Diagnose-Kommunikationsprotokolle wie CAN-TP, UDS, DoIP

Kompetenz-/Schulungsmodul

3 Wartung & Testing

- Entwicklung von Teststrategien zur langzeitlichen Software-Wartung
- Verifikationsmaßnahmen und -techniken
- Validierungsmaßnahmen und -techniken
- Einsatz von Regressionstests und Kompatibilitätstests
- Einrichtung langzeitlich wartungsfähiger Testumgebungen
- Testen von Software über Fahrzeuglebensdauer hinweg
- Anwendung von Traceability-Methoden (Anforderung → Test → Release)
- Nutzung von CI/CD zur Testautomatisierung
- Langzeitlicher Umgang mit Hardware-in-the-Loop (HiL) und Simulation
- Versions- und Variantentest (z. B. für unterschiedliche Fahrzeugkonfigurationen)
- SBOM-Management
- Pflege, Dokumentation und Archivierung von Testergebnissen, u.a. für Audits
- Zusammenarbeit mit Verantwortlichen für Architektur, Security und Projektleitung

Kompetenz-/Schulungsmodul

4 Kompatibilität & Modulare Bauweise

- Konzepte und Strategien zur Abwärts- und Aufwärtskompatibilität
- Entwicklung von Kompatibilitätsmatrizen
- Modularisierung von Softwarearchitekturen
- Schnittstellenmanagement (interne/externe APIs)
- Umgang mit Plattform- und Hardwarevarianten
- SBOM-Management
- Strategien zur Wiederverwendung bestehender Module
- Wartbarkeit von Software über mehrere Generationen
- Abhängigkeiten & Interoperabilität analysieren
- Integration von Sicherheitsmechanismen in modulare Architekturen
- Bewertung von Änderungseinflüssen auf Kompatibilität

Kompetenz-/Schulungsmodul

5 Prozesse & Rahmenbedingungen

- Grundlagen von FOSS-Management und Lizenzprüfung (z.B. FOSS-Lizenztypen und daraus resultierende rechtliche Rahmenbedingungen)
- SBOM-Management
- Relevante Normen und Standards (u.a. A-SPICE, ISO 21434, UNECE R155 / R156, …)
- Nachweisführung und Dokumentation im Produktlebenszyklus
- Traceability & Änderungsverfolgung über Softwareversionen
- Prozessintegration von Zulieferern (z. B. Releasefreigaben)
- Tools zur Konfigurations- und Release-Steuerung
- Rollenbasierte Prozessverantwortung (z. B. RASI, Prozessowner)

Kompetenz-/Schulungsmodul

6 Risikomanagement

- Einführung in technische und organisatorische Risikoarten
- Risikostrategien zum Umgang mit Risiken und deren Umsetzung
- Anwendung von TARA (Risikobewertung Gesamt = Beurteilung von Risiken hinsichtlich Wahrscheinlichkeit und Konsequenz, Konzentration auf wahrscheinliche und folgenschwere Risiken) im Softwarekontext
- Risikoabschätzung für Wartungs- und Updateprozesse
- Umgang mit sicherheitskritischen Abhängigkeiten (z. B. Drittcode)
- Einbezug rechtlicher Risiken (Produkthaftung, Updatepflichten)
- Planung und Dokumentation von Notfallmaßnahmen
- Aufbau eines Frühwarnsystems (technisch & organisatorisch)
- Risikoanalysen in der Lieferkette (Tier-N)
- Umgang mit Schwachstellenmanagement (CVE, Security Advisories)
- Integration von Risikomanagement in Projekt- und Produktentwicklung, auch bei IT-Systemen

Kompetenz-/Schulungsmodul

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

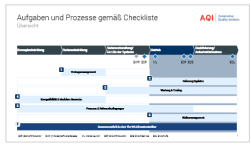
- Aufbau transparenter Kommunikationsstrukturen
- Weitergabe von Anforderungen und SBOM-Management entlang der Kette
- Vertragsgestaltung mit Lieferanten bzgl. Update- & Wartungspflichten
- Dokumentationspflichten und Nachweisführung bei Tier-1/2
- Standardisierung von Schnittstellen & Übergabedokumenten
- Steuerung von Drittanbietern und Service-Providern
- Schulung & Awareness bei externen Partnern
- Auditfähigkeit in der Lieferkette sicherstellen
- Eskalations- und Meldeketten im Fehlerfall
- Gemeinsame Lessons Learned und Qualitätsvereinbarungen

Zusammenfassung und Ergebnis

Mögliche Ausrichtung und Inhalte zur Sicherstellung von „Software-Langzeit-Qualität“ in Unternehmen

Checkliste mit
7 Hauptkategorien und
insgesamt 166 Prüfpunkten

Alle Prüfpunkte nach Verantwortlichkeit (RASI) und zeitlicher Einordnung bewertet

Prozesse		▪ Ableitung einer Prozesslandschaft zur Zusammenfassung der Kernaufgaben/ Prozesselemente gemäß Checkliste
Rollenprofile		▪ Definition einer Struktur und involvierter Organisationseinheiten zur Steuerung von Software-Langzeitqualität
Verantwortlichkeiten		▪ RACI-Matrix zur Zuweisung der Zuständigkeiten entlang der 7 Checklisten-Kategorien
Schulungsmodule		▪ Definition von sieben Rollen inkl. Kernaufgaben und Kompetenzen ▪ Ableitung von Kompetenz-/Schulungsmodulen basierend auf den Kategorien der Checkliste

Ergebnis

Das Konzept zur Software-Langzeitqualität umfasst eine rollenbasierte Verankerung, definierte Prozesse entlang regulatorischer Anforderungen, verbindliche Verantwortlichkeiten sowie rollenbasierte Schulungsmodule zur nachhaltigen Kompetenzsicherung

Orientierung für Unternehmen zur Individuellen Umsetzung

Agenda

AQI Automotive Quality Institute

Projektbeschreibung der Vorgehensweise

Projektinhalte

Checklistenbezug – Zeitliche Einordnung und Verantwortlichkeiten

Checkliste zur Sicherstellung der Langzeitqualität von Software-intensiven Systemen

AQI Automotive Quality Institute

1 Vertragsmanagement

- Wartungsverträge
- Zeiträume
- Gewährleistung und Haftung
- Standarddokumente (z.B. AGBs)
- Zugriffsabsicherung

2 Fahrzeug-Updates

- (F)OTA-Fähigkeit und Schnittstellen
- Sicherheits- und Funktions-anforderungen

3 Wartung & Testing

- Teststrategien
- Entwicklungs- und Testumgebungen
- Verfügbarkeiten
- Wissensmanagement

4 Kompatibilität & Modulare Bauweise

- Kompatibilitätsstrategie
- Modulares Design

5 Prozesse & Rahmenbedingungen

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

6 Risikomanagement

- Risikobewertung und -absicherung
- Notfall- und Krisenmanagement
- Rechtliche Rahmen-bedingungen und Stand der Technik
- Störungs- und Endkundenverhalten

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

- Kollaborationsmodelle (bzg (F)OTA, Testing etc.)
- Zusammenarbeit mit Unterlieferanten
- Dokumentation (S-/C-BOM)

1 Vertragsmanagement

AQI Automotive Quality Institute

1.1 **Wartungsverträge:** Klare Definition und Festlegung von Wartungsverträgen zur Sicherstellung der kontinuierlichen Softwarequalität.

1.2 **Zeiträume:** Bestimmung der Zeiträume im Projekt, um eine langfristige Pflege und Aktualisierung der Software zu gewährleisten.

1.3 **Gewährleistung und Haftung:** Vereinbarungen zu Gewährleistung und Haftung, um Verantwortlichkeiten im Fehlerfall klar zu regeln.

1.4 **Standarddokumente:** Verwendung standardisierter Dokumente, wie z.B. AGBs, um einheitliche Vertragsgrundlagen zu schaffen.

1.5 **Zugriffsabsicherung:** Implementierung von Maßnahmen wie Escrow-Vereinbarungen, um den langfristigen Zugriff auf Software und Quellcode sicherzustellen.

1 Vertragsmanagement

1.1 Wartungsverträge (1/2)

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Vertragsumfang ist klar definiert: Der Umfang der Wartungsverträge ist detailliert festgelegt, einschließlich aller unterstützten Softwaremodule, Versionen und Hardware-Komponenten.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Verantwortlichkeiten sind eindeutig zugewiesen: Die Verantwortlichkeiten für alle beteiligten Parteien, einschließlich der Zuständigkeiten für Updates, Analyse, Bugfixes und Support, sind klar festgelegt.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Reaktionszeiten sind verbindlich festgelegt: Verbindliche Reaktionszeiten für die Bearbeitung von Support-Anfragen und die Behebung von Fehlern sind im Vertrag verankert.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Leistungskennzahlen (KPIs) sind vereinbart: KPIs für die Wartungsleistungen sind definiert, um die Servicequalität regelmäßig zu überwachen und zu bewerten.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Laufzeiten und Verlängerungsoptionen sind bestimmt: Die Laufzeit des Wartungsvertrags sowie Optionen und Bedingungen für Vertragsverlängerungen sind klar geregelt.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Eskalationsprozesse sind festgelegt: Eskalationsstufen und -verfahren im Falle von Streitigkeiten oder bei Nichteinhaltung der vertraglichen Verpflichtungen sind definiert.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Eine Abgrenzung zwischen Fehlerbehebung, Implementierung von neuen Funktionen und Cybersecurity ist vertraglich erfolgt: Die Abgrenzung „Fehlerbehebung (Bug Fix)“, „Implementierung neuer Funktionen“ und „Cybersecurity-Maßnahmen“ ist definiert, um etwaige Unterschiede in der Leistungserbringung zu regeln.		x				R: SW-PM A: S: : SW-A I: Einkauf	SW-PM
Die Implementierung eines Wartungsteams mit entsprechender Kompetenz ist vertraglich geregelt: Die Implementierung eines Wartungsteams mit den notwendigen technischen Kompetenzen und regelmäßiger Schulungen ist vertraglich geregelt.		x				R: SW-PM A: S: SW-A I: Einkauf	SW-PM

1 Vertragsmanagement

1.1 Wartungsverträge (2/2)

AQI Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Kostenstruktur ist transparent gestaltet: Eine transparente und nachvollziehbare Kostenstruktur für alle Wartungsleistungen, einschließlich regelmäßiger Updates und Anpassungen, ist erstellt.		x				R: Einkauf A: SW-PM S: TV-Ing I:	Einkauf
Datensicherheitsanforderungen sind integriert: Anforderungen an die Datensicherheit und den Schutz vertraulicher Informationen im Rahmen der Wartungsleistungen sind definiert und implementiert.		x				R: SW-PM A: S: Security I: Einkauf	SW-PM
Dokumentationspflichten sind verbindlich festgelegt: Verbindliche Anforderungen an die Dokumentation aller durchgeführten Wartungsarbeiten und Änderungen sind festgelegt, um die Nachvollziehbarkeit sicherzustellen.		x				R: SW-PM A: S: TV-Ing I: Einkauf	SW-PM
Regelmäßige Überprüfung und Anpassung sind vereinbart: Es ist vereinbart, dass der Wartungsvertrag regelmäßig überprüft und bei Bedarf an neue technische oder regulatorische Anforderungen angepasst wird.		x				R: SW-PM A: S: TV-Ing I: JUR	SW-PM

1 Vertragsmanagement

1.2 Zeiträume

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Zeiträume für die Entwicklungs- und die Wartungsphase sind klar definiert: Die Lebensdauer eines Softwareprodukts ist in die Entwicklungsphase und die Wartungsphase unterteilt, und diese Zeiträume sind im Wartungsvertrag eindeutig festgelegt.		x				R: SW-PM A: S: TV-Ing, SW-A I: JUR	SW-PM
End-of-Production (EOP) und End-of-Service (EOS) sind eindeutig bestimmt: EOP und EOS, wie z.B. 15 Jahre nach Produktionsende, sind klar mit festen Daten versehen und in den Wartungsverträgen berücksichtigt.		x				R: SW-PM A: S: TV-Ing, SW-A I: JUR	SW-PM
Wartungszeiträume umfassen den gesamten Produktlebenszyklus: Die definierten Wartungszeiträume decken den gesamten Lebenszyklus ab, einschließlich der Nachbetreuung in der Wartungsphase.		x				R: SW-PM A: S: TV-Ing, SW-A I: JUR	SW-PM
Modellpflege- und Produktaufwertungszyklen sind festgelegt: Die Zyklen für Modellpflege, Produktaufwertung und Software-Upgrades sind klar definiert und an die Wartungsphasen angepasst.		x				R: SW-PM A: S: TV-Ing, SW-A I: Einkauf	SW-PM
Haftungszeiträume sind über die gesamte Lieferkette geregelt: Die Haftungszeiträume sind transparent und über die gesamte Zulieferkette hinweg klar geregelt und vertraglich verankert.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Anpassungen bei Änderungen des Produktzyklus sind berücksichtigt: Falls sich der Produktzyklus oder die Produktionsdauer ändern, sind die Wartungsverträge flexibel genug, um diese Änderungen zu berücksichtigen.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Alle beteiligten Parteien sind über die Zeiträume informiert: Die festgelegten Wartungszeiträume und deren Konsequenzen sind allen Vertragspartnern und Beteiligten in der Zulieferkette transparent kommuniziert.		x				R: SW-PM A: S: TV-Ing, SW-A I: JUR	SW-PM

1 Vertragsmanagement

1.3 Gewährleistung und Haftung

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Maximale Haftungsbegrenzung (Haftungscap) ist festgelegt: Die Haftung für Schäden ist auf eine maximale Summe in Form von einer Haftungsgrenze begrenzt, z.B. das Zweifache der Entwicklungskosten bei rein softwarebasierten Lösungen.		x				R: Einkauf A: S: JUR I: SW-PM	Einkauf
Haftungsrisiken sind umfassend analysiert: Alle potenziellen Haftungsrisiken wurden identifiziert und im Vertrag berücksichtigt, um unerwartete Kosten zu minimieren.		x				R: Einkauf A: S: JUR, SW-E I:SW-PM	Einkauf
Vertragsstrafen bei Nichterfüllung sind definiert: Es sind klare Vertragsstrafen vorgesehen, falls die vertraglich festgelegten Gewährleistungs- oder Haftungsbedingungen nicht eingehalten werden.		x				R: Einkauf A: JUR S: I: SW-PM	Einkauf
Haftungsgrenzen sind auf Zulieferer abgestimmt: Die festgelegten Haftungsgrenzen sind über die gesamte Lieferkette hinweg konsistent und mit den Zulieferern abgestimmt.		x				R: Einkauf A: S: JUR I: SW-PM	Einkauf
Rückgriffsansprüche sind klar geregelt: Die Bedingungen für Rückgriffsansprüche im Falle von Mängeln oder Schäden sind eindeutig festgelegt und vertraglich abgesichert.		x				R: JUR A: S: SW-PM I: Einkauf	JUR
Kommunikation der Haftungsbedingungen ist gewährleistet: Alle relevanten Parteien in der Lieferkette sind über die festgelegten Haftungs- und Gewährleistungsbedingungen informiert und verstehen ihre Verpflichtungen.		x				R: SW-PM, Einkauf A: S: Einkauf I:	SW-PM, Einkauf
Der Gewährleistungszeitraum ist über die gesamte Produktlebensdauer definiert: Der Gewährleistungszeitraum ist so festgelegt, dass die gesamte Lebensdauer des Produkts einschließlich der Nachproduktionsphase betrachtet wurde und Teile aktiv ein- oder ausgeschlossen sind.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM

1 Vertragsmanagement

1.4 Standarddokumente

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Verwendung standardisierter Vertragsvorlagen ist sichergestellt: Alle Verträge und Vereinbarungen basieren auf einheitlichen, standardisierten Dokumentvorlagen, um Konsistenz und Rechtssicherheit zu gewährleisten.		x				R: JUR A: S: Einkauf I: SW-PM	JUR
Zugänglichkeit der Standarddokumente ist gewährleistet: Standarddokumente sind für alle relevanten Parteien leicht zugänglich, entweder über ein zentrales Dokumentenmanagementsystem oder eine andere vereinbarte Plattform.		x				R: Einkauf, SW-PM A: S: I: JUR	Einkauf, SW-PM
Konsistenz über die Lieferkette ist sichergestellt: Die Verwendung von Standarddokumenten ist über die gesamte Lieferkette hinweg durchgesetzt, um einheitliche Bedingungen und Vorgehensweisen sicherzustellen.		x				R: Einkauf A: S: I: JUR	Einkauf
Die Standarddokumente beinhalten rechtliche Anforderungen an Datenschutz, Haftung und Vertraulichkeit: Alle rechtlich relevanten Klauseln, einschließlich Datenschutz, Haftung und Vertraulichkeit, sind in den Standarddokumenten umfassend abgedeckt.		x				R: JUR A: S: Einkauf I: SW-PM	JUR
Relevante AGB sind allen Parteien bekannt und zugänglich: Alle relevanten Allgemeinen Geschäftsbedingungen (AGB) sind eindeutig dokumentiert, allen beteiligten Parteien bekannt und jederzeit zugänglich gemacht.		x				R: Einkauf A: S: SW-PM I: JUR	Einkauf
Archivierung und Versionierung sind gewährleistet: Alle Versionen der Standarddokumente werden revisionssicher archiviert, um eine lückenlose Nachvollziehbarkeit und historische Überprüfung zu ermöglichen.		x				R: Einkauf A: S: SW-PM I: JUR	Einkauf

1 Vertragsmanagement

1.5 Zugriffsabsicherung (1/2)

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetriebnahme		
Zugriff auf Quellcode und Dokumentation ist abgesichert: Der Zugriff für den Kunden auf den Quellcode und die zugehörige Dokumentation der Software ist eindeutig festgelegt und vertraglich abgesichert.		x				R: SW-PM A: S: JUR I: Einkauf	SW-PM
Escrow-Verträge sind abgeschlossen: Im Falle einer Insolvenz oder eines anderen kritischen Ereignisses sind Escrow-Verträge vorhanden, die den Zugang zu allen notwendigen Softwarekomponenten und Dokumentationen sicherstellen.		x				R: Einkauf A: S: SW-PM I:	Einkauf
Due-Diligence-Prüfungen sind durchgeführt: Eine umfassende Due-Diligence der einzelnen Anbieter und Unterlieferanten ist erfolgt, um die Qualität und Zuverlässigkeit der Lieferanten zu gewährleisten, einschließlich der Prüfung von Multi-Vendor-Lösungen.		x				R: Einkauf A: S: SW-PM I:	Einkauf
Code-Generierung ist umfassend geplant: liche erforderliche Engineering-Artefakte für die Code-Generierung sind identifiziert, um sicherzustellen, dass alle notwendigen Modelle korrekt in Code umgesetzt werden können.		x				R: SW-A A: S: SW-PM I:	SW-A
Serienreleases sind an den Treuhändler übergeben: Es ist sichergestellt, dass alle Serienreleases, einschließlich derjenigen vor besonderen Ereignissen wie Insolvenzen, an den Treuhändler übergeben werden, gemäß den Escrow-Verträgen.		x				R: SW-PM A: S: SW-A I: Einkauf	SW-PM
Klarheit über Multi-Vendor-Strategien ist gewährleistet: Die Strategie zur Nutzung von Multi-Vendor-Lösungen ist klar definiert und berücksichtigt, um die Abhängigkeit von einem einzelnen Anbieter zu minimieren und die Zugriffsabsicherung zu verstärken.		x				R: Einkauf A: S: SW-PM I:	Einkauf
Regelmäßige Überprüfung der Escrow-Vereinbarungen ist implementiert: Escrow-Vereinbarungen werden regelmäßig überprüft und bei Bedarf angepasst, um sicherzustellen, dass sie den aktuellen Anforderungen entsprechen.		x				R: Einkauf A: S: JUR I:	Einkauf
Zugriffsrechte sind transparent geregelt: Alle Zugriffsrechte auf den Quellcode, Dokumentation und sonstige kritische Softwarekomponenten sind transparent dokumentiert und für alle relevanten Parteien nachvollziehbar.		x				R: SW-PM A: S: Einkauf, SW-A I:	SW-PM

1 Vertragsmanagement

1.5 Zugriffsabsicherung (2/2)

Prüfpunkte

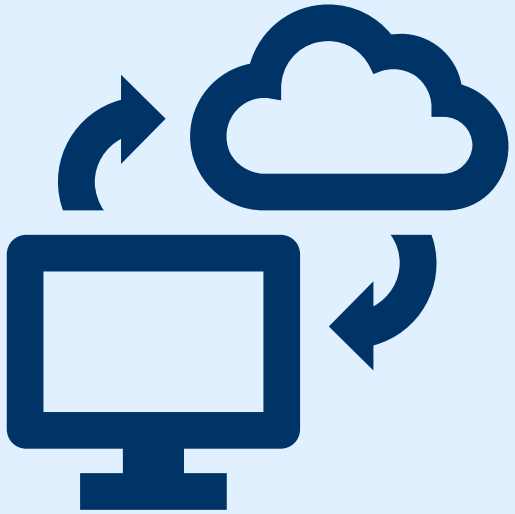
	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Notfallpläne für den Zugriff auf Software sind vorhanden: Es sind Notfallpläne implementiert, die den sofortigen Zugang zu wichtigen Softwarekomponenten und Dokumentationen sicherstellen, falls ein Anbieter ausfällt oder insolvent wird.		x				R: SW-PM A: S: SW-A I: Einkauf	SW-PM

2 Fahrzeug-Updates

AQI Automotive Quality Institute

2.1 (F)OTA-Fähigkeit und Schnittstellen: Sicherstellung der technischen Voraussetzungen und Schnittstellen für zuverlässige Over-the-Air-Updates.

2.2 Sicherheits- und Funktionsanforderungen: Umsetzung von Sicherheitsstandards und Funktionsanforderungen, um die Integrität und Zuverlässigkeit von (F)OTA-Updates zu gewährleisten.



2 Fahrzeug-Updates

2.1 (F)OTA-Fähigkeit und Schnittstellen (1/2)

AQI | Automotive Quality Institute

Prüfpunkte

Prüfpunkte	Wann? Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme	Wer?	Wer muss geschult werden?
Verantwortungsbereich ist klar definiert: Der Zugriff und der Einfluss des Zulieferers auf (F)OTA-Updates sind im Wartungsvertrag klar festgelegt und dokumentiert.		x				R: SW-PM A: S: JUR Einkauf I:	SW-PM
Befähigung der relevanten Steuergeräte ist im Design berücksichtigt: Die Fähigkeit der Steuergeräte, (F)OTA-Updates zu unterstützen, wurde bereits im Designprozess berücksichtigt und ist in der Zusammenarbeit zwischen OEM und Zulieferer eindeutig bestimmt.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Schnittstellen sind standardisiert: Die Schnittstellen für (F)OTA-Updates sind projektübergreifend sowohl für den OEM als auch für den Zulieferer vereinheitlicht und standardisiert.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Prozesse für (F)OTA-Updates sind vereinheitlicht: Alle relevanten Prozesse für die Durchführung von (F)OTA-Updates sind klar definiert und über alle Projektbeteiligten hinweg konsistent implementiert.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Dokumentationsstrategie ist klar beschrieben: Eine klare Dokumentationsstrategie ist implementiert, die alle Aspekte der (F)OTA-Updates abdeckt, einschließlich der Beschreibung und Nachverfolgbarkeit des Update-Status.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Update-Strategie ist transparent: Die Strategie für die Durchführung von Updates ist transparent und für alle Beteiligten nachvollziehbar, einschließlich der Festlegung von Prioritäten und Zeitplänen.		x	x			R: SW-PM A: S: SW-A I:	SW-PM
Variantenmanagement ist berücksichtigt: Varianten und Updates sind aufeinander abgestimmt, damit potentiell alle Fahrzeuge erreicht werden können und Softwarevarianten gezielt und effizient aktualisiert werden können.		x	x	x		R: SW-A A: S: SW-PM I:	SW-A
Kommunikation zwischen OEM und Zulieferer ist sichergestellt: Die Kommunikation über (F)OTA-Updates zwischen OEM und Zulieferer ist klar geregelt, um eine reibungslose Koordination und Umsetzung der Updates zu gewährleisten.		x	x			R: SW-PM A: S: SW-A I:	SW-PM

2 Fahrzeug-Updates

2.1 (F)OTA-Fähigkeit und Schnittstellen (2/2)

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Durchgängigkeit der (F)OTA-Prozesse ist gewährleistet: Die Prozesse für (F)OTA-Updates sind durchgängig und ohne Brüche gestaltet, um eine konsistente und zuverlässige Durchführung der Updates sicherzustellen.	x	x				R: SW-A A: S: I: SW-PM	SW-A
KPIs für (F)OTA-Updates sind definiert: Wichtige Leistungskennzahlen (KPIs) für die Durchführung von (F)OTA-Updates sind festgelegt, um die Effizienz und Qualität der Updates kontinuierlich zu überwachen und zu bewerten.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Teststrategien für Schnittstellen sind etabliert: Klare Teststrategien sind für alle (F)OTA-Schnittstellen etabliert, um sicherzustellen, dass diese vor dem Rollout von Updates umfassend validiert werden.		x	x			R: TV-Ing A: S: SW-A I: SW-PM	TV-Ing

2 Fahrzeug-Updates

2.2 Sicherheits- und Funktionsanforderungen (1/2)

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Der (F)OTA-Prozess ist klar definiert: Der gesamte (F)OTA-Prozess ist klar definiert, einschließlich der Sicherheits- und Funktionsanforderungen, die während der Durchführung eines Updates eingehalten werden müssen.	x	x				R: SW-A A: S: Security I: SW-PM	SW-A
Ein abgesichertes Einspielen der (F)OTA-Updates ist gewährleistet: Der (F)OTA-Updateprozess ist durch robuste Sicherheitsmechanismen abgesichert, um unautorisierte Zugriffe oder Manipulationen im Übertragungsprozess zu verhindern.		x	x	x		R: Security A: S: SW-A I: SW-PM	Security
Prozessrate für (F)OTA-Updates ist optimiert: Die Prozessrate, d.h. die Geschwindigkeit und Effizienz, mit der (F)OTA-Updates durchgeführt werden, ist optimiert und stellt sicher, dass Updates in einem akzeptablen Zeitrahmen erfolgen.		x	x	x		R: SW-A A: S: SW-PM I:	SW-A
Verification & Validation (V&V) ist umfassend durchgeführt: Vor jedem (F)OTA-Update werden umfassende Verification & Validation (V&V)-Prozesse durchgeführt, um sicherzustellen, dass die Updates den festgelegten Sicherheits- und Funktionsanforderungen entsprechen.		x	x	x		R: TV-Ing A: S: SW-A I: SW-PM	TV-Ing
Datenschutzrichtlinien sind implementiert: Strenge Datenschutzrichtlinien sind implementiert, um sicherzustellen, dass personenbezogene und sicherheitsrelevante Daten während des (F)OTA-Prozesses geschützt bleiben.		x	x	x		R: Security A: S: SW-PM I:	Security
Sicherheitsstandards sind eingehalten: Alle (F)OTA-Updates erfüllen die festgelegten Sicherheitsstandards und regulatorischen Anforderungen, um die Integrität und Sicherheit der Fahrzeugsoftware zu gewährleisten.		x	x	x		R: Security A: S: SW-PM I:	Security
Sicherheitsaspekte sind in den Schnittstellen berücksichtigt: Alle Schnittstellen für (F)OTA-Updates sind so gestaltet, dass sie den höchsten Sicherheitsanforderungen entsprechen, um unautorisierten Zugriff zu verhindern.	x	x				R: SW-A A:Security S: SW-PM I: QM	SW-A
Regelmäßige Sicherheitsbewertungen sind vorgesehen: Es sind regelmäßige Sicherheitsbewertungen geplant, um potenzielle Schwachstellen in den (F)OTA-Prozessen frühzeitig zu erkennen und zu beheben.		x	x	x		R: Security A: S: SW-A I: QM	Security

2 Fahrzeug-Updates

2.2 Sicherheits- und Funktionsanforderungen (2/2)

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Sicherheitsprotokolle werden kontinuierlich überwacht: Alle sicherheitsrelevanten Protokolle und Logs werden kontinuierlich überwacht, um Anomalien oder sicherheitskritische Ereignisse sofort zu erkennen.		x	x			R: SW-PM A: S: Security I:	SW-PM
Vorkehrungen für den Datenschutz sind getroffen: Spezielle Vorkehrungen sind getroffen, um sicherzustellen, dass alle (F)OTA-Updates datenschutzkonform durchgeführt werden und keine sensiblen Informationen preisgegeben werden.	x	x	x	x		R: Security A: S: SW-PM, SW-A I: QM	Security

3 Wartung & Testing

AQI Automotive Quality Institute

3.1 **Teststrategien:** Entwicklung und Implementierung klarer Teststrategien, um die Softwarequalität kontinuierlich zu überwachen und zu sichern.

3.2 **Entwicklungs- und Testumgebungen:** Bereitstellung und Wartung von Entwicklungs- und Testumgebungen, die für die Software-Entwicklung sowie regelmäßige und umfassende Softwaretests notwendig sind.

3.3 **Verfügbarkeiten:** Sicherstellung der langfristigen Verfügbarkeit von Tools und Infrastruktur, um den gesamten Produktlebenszyklus abzudecken.

3.4 **Wissensmanagement:** Implementierung eines Wissensmanagements zur Sicherstellung der langfristigen Verfügbarkeit und Weitergabe von Fachwissen.

3 Wartung & Testing

3.1 Teststrategien (1/2)

Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Teststrategien und -umgebungen sind festgelegt und transparent: Alle Teststrategien sowie die entsprechenden Testumgebungen, einschließlich der „Lagerung“ der Testdaten, sind festgelegt und für alle Beteiligten klar und nachvollziehbar geregelt.		x	x			R: TV-Ing A: S: I: SW-PM	TV-Ing
Vertragliche Regelungen zur Analyse- und Updatefähigkeit sind definiert: Klare vertragliche Regelungen zur Analyse- und Updatefähigkeit der Software, einschließlich festgelegter Zeiträume, sind implementiert.		x				R: SW-PM, Einkauf A: S: TV-Ing I:	SW-PM, Einkauf
Teststrategien für (F)OTA-Schnittstellen sind etabliert: Klare Teststrategien für alle (F)OTA-Schnittstellen sind festgelegt, um sicherzustellen, dass diese umfassend validiert werden, bevor Updates ausgerollt werden.			x			R: TV-Ing A: S: I: SW-PM	TV-Ing
Abstimmung der Teststrategien zwischen allen Partnern in der Lieferkette: Es besteht eine klare Abstimmung zwischen allen Partnern, welche Änderungen welche Tests erfordern, einschließlich der Unterscheidung zwischen Bug-Fix-Verifizierung und Regressionstests.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
Testzeitraum entspricht dem Wartungszeitraum: Die Testfähigkeit der Software wird über den gesamten Wartungszeitraum hinweg sichergestellt, um kontinuierliche Qualität und Zuverlässigkeit zu gewährleisten.			x	x		R: SW-PM A: S: TV-Ing I:	SW-PM
Technologieakzeptanz ist in der Lieferkette geklärt: Die Akzeptanz der verwendeten Testtechnologien ist zwischen allen Partnern geklärt, insbesondere im Hinblick auf die Behandlung unvollständiger Anforderungen.		x				R: SW-PM A: S: TV-Ing I:	SW-PM
State-of-the-Art wird sichergestellt: Die eingesetzten Testsysteme und Modelle werden regelmäßig überprüft und an aktuelle Standards und Technologien angepasst, um den State-of-the-Art zu gewährleisten.		x	x	x		R: TV-Ing A: S: I: SW-PM	TV-Ing
Spezifische Testprozesse nach SOP sind vorhanden: Nach der SOP existieren spezifische Testprozesse, die entweder aus dem Entwicklungsprozess übernommen oder entsprechend angepasst wurden, um die Anforderungen in der Serienproduktion zu erfüllen.			x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Wartung & Testing

3.1 Teststrategien (2/2)

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Änderungen und Testanforderungen sind abgestimmt: Alle Änderungen an der Software und die daraus resultierenden Testanforderungen sind zwischen den beteiligten Partnern klar abgestimmt, um eine reibungslose Integration in den Testprozess zu gewährleisten.				x		R: TV-Ing A: S: SW-PM I:	TV-Ing
Kontinuität der Tests ist gewährleistet: Die Kontinuität der Testprozesse wird über den gesamten Produktlebenszyklus hinweg gewährleistet, um die dauerhafte Einhaltung aller Qualitätsstandards zu sichern.				x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Wartung & Testing

3.2 Entwicklungs- und Testumgebungen

AQI Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetriebnahme		
Tools und Umgebungen sind strategisch geplant: Es ist sichergestellt, dass Entwicklungs- und Testtools sowie deren Umgebungen strategisch geplant und über die Jahre hinweg sinnvoll genutzt werden, wobei eine kontinuierliche Überprüfung und Anpassung erfolgt, um veraltete Systeme zu vermeiden.	x	x	x	x		R: TV-Ing A: S: SW-A, SW-PM I:	TV-Ing
Langfristige Verfügbarkeit der Toolchain ist gewährleistet: Die Build- und Test-Toolchain wird über die festgelegten Zeiträume hinweg aufrechterhalten, um die kontinuierliche Testfähigkeit während des gesamten Produktlebenszyklus sicherzustellen.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
Entwicklungs- und Testumgebungen sind für zukünftige Anforderungen flexibel und skalierbar: Die Testumgebungen sind so gestaltet, dass sie flexibel an verschiedene Anforderungen angepasst werden können und skalierbar sind, um auch zukünftige Testanforderungen zu erfüllen, die zum SOP noch nicht bekannt waren.	x	x	x	x		R: TV-Ing A: S: SW-A, SW-PM I:	TV-Ing
Verantwortlichkeiten für Entwicklungs- und Testumgebungen in der gesamten Lieferkette sind zugewiesen: Die Verantwortlichkeiten für die Wartung, Aktualisierung und den Betrieb der Entwicklungs- und Testumgebungen sind klar in der gesamten Lieferkette über den Einsatzzeitraum bis EOS zugewiesen und in den Verträgen verankert.		x	x	x		R: SW-PM A: S: TV-Ing I:	SW-PM
Technologische Aktualität der Entwicklungs- und Testumgebungen wird sichergestellt: Es wird regelmäßig überprüft, ob die Entwicklungs- und Testumgebungen technologisch auf dem neuesten Stand sind, um eine State-of-the-Art-Testdurchführung zu gewährleisten.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
Anpassung der Entwicklungs- und Testumgebungen erfolgt regelmäßig: Eine regelmäßige Anpassung der Entwicklungs- und Testumgebungen wird, wenn nötig, durchgeführt, um sicherzustellen, dass sie den aktuellen und zukünftigen Anforderungen gerecht werden.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Wartung & Testing

3.3 Verfügbarkeiten

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Langfristige Verfügbarkeit der Testumgebungen ist sichergestellt: Es ist gewährleistet, dass alle notwendigen Testumgebungen über den gesamten Produktlebenszyklus hinweg verfügbar bleiben und bei Bedarf aktualisiert oder ersetzt werden, um kontinuierliche Tests und die Testfähigkeit aufrechtzuerhalten.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing
Redundanz bei Testtools und Umgebungen ist eingeplant: Es ist eine Redundanzstrategie implementiert, um alternative Testtools und Umgebungen bereitzuhalten, falls Primärressourcen ausfallen.	x	x	x	x		R: TV-Ing A: S: SW-PM, SW-A I:	TV-Ing
Verfügbarkeit von Testpersonal ist geplant: Die Verfügbarkeit von qualifiziertem Testpersonal ist über den gesamten Test- und Wartungszeitraum hinweg sichergestellt, einschließlich Schulungen und Ressourcenplanung.		x	x	x		R: SW-PM A: S: TV-Ing I:	SW-PM
Kapazitätsplanung für Testressourcen ist in der gesamten Lieferkette bis EOS durchgeführt: Eine gründliche Kapazitätsplanung stellt sicher, dass ausreichend Testressourcen und -kapazitäten für alle geplanten Tests vorhanden sind, insbesondere in Spitzenzeiten und nach Ende der Produktion (EOP) oder des Service (EOS).		x	x			R: SW-PM A: S: TV-Ing I:	SW-PM
Regelmäßige Überprüfung der Funktionsfähigkeit: Die Funktionsfähigkeit aller Testressourcen wird regelmäßig überprüft, und Anpassungen werden vorgenommen, um auf Änderungen in den Anforderungen oder der Technologie schnell reagieren zu können.		x	x	x		R: TV-Ing A: S: SW-PM I:	TV-Ing

3 Wartung & Testing

3.4 Wissensmanagement

AQI | Automotive Quality Institute

Prüfpunkte

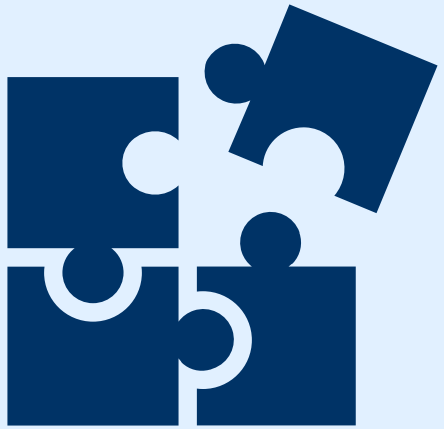
	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Systematische Dokumentation ist implementiert: Alle relevanten Informationen, Prozesse und Erfahrungen werden systematisch dokumentiert und in einem zentralen Wissensmanagementsystem gespeichert, um den Zugang für alle Beteiligten zu gewährleisten.		x	x	x		R: SW-PM A: S: SW-A I: Alle	SW-PM
Wissenstransfer ist sichergestellt: Ein formalisierter Prozess für den Wissenstransfer zwischen Mitarbeitern, Teams und über den gesamten Produktlebenszyklus hinweg ist etabliert, um den Erhalt von kritischem Know-how sicherzustellen.		x	x	x		R: SW-PM A: S: SW-A I: Alle	SW-PM
Schulungskonzept für den langfristigen Technologieeinsatz ist vorgesehen: Es werden regelmäßige Schulungen und Workshops geplant, um sicherzustellen, dass das Wissen aktuell bleibt, neue Erkenntnisse kontinuierlich integriert werden und das Know-How bei langfristigem Technologieeinsatz erhalten bleibt.	x	x	x	x	x	R: SW-PM A: S: Alle I: QM	SW-PM, R: Alle
Wissensmanagementsystem ist zugänglich und benutzerfreundlich: Das Wissensmanagementsystem ist für alle relevanten Mitarbeiter leicht zugänglich und benutzerfreundlich gestaltet, um eine effektive Nutzung zu fördern.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
Erfahrungen und Best Practices werden regelmäßig aktualisiert: Erfahrungen und Best Practices aus der täglichen Arbeit und abgeschlossenen Projekten werden regelmäßig gesammelt, ausgewertet und im Wissensmanagementsystem aktualisiert.		x	x	x		R: SW-PM A: S: Alle I:	SW-PM
Verantwortlichkeiten für Wissensmanagement sind festgelegt: Es sind klare Verantwortlichkeiten für die Pflege und Aktualisierung des Wissensmanagementsystems zugewiesen, um dessen kontinuierliche Relevanz und Aktualität sicherzustellen.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
Wissen ist über die gesamte Lieferkette hinweg integriert: Das Wissensmanagement umfasst nicht nur interne Informationen, sondern auch Wissen aus der gesamten Lieferkette, um eine umfassende Sicht auf alle relevanten Prozesse und Technologien zu gewährleisten.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
Softwarewartungsbericht ist veröffentlicht: Ein Softwarewartungsbericht mit Betriebszustand des Systems, Inspektions- und Testergebnisse, Softwareänderungen, statistische Analysen von Fehlern und Optimierungsvorschläge etc. wird erstellt und transparent gemacht		x	x	x		R: SW-PM A: S: TV-Ing I: QM	SW-PM

4 Kompatibilität & Modulare Bauweise

AQI | Automotive Quality Institute

4.1 **Kompatibilitätsstrategie:** Sicherstellung der Abwärts- und Aufwärtskompatibilität von Software und Hardware über die gesamte Lebensdauer.

4.2 **Modulares Design:** Förderung einer modularen Softwarearchitektur, die Wartung und Erweiterung erleichtert.



4 Kompatibilität & Modulare Bauweise

4.1 Kompatibilitätsstrategie

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Kompatibilitätsstrategie über die gesamte Lieferkette ist festgelegt: Eine umfassende Kompatibilitätsstrategie, die alle Ebenen der Lieferkette einschließt, ist definiert und stellt sicher, dass sowohl Abwärts- als auch Aufwärtskompatibilität über alle Lieferanten hinweg gewährleistet ist.	x					R: SW-A A: S: SW-PM I:	SW-A
Abwärtskompatibilität ist sichergestellt: Die Abwärtskompatibilität der Software und Hardware ist strategisch berücksichtigt und implementiert, um sicherzustellen, dass neue Komponenten mit älteren Systemen kompatibel sind.	x					R: SW-A A: S: SW-PM I:	vorgeschriebener Prozess
Aufwärtskompatibilität der Hardware ist eingeplant: Die Strategie zur Aufwärtskompatibilität der Hardware berücksichtigt zukünftige Anforderungen und enthält Maßnahmen zur Überdimensionierung der Hardware, um spätere Upgrades zu erleichtern.	x					R: SW-A A: S: SW-PM I:	vorgeschriebener Prozess
Wirtschaftlichkeitsrechnung für Abwärts-/Aufwärtskompatibilität ist erstellt: Eine detaillierte Wirtschaftlichkeitsrechnung zur Bewertung der Kosten und Nutzen der Abwärts- und Aufwärtskompatibilität ist durchgeführt und berücksichtigt im strategischen Entscheidungsprozess.	x	x				R: SW-A A: S: SW-PM, Einkauf I:	vorgeschriebener Prozess
Regelmäßige Kompatibilitätsprüfungen sind eingeplant: Es sind regelmäßige Überprüfungen und Tests vorgesehen, um sicherzustellen, dass die Kompatibilitätsstrategie über den gesamten Produktlebenszyklus hinweg eingehalten wird.		x	x	x	x	R: SW-PM A: S: TV-Ing I:	SW-PM
Dokumentation der Kompatibilitätsanforderungen ist für die Lieferkette transparent: Alle Kompatibilitätsanforderungen sind umfassend dokumentiert und für alle Beteiligten in der Lieferkette zugänglich, um Missverständnisse zu vermeiden.		x				R: SW-PM A: S: Einkauf I:	SW-PM
Langfristige Unterstützung älterer Systeme ist gewährleistet: Die Strategie beinhaltet die langfristige Unterstützung und Wartung älterer Systeme, um eine nachhaltige Nutzung der bestehenden Infrastruktur zu ermöglichen.	x	x	x	x	x	R: SW-A A: S: SW-PM I:	SW-A
Software-basierte Realisierung von Funktionen wird bevorzugt: Funktionen werden, nach Abwägung der langfristigen Wartbarkeit und Kosten, bevorzugt in Software statt in Hardware realisiert, um auf technologische Änderungen (z. B. Mobilfunkabschaltungen) flexibel und ohne bzw. mit geringer Hardwareanpassung reagieren zu können.	x	x				R: SW-A A: S: SW-PM, Einkauf I:	SW-A

4 Kompatibilität & Modulare Bauweise

4.2 Modulares Design

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Modulares Design zur Beherrschung der Komplexität ist implementiert: Ein modulares Design ist eingeführt, um die Komplexität des Systems zu beherrschen und eine flexible Anpassung an zukünftige Anforderungen zu ermöglichen.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Strategie zur Abschaltbarkeit von Funktionen und Komponenten ist festgelegt: Es wurde eine klare Strategie entwickelt, die es ermöglicht, Funktionen und Komponenten, die bei der Nutzung des Fahrzeugs relevant sind, bei Bedarf abzuschalten, um Ressourcen zu schonen und die Systemstabilität zu erhöhen.	x	x				R: SW-A A: S: SW-PM I:	SW-A
„Upgradeability of Hardware" ist berücksichtigt: Die Möglichkeit zur Erweiterung und Aufrüstung der Hardware, wie z.B. durch Speichererweiterungen, ist eingeplant, um zukünftige Anforderungen ohne vollständigen Austausch der Hardware erfüllen zu können.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Strategie zur modularen Erweiterung ist definiert: Es gibt eine klar definierte Strategie zur modularen Erweiterung des Systems, die sicherstellt, dass neue Funktionen und Komponenten problemlos integriert werden können, ohne die bestehende Architektur zu beeinträchtigen.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Regelmäßige Überprüfung und Anpassung der modularen Strategie: Die modulare Strategie wird regelmäßig überprüft und an neue technologische Entwicklungen und Geschäftsanforderungen angepasst, um die Wettbewerbsfähigkeit und Effizienz des Systems zu erhalten.		x	x	x	x	R: SW-PM A: S: SW- A I:	SW-PM
Abschaltbarkeit von bestimmten Funktionen und Komponenten wurde juristisch geprüft : Die Abschaltbarkeit von bestimmten Funktionen und Komponenten wurde juristisch geprüft und ist aus juristischer Sicht unbedenklich.	x	x				R: JUR A: S: SW-PM, SW-A I:	JUR

5 Prozesse & Rahmenbedingungen

AQI Automotive Quality Institute

5.1 **Freie und Open Source Software (FOSS):** Integration und Pflege von Open-Source-Software, um die langfristige Wartbarkeit und Anpassungsfähigkeit zu sichern.

5.2 **A-Spice/VDA 6.3:** Einhaltung von Standards wie A-SPICE und VDA 6.3 zur Sicherstellung der Prozessqualität in der Softwareentwicklung und -wartung.

5.3 **Cybersecurity:** Regelmäßige Überprüfung und Aktualisierung von Cybersecurity-Maßnahmen, um den Schutz vor Bedrohungen sicherzustellen.

5 Prozesse & Rahmenbedingungen

5.1 Freie und Open Source Software (FOSS)

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetriebnahme		
Lizenzkonformität geprüft: Die Einhaltung aller FOSS-Lizenzbedingungen wurde juristisch geprüft und ist mit den Projekt- und Unternehmenszielen vereinbar	x	x				R: SW-A A: S: JUR I: SW-PM	SW-A
FOSS-Komponenten sind dokumentiert und nachverfolgbar: Alle verwendeten FOSS-Komponenten sind vollständig dokumentiert und die Versionen sind eindeutig nachverfolgbar, um eine konsistente Wartung und Aktualisierung zu gewährleisten.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Sicherheitsupdates für FOSS-Komponenten werden zeitnah implementiert: Sicherheitsrelevante Updates für FOSS-Komponenten werden zeitnah geprüft und implementiert, um Schwachstellen im System zu vermeiden.		x	x	x	x	R: SW-PM A: S: Security I:	SW-A
Wartungspläne für Open-Source-Komponenten sind definiert: Es sind klare Wartungspläne für alle verwendeten FOSS-Komponenten festgelegt, um deren langfristige Funktionsfähigkeit und Sicherheit sicherzustellen.		x	x			R: SW-PM A: S: SW-A I:	SW-PM
Kompatibilität von FOSS-Komponenten wird regelmäßig geprüft: Die Kompatibilität der FOSS-Komponenten mit den übrigen Systemen wird regelmäßig überprüft, um Integrationsprobleme frühzeitig zu erkennen und zu beheben.		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
Risikoanalyse für FOSS-Nutzung ist durchgeführt: Eine umfassende Risikoanalyse bezüglich der Nutzung von FOSS-Komponenten wurde durchgeführt, um potenzielle Risiken zu identifizieren und entsprechende Maßnahmen zu planen.	x	x				R: SW-A A: S: SW-PM, Security I: QM	SW-A
Strategie für den Umgang mit FOSS-Abhängigkeiten ist definiert: Eine klare Strategie für den Umgang mit Abhängigkeiten von FOSS-Komponenten, einschließlich der Planung von Alternativen, ist festgelegt, um die Systemstabilität auch bei Änderungen in der FOSS-Community zu gewährleisten.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Entwicklungsteam vorhanden und gewährleistet Long Term Support (LTS): Das Entwicklungsteam der FOSS ist vertrauenswürdig, kann eine langzeitliche Wartung der Software sicherstellen und gewährleistet „Long Term Support (LTS).	x	x	x	x	x	R: SW-A A: S: SW-PM, Security I:	SW-A

5 Prozesse & Rahmenbedingungen

5.2 A-Spice/VDA 6.3

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
A-SPICE Assessment erfolgreich durchgeführt : Internes oder externes A-SPICE Assessment wurde erfolgreich durchgeführt, so dass alle relevanten Entwicklungs- und Wartungsprozesse A-SPICE-konform umgesetzt werden können.		x				R: SW-PM A: S: QM I:	SW-PM
VDA 6.3 Audit erfolgreich durchgeführt: Ein VDA 6.3 Audit wurde erfolgreich durchgeführt, so dass Qualität und Leistungsfähigkeit von Prozessen und deren Output den Anforderungen des VDA 6.3-Standards entsprechen.		x				R: SW-PM A: S: QM I:	SW-PM
Prozessdokumentation ist vollständig und aktuell: Alle A-SPICE- und VDA 6.3-relevanten Prozesse sind umfassend dokumentiert und werden regelmäßig auf ihre Aktualität und Wirksamkeit überprüft.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Regelmäßige Schulungen zu A-SPICE/VDA 6.3 sind durchgeführt: Mitarbeiter, die in den relevanten Prozessen involviert sind, erhalten regelmäßige Schulungen, um sicherzustellen, dass sie mit den Anforderungen und Best Practices vertraut sind.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
A-SPICE Assessments und VDA 6.3 Audits werden regelmäßig wiederholt: A-SPICE Assessments und VDA 6.3 Audits werden regelmäßig wiederholt, um die Einhaltung der Standards zu überprüfen und Verbesserungsmöglichkeiten zu identifizieren		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

5 Prozesse & Rahmenbedingungen

5.3 Cybersecurity

Prüfpunkte

	Wann? Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme	Wer?	Wer muss geschult werden?
Cybersecurity-Maßnahmen sind umfassend umgesetzt: Alle relevanten Maßnahmen, die sich aus dem normativ rechtlichen Rahmenwerk und dem Stand der Technik ergeben, wurden vollständig implementiert und an die aktuellen Anforderungen angepasst.[1]	x	x				R: Security A: S: SW-A, SW-PM I:	Security
Einheitliche Umsetzung von Cybersecurity-Maßnahmen in der Lieferkette ist gewährleistet: Eine langfristige Strategie stellt sicher, dass alle Cybersecurity-Maßnahmen konsistent über die gesamte Lieferkette hinweg umgesetzt werden, einschließlich der Anpassung an neue gesetzliche Vorgaben und den aktuellen Stand der Technik.		x	x	x	x	R: SW-PM A: S: Security I:	SW-PM

[1]Es existieren zahlreiche Standards/Vorgaben, die Cybersecurity adressieren. Abhängig vom Anwendungskotext sind u.a. die folgenden Standards/Vorgaben für die deutschen Automobilindustrie relevant:

- UNECE R155: Anforderungen an Cybersecurity-Managementsysteme (CSMS).
- UNECE R156: Regelungen für Over-the-Air (OTA)-Updates.
- ISO/SAE 21434: Cybersecurity-Engineering über den gesamten Fahrzeuglebenszyklus.
- ISO 24089: Software-Update-Management-Systeme (SUMS).
- ISO/IEC 27001: Informationssicherheits-Managementsysteme.
- ISO/TR 4804: Leitlinien zur Cybersecurity in vernetzten Fahrzeugen.
- IEC 62443: Industrial Cybersecurity, anwendbar auf Fahrzeugarchitekturen.
- VDA TISAx und ISA: Standards für Informationssicherheitsbewertungen und Assessment, speziell für die Automobilindustrie entwickelt.
- VDA Band „Cybersecurity für Fahrzeuge“: VDA-Leitfaden zur Absicherung von Fahrzeugsoftware.
- ASPICE for Cybersecurity 2.0 (ab 2025)

6 Risikomanagement

AQI Automotive Quality Institute

6.1 Risikobewertung und -absicherung: Durchführung systematischer Risikobewertungen und Implementierung von Maßnahmen zur Risikominimierung.

6.2 Notfall- und Krisenmanagement: Entwicklung und Implementierung von Prozessen für den Umgang mit Notfällen und Krisensituationen, insbesondere bei Cybersecurity-Vorfällen.

6.3 Rechtliche Rahmenbedingungen und Stand der Technik: Überwachung von rechtlichen und technischen Entwicklungen, um Softwareanpassungen rechtzeitig zu planen und durchzuführen.

6.4 Störungs- und Endkundenverhalten: Identifizierung und Bewertung von Risiken, die aus Störungen der Infrastruktur und dem sich ändernden Endkundenverhalten resultieren.

6 Risikomanagement

6.1 Risikobewertung und -absicherung

AQI | Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Regelmäßige Risikobewertungen sind implementiert: Es werden regelmäßig umfassende Risikobewertungen durchgeführt, um potenzielle Risiken im Software- und Systembetrieb frühzeitig zu identifizieren und zu dokumentieren.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Risikokategorien sind klar definiert: Alle relevanten Risiken werden in klaren Kategorien erfasst, z.B. technische Risiken, Sicherheitsrisiken, Lieferkettenrisiken, um eine gezielte Analyse und Priorisierung zu ermöglichen.	x	x				R: SW-A A: S: SW-PM, QM I:	SW-A
Maßnahmen zur Risikominderung sind etabliert: Für alle identifizierten Risiken sind spezifische Maßnahmen zur Risikominderung definiert und implementiert, um die Auswirkungen potenzieller Risiken zu minimieren.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Verantwortlichkeiten für Risikomanagement sind festgelegt: Es sind klare Verantwortlichkeiten für die Überwachung, Bewertung und Steuerung von Risiken festgelegt, die über den gesamten Produktlebenszyklus hinweg gelten.		x				R: SW-PM A: S: QM I:	SW-PM
Risikomanagement ist in Entscheidungsprozesse integriert: Das Risikomanagement ist fest in alle strategischen und operativen Entscheidungsprozesse integriert, um sicherzustellen, dass Risiken bei allen wichtigen Entscheidungen berücksichtigt werden.		x				R: SW-PM A: S: QM I:	SW-PM
Kontinuierliche Überwachung der Risikomaßnahmen ist sichergestellt: Alle implementierten Maßnahmen zur Risikominderung werden kontinuierlich überwacht und auf ihre Wirksamkeit überprüft, um bei Bedarf Anpassungen vorzunehmen.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Dokumentation und Kommunikation der Risiken sind gewährleistet: Alle identifizierten Risiken, deren Bewertung und die ergriffenen Maßnahmen sind umfassend dokumentiert und werden regelmäßig an alle relevanten Stakeholder kommuniziert.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

6 Risikomanagement

6.2 Notfall- und Krisenmanagement

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Notfallpläne sind umfassend definiert: Umfassende Notfallpläne sind entwickelt, die klare Anweisungen und Protokolle für den Umgang mit verschiedenen Krisenszenarien, wie Systemausfällen oder Sicherheitsvorfällen, enthalten.		x				R: SW-PM A: S: SW-A, QM I:	SW-PM
Krisenmanagement-Team ist benannt: Ein spezialisiertes Krisenmanagement-Team ist benannt und verantwortlich für die Umsetzung der Notfallpläne sowie die Koordination aller Aktivitäten im Krisenfal		x				R: SW-PM A: S: QM I:	SW-PM
Regelmäßige Notfallübungen sind durchgeführt: Regelmäßige Notfallübungen und Simulationen werden durchgeführt, um die Reaktionsfähigkeit des Teams zu testen und Schwachstellen in den Notfallplänen zu identifizieren und zu beheben.		x	x	x	x	R: SW-PM A: S: TV-Ing, QM I:	SW-PM
Kommunikationsprotokolle sind festgelegt: Klare Kommunikationsprotokolle für den Krisenfall sind definiert, um eine schnelle und effektive Informationsweitergabe sowohl intern als auch extern zu gewährleisten.		x				R: SW-PM A: S: QM I:	SW-PM
Krisenbewältigungsstrategien sind dokumentiert: Detaillierte Strategien zur Bewältigung von Krisen, einschließlich Eskalationsstufen und Entscheidungspfaden, sind dokumentiert und werden regelmäßig aktualisiert.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Ressourcen für den Krisenfall sind bereitgestellt: Alle notwendigen Ressourcen, wie alternative IT-Infrastrukturen, Ersatzteile oder externe Dienstleister, sind für den Krisenfall eingeplant und schnell verfügbar.		x	x	x	x	R: SW-PM A: S: SW-A I: QM	SW-PM
Lernprozess nach Krisen ist implementiert: Ein formalisierter Prozess zur Auswertung und Dokumentation von Erkenntnissen aus durchgeführten Notfallübungen und realen Krisenfällen ist implementiert, um kontinuierliche Verbesserungen im Krisenmanagement sicherzustellen.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

6 Risikomanagement

6.3 Rechtliche Rahmenbedingungen und Stand der Technik (1/2)

AQI Automotive Quality Institute

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Änderungen im normativen und rechtlichen Rahmenwerk werden regelmäßig überwacht: Ein regelmäßiges Screening erfolgt, um Gesetzesänderungen, Gerichtsurteile, neue Regulierungen und Normen frühzeitig zu identifizieren und ihre Auswirkungen auf die Software und Prozesse zu bewerten.		x	x	x	x	R: SW-PM A: S: QM I: JUR	SW-PM
Langfristige Softwareanpassungen aufgrund von Gesetzesänderungen sind eingeplant: Langfristige Anpassungen der Software, die aufgrund neuer gesetzlicher Anforderungen, Gerichtsurteile oder regulatorischer Änderungen notwendig sind, werden in der Entwicklungs- und Wartungsplanung berücksichtigt, auch in der Lieferkette.		x	x	x	x	R: SW-PM A: S: QM I: JUR	SW-PM
Verantwortungsbereich für Gesetzesänderungen ist definiert: Der Verantwortungsbereich für die Aktualisierung von Softwarekomponenten infolge von Gesetzesänderungen ist über die gesamte Lieferkette hinweg klar definiert und dokumentiert.		x				R: SW-PM A: S: QM I: JUR	SW-PM
Weltweites Screening für Gesetzesänderungen ist implementiert: Ein globales Screening wird regelmäßig durchgeführt, um mittel- und langfristige rechtliche und regulatorische Änderungen zu erkennen und rechtzeitig in die Softwareplanung einfließen zu lassen.		x	x	x	x	R: SW-PM A: S: QM I: JUR	SW-PM
Änderungen im Stand der Technik werden kontinuierlich überwacht: Es erfolgt eine kontinuierliche Überwachung der Entwicklungen im Stand der Technik, um sicherzustellen, dass die eingesetzten Softwarekomponenten und Technologien den aktuellen Standards entsprechen.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Langfristige Softwareanpassungen aufgrund technischer Entwicklungen sind eingeplant: Langfristige Anpassungen der Software, die durch technologische Entwicklungen oder neue Industriestandards erforderlich sind, werden in der gesamten Lieferkette geplant und umgesetzt.		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
Verantwortungsbereich für Änderungen beim Stand der Technik ist klar geregelt: Die Verantwortlichkeiten für die Aktualisierung von Softwarekomponenten infolge von Änderungen beim Stand der Technik sind für alle Zulieferer und Beteiligten eindeutig festgelegt.		x				R: SW-PM A: S: QM I:	SW-PM
Screening für technologische Entwicklungen ist implementiert: Ein vorausschauendes Screening, das potenzielle technologische Änderungen und deren Auswirkungen auf die Softwareentwicklung mittel- und langfristig identifiziert, ist fest in den Planungsprozess integriert.		x				R: SW-PM A: S: QM I:	SW-PM

6 Risikomanagement

6.3 Rechtliche Rahmenbedingungen und Stand der Technik (2/2)

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Residual Risks werden fortlaufend analysiert: Die Restrisiken, die nach der Anwendung von Security-Maßnahmen verbleiben, werden regelmäßig durch Threat Assessment and Risk Analysis (TAJUR) überprüft und an Veränderungen im Stand der Technik angepasst, um Sicherheitslücken frühzeitig zu identifizieren und zu minimieren.		x	x	x	x	R: SW-PM A: S: Security, QM I:	SW-PM

6 Risikomanagement

6.4 Infrastruktur und Endkundenverhalten

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Risikomanagement bei temporären Störungen und Infrastrukturausfällen ist implementiert: Maßnahmen zur Risikominimierung bei temporären Störungen von Infrastruktur und Diensten, wie GPS-Ausfällen oder Mobilfunkunterbrechungen, sind etabliert, um die Funktionsfähigkeit der Software zu gewährleisten.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM
Strategien für das Ende von unterstützten Protokollen oder Standards sind definiert: Es sind klare Strategien und Alternativen implementiert, um auf das Ende der Unterstützung genutzter Protokolle oder die Abschaltung von Mobilfunkstandards flexibel reagieren zu können.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Langfristige Infrastrukturänderungen werden proaktiv berücksichtigt: Technologische Änderungen, wie das Einstellen von Mobilfunkstandards oder Protokollen, werden frühzeitig erkannt und in die langfristige Softwareplanung integriert, um rechtzeitig alternative Lösungen zu implementieren.	x	x				R: SW-A A: S: SW-PM I:	SW-A
Veränderungen im Kundenverhalten werden kontinuierlich überwacht: Das Verhalten der Endkunden, insbesondere in Bezug auf Datenschutz, Nutzerinteraktion und Umweltbewusstsein, wird regelmäßig analysiert, um frühzeitig auf veränderte Erwartungen reagieren zu können.				x		R: SW-PM A: S: QM I:	SW-PM
Anpassung der User Experience an Kundenbedürfnisse ist gewährleistet: Die User Experience und das User Interface der Software werden regelmäßig an die sich verändernden Gewohnheiten und Erwartungen der Endkunden angepasst, um Akzeptanzverlust zu verhindern und moderne Benutzeranforderungen zu erfüllen.	x			x		R: SW-PM A: S: QM I:	SW-PM

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

AQI Automotive Quality Institute

7.1 **Kollaborationsmodelle:** Entwicklung und Umsetzung von Modellen zur Zusammenarbeit zwischen OEMs und Lieferanten, um (F)OTA, Testing und andere Prozesse zu optimieren.

7.2 **Zusammenarbeit mit Unterlieferanten:** Sicherstellung der reibungslosen Zusammenarbeit und Koordination mit Unterlieferanten in der Lieferkette.

7.3 **Dokumentation (SBOM, CBOM):** Verwendung und Pflege von Software Bills of Materials (SBOMs) und Cryptograhic Bills of Materials (CBOMs), um eine Bestandsaufnahme aller Bausteine eines Softwareprodukts für die gesamte Lieferkette nachvollziehbar und transparent zu machen.

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.1 Kollaborationsmodelle

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
Kollaborationsmodelle sind klar definiert: Es sind klare Kollaborationsmodelle zwischen OEMs und Zulieferern etabliert, die Verantwortlichkeiten, Schnittstellen und Kommunikationswege eindeutig regeln.	x					R: SW-PM A: S: Einkauf I:	SW-PM
Regelmäßige Abstimmungsmeetings sind vorgesehen: Regelmäßige Meetings zwischen allen Beteiligten sind eingeplant, um die Zusammenarbeit zu koordinieren und auftretende Probleme oder Änderungen zeitnah zu besprechen.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
Informationsaustausch ist transparent und standardisiert: Ein transparenter und standardisierter Prozess für den Informationsaustausch zwischen allen Partnern ist implementiert, um Verzögerungen und Missverständnisse zu vermeiden.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
Verantwortlichkeiten und Zuständigkeiten sind dokumentiert: Alle Verantwortlichkeiten und Zuständigkeiten innerhalb der Kollaborationsmodelle sind klar dokumentiert und den jeweiligen Parteien zugewiesen.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
Flexibilität in der Zusammenarbeit ist gewährleistet: Die Kollaborationsmodelle sind flexibel gestaltet, um auf Änderungen in der Lieferkette, wie neue Anforderungen oder Partner, schnell reagieren zu können.	x	x	x	x	x	R: SW-PM A: S: I: Alle	SW-PM
Risiko- und Konfliktmanagement sind integriert: Prozesse für das Risiko- und Konfliktmanagement sind in die Kollaborationsmodelle integriert, um potenzielle Herausforderungen in der Zusammenarbeit frühzeitig zu erkennen und zu bewältigen.		x	x	x		R: SW-PM A: S: QM I: Alle	SW-PM
Kontinuierliche Verbesserung der Kollaboration ist sichergestellt: Es sind Mechanismen zur kontinuierlichen Verbesserung der Zusammenarbeit implementiert, die regelmäßige Feedback-Schleifen und Optimierungsmaßnahmen vorsehen.		x	x	x		R: SW-PM A: S: I: Alle	SW-PM

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.2 Zusammenarbeit mit Unterlieferanten

Prüfpunkte

Prüfpunkte	Wann? Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme	Wer?	Wer muss geschult werden?
Strategisches Wissensmanagement ist implementiert: Ein strategisches Wissensmanagementsystem ist etabliert, das sicherstellt, dass das Know-how der Unterlieferanten langfristig gesichert und bei Bedarf weitergegeben wird.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
Kompetenzverteilung ist klar definiert: Die Verteilung von Kompetenzen zwischen OEM, Zulieferern und Unterlieferanten ist klar geregelt und dokumentiert, um eine reibungslose Zusammenarbeit zu gewährleisten.	x	x	x	x	x	R: SW-PM A: S: SW-A, QM I:	SW-PM
Dokumentationen sind transparent und zugänglich: Alle relevanten Dokumentationen, einschließlich technischer Spezifikationen und Prozessbeschreibungen, sind für alle Partner zugänglich und werden regelmäßig aktualisiert.		x	x	x		R: SW-PM A: S: QM I:	SW-PM
Zukunftssichere Standards sind festgelegt: Zukunftssichere und State-of-the-art Standards sowie Programmiersprachen sind gemeinsam festgelegt und werden von allen Beteiligten konsequent angewendet.	x	x				R: SW-A A: S: SW-PM I:	SW-PM
Nutzung gemeinsamer Tools ist gewährleistet: Es wird sichergestellt, dass OEMs, Zulieferer und Unterlieferanten auf eine gemeinsame Tool-Infrastruktur zugreifen, um die Effizienz und Konsistenz in der Zusammenarbeit zu maximieren.		x	x	x		R: SW-PM A: S: SW-A I:	SW-PM
Transparente Kommunikationswege sind etabliert: Es sind klare und transparente Kommunikationswege zwischen OEM, Zulieferern und Unterlieferanten etabliert, um den Informationsfluss und die Koordination zu optimieren.		x	x	x	x	R: SW-PM A: S: Einkauf I:	SW-PM
Regelmäßige Überprüfung der Zusammenarbeit erfolgt: Die Zusammenarbeit mit Unterlieferanten wird regelmäßig überprüft und optimiert, um sicherzustellen, dass alle Partner weiterhin den festgelegten Standards und Prozessen folgen.		x	x	x	x	R: SW-PM A: S: Einkauf I:	SW-PM
Risikoanalyse und Notfallpläne für Unterbrechungen in der Lieferkette sind implementiert: Robuste Notfallpläne und Risikoanalysen sind etabliert, um auf Engpässe in der Software-Wartung und -Pflege aufgrund von Extremsituationen wie politischen Konflikten, Umwelteinflüsse oder blockierten Handelsrouten schnell reagieren zu können.		x	x	x	x	R: SW-PM A: S: QM I:	SW-PM

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.3 Dokumentation (SBOM, CBOM)

Prüfpunkte

	Wann?					Wer?	Wer muss geschult werden?
	Konzept-entwicklung	Serien-entwicklung	Serien-vorbereitung	Betrieb	Deaktivierung/ Außerbetrieb-nahme		
SBOM nach aktuellem Stand der Technik umgesetzt: Der Umgang mit SBOMs (Software Bills of Materials) entspricht dem aktuellen Stand der Technik und Empfehlungen / Guidelines von Behörden und anderen relevanten Institutionen werden umgesetzt.[1]		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
CBOM nach aktuellem Stand der Technik umgesetzt: Der Umgang mit CBOMs (Cryptographic Bills of Materials) entspricht dem aktuellen Stand der Technik und alle im Produkt verwendeten kryptographischen Mechanismen, einschließlich Algorithmen und Schlüssellängen, werden detailliert dokumentiert und Richtlinien berücksichtigt.		x	x	x	x	R: SW-PM A: S: SW-A I:	SW-PM
Einheitliche Umsetzung in der Lieferkette: Der Umgang mit SBOMs und CBOMs ist für die gesamte Lieferkette einheitlich umgesetzt.		x				R: SW-PM A: S: SW-A I:	SW-PM

[1] In der deutschen Automobilindustrie existiert bislang kein standardisierter Umgang mit SBOMs – folgende Quellen geben u.a. Empfehlungen für den Umgang mit SBOMs:

Empfehlung für Softwarehersteller durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Teil 2 der Technischen Richtlinie TR-03183 „Cyber-Resilienz Anforderungen“: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=5

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

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

Empfehlungen der US Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov/sbom