AQI Automotive Quality Institute

Langzeitqualität von Software-intensiven Systemen

Checkliste

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

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 (bzgl. (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)

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Vertragsumfang ist klar definiert: Der Umfang der Wartungsverträge ist detailliert festgelegt, einschließlich aller unterstützten Softwaremodule, Versionen und Hardware-Komponenten.	☐	☐	
Verantwortlichkeiten sind eindeutig zugewiesen: Die Verantwortlichkeiten für alle beteiligten Parteien, einschließlich der Zuständigkeiten für Updates, Analyse, Bugfixes und Support, sind klar festgelegt.	☐	☐	
Reaktionszeiten sind verbindlich festgelegt: Verbindliche Reaktionszeiten für die Bearbeitung von Support-Anfragen und die Behebung von Fehlern sind im Vertrag verankert.	☐	☐	
Leistungskennzahlen (KPIs) sind vereinbart: KPIs für die Wartungsleistungen sind definiert, um die Servicequalität regelmäßig zu überwachen und zu bewerten.	☐	☐	
Laufzeiten und Verlängerungsoptionen sind bestimmt: Die Laufzeit des Wartungsvertrags sowie Optionen und Bedingungen für Vertragsverlängerungen sind klar geregelt.	☐	☐	
Eskalationsprozesse sind festgelegt: Eskalationsstufen und -verfahren im Falle von Streitigkeiten oder bei Nichteinhaltung der vertraglichen Verpflichtungen sind definiert.	☐	☐	
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.	☐	☐	
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.	☐	☐	

1 Vertragsmanagement

1.1 Wartungsverträge (2/2)

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Kostenstruktur ist transparent gestaltet: Eine transparente und nachvollziehbare Kostenstruktur für alle Wartungsleistungen, einschließlich regelmäßiger Updates und Anpassungen, ist erstellt.	☐	☐	
Datensicherheitsanforderungen sind integriert: Anforderungen an die Datensicherheit und den Schutz vertraulicher Informationen im Rahmen der Wartungsleistungen sind definiert und implementiert.	☐	☐	
Dokumentationspflichten sind verbindlich festgelegt: Verbindliche Anforderungen an die Dokumentation aller durchgeführten Wartungsarbeiten und Änderungen sind festgelegt, um die Nachvollziehbarkeit sicherzustellen.	☐	☐	
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.	☐	☐	

1 Vertragsmanagement

1.2 Zeiträume

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
Wartungszeiträume umfassen den gesamten Produktlebenszyklus: Die definierten Wartungszeiträume decken den gesamten Lebenszyklus ab, einschließlich der Nachbetreuung in der Wartungsphase.	☐	☐	
Modellpflege- und Produktaufwertungszyklen sind festgelegt: Die Zyklen für Modellpflege, Produktaufwertung und Software-Upgrades sind klar definiert und an die Wartungsphasen angepasst.	☐	☐	
Haftungszeiträume sind über die gesamte Lieferkette geregelt: Die Haftungszeiträume sind transparent und über die gesamte Zulieferkette hinweg klar geregelt und vertraglich verankert.	☐	☐	
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.	☐	☐	
Alle beteiligten Parteien sind über die Zeiträume informiert: Die festgelegten Wartungszeiträume und deren Konsequenzen sind allen Vertragspartnern und Beteiligten in der Zulieferkette transparent kommuniziert.	☐	☐	

1 Vertragsmanagement

1.3 Gewährleistung und Haftung

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
Haftungsrisiken sind umfassend analysiert: Alle potenziellen Haftungsrisiken wurden identifiziert und im Vertrag berücksichtigt, um unerwartete Kosten zu minimieren.	☐	☐	
Vertragsstrafen bei Nichterfüllung sind definiert: Es sind klare Vertragsstrafen vorgesehen, falls die vertraglich festgelegten Gewährleistungs- oder Haftungsbedingungen nicht eingehalten werden.	☐	☐	
Haftungsgrenzen sind auf Zulieferer abgestimmt: Die festgelegten Haftungsgrenzen sind über die gesamte Lieferkette hinweg konsistent und mit den Zulieferern abgestimmt.	☐	☐	
Rückgriffsansprüche sind klar geregelt: Die Bedingungen für Rückgriffsansprüche im Falle von Mängeln oder Schäden sind eindeutig festgelegt und vertraglich abgesichert.	☐	☐	
Kommunikation der Haftungsbedingungen ist gewährleistet: Alle relevanten Parteien in der Lieferkette sind über die festgelegten Haftungs- und Gewährleistungsbedingungen informiert und verstehen ihre Verpflichtungen.	☐	☐	
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.	☐	☐	

1 Vertragsmanagement

1.4 Standarddokumente

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Verwendung standardisierter Vertragsvorlagen ist sichergestellt: Alle Verträge und Vereinbarungen basieren auf einheitlichen, standardisierten Dokumentvorlagen, um Konsistenz und Rechtssicherheit zu gewährleisten.	☐	☐	
Zugänglichkeit der Standarddokumente ist gewährleistet: Standarddokumente sind für alle relevanten Parteien leicht zugänglich, entweder über ein zentrales Dokumentenmanagementsystem oder eine andere vereinbarte Plattform.	☐	☐	
Konsistenz über die Lieferkette ist sichergestellt: Die Verwendung von Standarddokumenten ist über die gesamte Lieferkette hinweg durchgesetzt, um einheitliche Bedingungen und Vorgehensweisen sicherzustellen.	☐	☐	
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.	☐	☐	
Relevante AGB sind allen Parteien bekannt und zugänglich: Alle relevanten Allgemeinen Geschäftsbedingungen (AGB) sind eindeutig dokumentiert, allen beteiligten Parteien bekannt und jederzeit zugänglich gemacht.	☐	☐	
Archivierung und Versionierung sind gewährleistet: Alle Versionen der Standarddokumente werden revisionssicher archiviert, um eine lückenlose Nachvollziehbarkeit und historische Überprüfung zu ermöglichen.	☐	☐	

1 Vertragsmanagement

1.5 Zugriffsabsicherung (1/2)

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Code-Generierung ist umfassend geplant: Zusätzliche erforderliche Engineering-Artefakte für die Code-Generierung sind identifiziert, um sicherzustellen, dass alle notwendigen Modelle korrekt in Code umgesetzt werden können.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Regelmäßige Überprüfung der Escrow-Vereinbarungen ist implementiert: Escrow-Vereinbarungen werden regelmäßig überprüft und bei Bedarf angepasst, um sicherzustellen, dass sie den aktuellen Anforderungen entsprechen.	☐	☐	
Zugriffsrechte sind transparent geregelt: Alle Zugriffsrechte auf den Quellcode, Dokumentation und sonstige kritische Softwarekomponenten sind transparent dokumentiert und für alle relevanten Parteien nachvollziehbar.	☐	☐	

1 Vertragsmanagement

1.5 Zugriffsabsicherung (2/2)

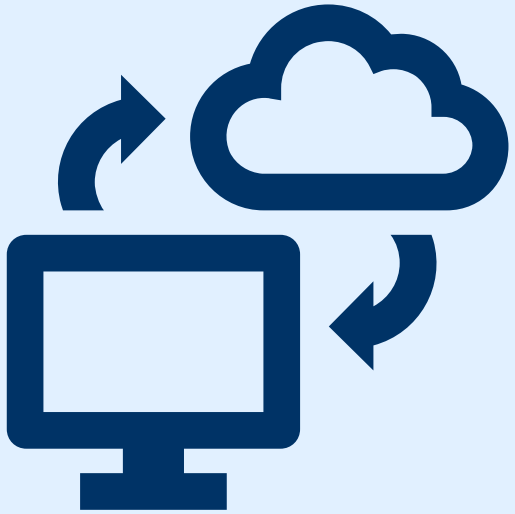
Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Notfallpläne für den Zugriff auf Software sind vorhanden: Es sind Notfallpläne implementiert, die den sofortigen Zugang zu wichtigen Softwarekomponenten und Dokumentationen sicherstellen, falls ein Anbieter ausfällt oder insolvent wird.	☐	☐	

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	Trifft zu	Trifft nicht zu	Bemerkung
Verantwortungsbereich ist klar definiert: Der Zugriff und der Einfluss des Zulieferers auf (F)OTA-Updates sind im Wartungsvertrag klar festgelegt und dokumentiert.	☐	☐	
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.	☐	☐	
Schnittstellen sind standardisiert: Die Schnittstellen für (F)OTA-Updates sind projektübergreifend sowohl für den OEM als auch für den Zulieferer vereinheitlicht und standardisiert.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Variantenmanagement ist berücksichtigt: Varianten und Updates sind aufeinander abgestimmt, damit potentiell alle Fahrzeuge erreicht werden können und Softwarevarianten gezielt und effizient aktualisiert werden können.	☐	☐	
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.	☐	☐	

2 Fahrzeug-Updates

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

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	

2 Fahrzeug-Updates

2.2 Sicherheits- und Funktionsanforderungen (1/2)

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Datenschutzrichtlinien sind implementiert: Strenge Datenschutzrichtlinien sind implementiert, um sicherzustellen, dass personenbezogene und sicherheitsrelevante Daten während des (F)OTA-Prozesses geschützt bleiben.	☐	☐	
Sicherheitsstandards sind eingehalten: Alle (F)OTA-Updates erfüllen die festgelegten Sicherheitsstandards und regulatorischen Anforderungen, um die Integrität und Sicherheit der Fahrzeugsoftware zu gewährleisten.	☐	☐	
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.	☐	☐	
Regelmäßige Sicherheitsbewertungen sind vorgesehen: Es sind regelmäßige Sicherheitsbewertungen geplant, um potenzielle Schwachstellen in den (F)OTA-Prozessen frühzeitig zu erkennen und zu beheben.	☐	☐	

2 Fahrzeug-Updates

2.2 Sicherheits- und Funktionsanforderungen (2/2)

Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Sicherheitsprotokolle werden kontinuierlich überwacht: Alle sicherheitsrelevanten Protokolle und Logs werden kontinuierlich überwacht, um Anomalien oder sicherheitskritische Ereignisse sofort zu erkennen.	☐	☐	
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.	☐	☐	

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)

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
Vertragliche Regelungen zur Analyse- und Updatefähigkeit sind definiert: Klare vertragliche Regelungen zur Analyse- und Updatefähigkeit der Software, einschließlich festgelegter Zeiträume, sind implementiert.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Testzeitraum entspricht dem Wartungszeitraum: Die Testfähigkeit der Software wird über den gesamten Wartungszeitraum hinweg sichergestellt, um kontinuierliche Qualität und Zuverlässigkeit zu gewährleisten.	☐	☐	
Technologieakzeptanz ist in der Lieferkette geklärt: Die Akzeptanz der verwendeten Testtechnologien ist zwischen allen Partnern geklärt, insbesondere im Hinblick auf die Behandlung unvollständiger Anforderungen.	☐	☐	
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.	☐	☐	
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.	☐	☐	

3 Wartung & Testing

3.1 Teststrategien (2/2)

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
Kontinuität der Tests ist gewährleistet: Die Kontinuität der Testprozesse wird über den gesamten Produktlebenszyklus hinweg gewährleistet, um die dauerhafte Einhaltung aller Qualitätsstandards zu sichern.	☐	☐	

3 Wartung & Testing

3.2 Entwicklungs- und Testumgebungen

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	

3 Wartung & Testing

3.3 Verfügbarkeiten

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
Redundanz bei Testtools und Umgebungen ist eingeplant: Es ist eine Redundanzstrategie implementiert, um alternative Testtools und Umgebungen bereitzuhalten, falls Primärressourcen ausfallen.	☐	☐	
Verfügbarkeit von Testpersonal ist geplant: Die Verfügbarkeit von qualifiziertem Testpersonal ist über den gesamten Test- und Wartungszeitraum hinweg sichergestellt, einschließlich Schulungen und Ressourcenplanung.	☐	☐	
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).	☐	☐	
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.	☐	☐	

3 Wartung & Testing

3.4 Wissensmanagement

AQI Automotive Quality Institute

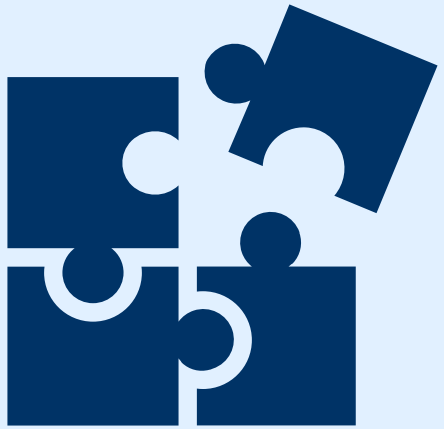
Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Systematische Dokumentation ist implementiert: Alle relevanten Informationen, Prozesse und Erfahrungen werden systematisch dokumentiert und in einem zentralen Wissensmanagementsystem gespeichert, um den Zugang für alle Beteiligten zu gewährleisten.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Wissensmanagementsystem ist zugänglich und benutzerfreundlich: Das Wissensmanagementsystem ist für alle relevanten Mitarbeiter leicht zugänglich und benutzerfreundlich gestaltet, um eine effektive Nutzung zu fördern.	☐	☐	
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.	☐	☐	
Verantwortlichkeiten für Wissensmanagement sind festgelegt: Es sind klare Verantwortlichkeiten für die Pflege und Aktualisierung des Wissensmanagementsystems zugewiesen, um dessen kontinuierliche Relevanz und Aktualität sicherzustellen.	☐	☐	
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.	☐	☐	
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	☐	☐	

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	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
Abwärtskompatibilität ist sichergestellt: Die Abwärtskompatibilität der Software und Hardware ist strategisch berücksichtigt und implementiert, um sicherzustellen, dass neue Komponenten mit älteren Systemen kompatibel sind.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Regelmäßige Kompatibilitätsprüfungen sind eingeplant: Es sind regelmäßige Überprüfungen und Tests vorgesehen, um sicherzustellen, dass die Kompatibilitätsstrategie über den gesamten Produktlebenszyklus hinweg eingehalten wird.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	

4 Kompatibilität & Modulare Bauweise

4.2 Modulares Design

	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
„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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	

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	Trifft zu	Trifft nicht zu	Bemerkung
Lizenzkonformität geprüft: Die Einhaltung aller FOSS-Lizenzbedingungen wurde juristisch geprüft und ist mit den Projekt- und Unternehmenszielen vereinbar	☐	☐	
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.	☐	☐	
Sicherheitsupdates für FOSS-Komponenten werden zeitnah implementiert: Sicherheitsrelevante Updates für FOSS-Komponenten werden zeitnah geprüft und implementiert, um Schwachstellen im System zu vermeiden.	☐	☐	
Wartungspläne für Open-Source-Komponenten sind definiert: Es sind klare Wartungspläne für alle verwendeten FOSS-Komponenten festgelegt, um deren langfristige Funktionsfähigkeit und Sicherheit sicherzustellen.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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).	☐	☐	

5 Prozesse & Rahmenbedingungen

5.3 A-Spice/VDA 6.3

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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	☐	☐	

5 Prozesse & Rahmenbedingungen

5.4 Cybersecurity

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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]	☐	☐	
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.	☐	☐	

[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

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Regelmäßige Risikobewertungen sind implementiert: Es werden regelmäßig umfassende Risikobewertungen durchgeführt, um potenzielle Risiken im Software- und Systembetrieb frühzeitig zu identifizieren und zu dokumentieren.	☐	☐	
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.	☐	☐	
Maßnahmen zur Risikominderung sind etabliert: Für alle identifizierten Risiken sind spezifische Maßnahmen zur Risikominderung definiert und implementiert, um die Auswirkungen potenzieller Risiken zu minimieren.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Kontinuierliche Überwachung der Risikomaßnahmen ist sichergestellt: Alle implementierten Maßnahmen zur Risikominderung werden kontinuierlich überwacht und auf ihre Wirksamkeit überprüft, um bei Bedarf Anpassungen vorzunehmen.	☐	☐	
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.	☐	☐	

6 Risikomanagement

6.2 Notfall- und Krisenmanagement

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Notfallpläne sind umfassend definiert: Umfassende Notfallpläne sind entwickelt, die klare Anweisungen und Protokolle für den Umgang mit verschiedenen Krisenszenarien, wie Systemausfällen oder Sicherheitsvorfällen, enthalten.	☐	☐	
Krisenmanagement-Team ist benannt: Ein spezialisiertes Krisenmanagement-Team ist benannt und verantwortlich für die Umsetzung der Notfallpläne sowie die Koordination aller Aktivitäten im Krisenfall.	☐	☐	
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.	☐	☐	
Kommunikationsprotokolle sind festgelegt: Klare Kommunikationsprotokolle für den Krisenfall sind definiert, um eine schnelle und effektive Informationsweitergabe sowohl intern als auch extern zu gewährleisten.	☐	☐	
Krisenbewältigungsstrategien sind dokumentiert: Detaillierte Strategien zur Bewältigung von Krisen, einschließlich Eskalationsstufen und Entscheidungspfaden, sind dokumentiert und werden regelmäßig aktualisiert.	☐	☐	
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.	☐	☐	
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.	☐	☐	

6 Risikomanagement

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

AQI Automotive Quality Institute

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	

6 Risikomanagement

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

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Residual Risks werden fortlaufend analysiert: Die Restrisiken, die nach der Anwendung von Security-Maßnahmen verbleiben, werden regelmäßig durch Threat Assessment and Risk Analysis (TARA) überprüft und an Veränderungen im Stand der Technik angepasst, um Sicherheitslücken frühzeitig zu identifizieren und zu minimieren.	☐	☐	

6 Risikomanagement

6.4 Infrastruktur und Endkundenverhalten

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	
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.	☐	☐	

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	Trifft zu	Trifft nicht zu	Bemerkung
Kollaborationsmodelle sind klar definiert: Es sind klare Kollaborationsmodelle zwischen OEMs und Zulieferern etabliert, die Verantwortlichkeiten, Schnittstellen und Kommunikationswege eindeutig regeln.	☐	☐	
Regelmäßige Abstimmungsmeetings sind vorgesehen: Regelmäßige Meetings zwischen allen Beteiligten sind eingeplant, um die Zusammenarbeit zu koordinieren und auftretende Probleme oder Änderungen zeitnah zu besprechen.	☐	☐	
Informationsaustausch ist transparent und standardisiert: Ein transparenter und standardisierter Prozess für den Informationsaustausch zwischen allen Partnern ist implementiert, um Verzögerungen und Missverständnisse zu vermeiden.	☐	☐	
Verantwortlichkeiten und Zuständigkeiten sind dokumentiert: Alle Verantwortlichkeiten und Zuständigkeiten innerhalb der Kollaborationsmodelle sind klar dokumentiert und den jeweiligen Parteien zugewiesen.	☐	☐	
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.	☐	☐	
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.	☐	☐	
Kontinuierliche Verbesserung der Kollaboration ist sichergestellt: Es sind Mechanismen zur kontinuierlichen Verbesserung der Zusammenarbeit implementiert, die regelmäßige Feedback-Schleifen und Optimierungsmaßnahmen vorsehen.	☐	☐	

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.2 Zusammenarbeit mit Unterlieferanten

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
Strategisches Wissensmanagement ist implementiert: Ein strategisches Wissensmanagementsystem ist etabliert, das sicherstellt, dass das Know-how der Unterlieferanten langfristig gesichert und bei Bedarf weitergegeben wird.	☐	☐	
Kompetenzverteilung ist klar definiert: Die Verteilung von Kompetenzen zwischen OEM, Zulieferern und Unterlieferanten ist klar geregelt und dokumentiert, um eine reibungslose Zusammenarbeit zu gewährleisten.	☐	☐	
Dokumentationen sind transparent und zugänglich: Alle relevanten Dokumentationen, einschließlich technischer Spezifikationen und Prozessbeschreibungen, sind für alle Partner zugänglich und werden regelmäßig aktualisiert.	☐	☐	
Zukunftssichere Standards sind festgelegt: Zukunftssichere und State-of-the-art Standards sowie Programmiersprachen sind gemeinsam festgelegt und werden von allen Beteiligten konsequent angewendet.	☐	☐	
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.	☐	☐	
Transparente Kommunikationswege sind etabliert: Es sind klare und transparente Kommunikationswege zwischen OEM, Zulieferern und Unterlieferanten etabliert, um den Informationsfluss und die Koordination zu optimieren.	☐	☐	
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.	☐	☐	
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.	☐	☐	

7 Zusammenarbeit in einer Tier-N-Lieferantenstruktur

7.3 Dokumentation (SBOM, CBOM)

Prüfpunkte	Trifft zu	Trifft nicht zu	Bemerkung
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]	☐	☐	
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.	☐	☐	
Einheitliche Umsetzung in der Lieferkette: Der Umgang mit SBOMs und CBOMs ist für die gesamte Lieferkette einheitlich umgesetzt.	☐	☐	

[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