AQI Automotive Quality Institute

Risikofaktoren bezüglich der Software-Langzeitqualität

Risikofaktorenkatalog mit den zwölf Risikofaktoren inklusive Ursachen, Kategorisierung und möglicher Risikostrategien

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

Projektergebnisse

Im Rahmen des Projekts entwickelte Ergebnisse

AQI Automotive Quality Institute

Risikofaktorenkatalog

Es wurde ein Katalog entwickelt, der 12 wichtige Risikofaktoren für die Softwarelangzeitqualität in der Automobilindustrie umfasst.

Mögliche Ursachen

Risikokategorisierung

Strategien zum Umgang mit den Risiken

Geeignete Risikoanalyseverfahren

Detailierungsebenen der einzelnen Risikofaktoren

Überblick Risikofaktoren

AQI Automotive Quality Institute

01 Wartungsvertrag hat Lücken bezgl. der Software-Pflege
→ Langfristige Wartungsaufwände bis EOL nicht kalkulierbar

02 Eingeschränkte Durchführbarkeit von (F)OTA-Updates
→ Teure Werkstattaufenthalte zur SW-Aktualisierung notwendig

03 Keine langfristige Wartung durch Software-Lieferanten
→ Wartung der SW nur mit erheblichem Aufwand möglich, ggf. Neuentwicklung von SW-Komponenten notwendig

04 Kompetenz- und Wissensverlust während des Lifecycles
→ Benötigte Wartung und Pflege der SW kann nicht über lange Zeiträume sichergestellt werden
→ SW muss komplett neu entwickelt werden bzw. ältere HW muss im Fahrzeug durch neue HW ersetzt werden

05 Modularität und Abschaltbarkeit von Komponenten nicht ausreichend umgesetzt
→ Wartungskosten steigen signifikant mit dem Alter der Fahrzeuge

06 Software-basiertes Design von Komponenten nicht ausreichend umgesetzt
→ HW muss aufwendig ersetzt werden

07 Ab- und Aufwärtskompatibilität der Soft- und Hardware nicht gewährleistet
→ Aktuelle SW-Versionen können in älteren Fahrzeugen nicht installiert werden, für ältere und neuere Fahrzeuge muss unterschiedliche SW entwickelt werden (zusätzliche Kosten)

08 Anforderungen der Fehleranalyse für im Feld befindliche Fahrzeuge nicht im Design beachtet
→ Aufwendige Fehleranalyse, langsamer Fehlerabstellprozess, Kundenunzufriedenheit

09 Änderungen im normativen, rechtlichen Rahmenwerk oder im Stand der Technik
→ Langfristige Anpassungen an älteren SW-Ständen
→ Schwierige Umsetzung, da Zuständigkeiten unklar sind

10 Einzelne Elemente in der Lieferkette fallen (zeitweise) aus
→ Wartung (temporär) nicht möglich

11 Nichtverfügbarkeit von Infrastruktur oder Diensten
→ Dienste und Fahrzeugfunktionen sind eingeschränkt oder können nicht mehr angeboten werden

12 Akzeptanzverlust von Technologien & „Verhaltensweisen“ beim Endkunden
→ Image des Herstellers leidet

AQI Automotive Quality Institute

Erläuterung: Risikokategorien und Risikostrategien

Risikokategorien

Gruppierung nach Ursachen

AQI Automotive Quality Institute

01 Mensch

Risiken, die durch fehlende Kompetenz, fehlerhaftes Verhalten oder unzureichende Kommunikation der beteiligten Personen entstehen.

- Fehlerhafte Transaktionen
- Strategische Fehlentscheidungen, Fluktuation
- Humanvermögen (z.B. Kompetenzmangel, Know-how-Verlust)
- Unautorisierte/gesetzeswidrige Handlungen (intern)

02 Technologie

Risiken, die entstehen, wenn Fehler, Defekte oder Mängel in der Hardware, Software, Infrastruktur oder den technischen Systemen eines Unternehmens auftreten / im Design vorhanden sind.

- Systemsicherheit (z.B. fehlende Patches, veraltete Verschlüsselungsprotokolle)
- Softwarefehler (z.B. Bugs, Programmabstürze)
- Hardwarefehler (z.B. Serverausfall, Festplattendefekt)
- Infrastruktur (Gebäude, Anlagen)

03 Prozesse

Risiken, die sich aus Schwächen im Management, in Kontrollmechanismen und in operativen Abläufen ergeben.

- Management-, Kontroll- und Prozessschwächen
- Projektmanagement

04 Externe Einflüsse

Risiken, die durch äußere Einflüsse und Faktoren entstehen, die außerhalb der direkten Kontrolle des Unternehmens liegen.

- Gesetzeswidrige Handlungen, Betrug (extern)
- Politische Risiken
- Supply-Chain-Risiken, externe Dienstleister
- Infrastruktur (z.B. Strom, Netzinfrastruktur)
- Naturkatastrophen, sonstige Katastrophen
- Rechtliche Entwicklungen/Compliance

Der Begriff Risiko ist als Auswirkung von Unsicherheit auf Ziele definiert.
Eine Auswirkung stellt dabei eine positive und/oder negative Abweichung vom Erwartbaren dar.

Risikostrategien

Von uns gewählte vier Risikostrategien aus der Literatur

AQI Automotive Quality Institute

Die 4 Strategien befassen sich mit dem wirtschaftlichen Umgang des Schadens und dessen Folgen

Vermeidung

- Risikobehaftete Aktivität abbrechen oder nicht beginnen.
- Eliminierung der Eintrittswahrscheinlichkeit oder Schadensausmaßes.
- Verlust und Chance eliminiert.
- Mögliche Verschlechterung von Unternehmenszielen.

Vermindern/Begrenzen

- Reduzierung der Eintrittswahrscheinlichkeit oder Schadenshöhe.
- Sinnvoll bei hohen Eintrittswahrscheinlichkeiten.
- Durch: Personalschulungen, technische Maßnahmen (Sicherheitssysteme, Monitoring), Risiko-Streuung (Diversifikation von Ressourcen und Lagerorten).

Transfer

- Wechsel des Risiko-Trägers.
- Teilweise oder vollständige Übertragung auf Vertragspartner.
- Häufig durch Versicherungen bei niedriger Eintrittswahrscheinlichkeit aber hohem Schadenspotenzial.

Akzeptanz

- Risiko wird akzeptiert, Rücklagen werden gebildet.
- Entscheidung basiert auf Abwägung möglicher Folgen.
- Selbstversicherung, Einsparung von Versicherungsprämien.
- Unternehmen trägt Kosten im Schadensfall selbst.

Risikostrategien zielen darauf ab, wirtschaftlich mit Risiken und deren Folgen umzugehen. Im Fokus stehen die Vermeidung untragbarer Risiken, die Reduktion und der Transfer unvermeidbarer Risiken sowie unter bestimmten Voraussetzungen die bewusste Akzeptanz von Risiken. Eine effektive Strategie sichert den Unternehmenserfolg, indem sie Risiken angemessen steuert.

AQI Automotive Quality Institute

Risikofaktorenkatalog

RF01 Wartungsvertrag hat Lücken bezgl. der Software-Pflege

Mögliche Ursachen und Beispiele

AQI Automotive Quality Institute

Ursache 1.1: Zeiträume nicht klar definiert:

Beispiele:

- Keine klare Abgrenzung zwischen 1. Fehlerbehebung (Bug Fix), 2. Implementierung von Funktionen und 3. Cyber-Security
- Keine klare Definition der Zeiträume (z.B. aktive Phase und die passive Wartung; Neuverhandlungsklauseln für technische Rahmenbedingungen, die langfristig nicht kontrollierbar sind)
- Keine eindeutige und transparent geregelte Festlegung der Gewährleistungs- und Haftungszeiträume über die gesamte Zulieferkette

Prozessrisiko

Geeignete Risikoanalyseverfahren: z.B. „Simulation im V-Modell“ (siehe Projektbericht)

RF01 Wartungsvertrag hat Lücken bezgl. der Software-Pflege

Mögliche Ursachen und Beispiele

AQI | Automotive Quality Institute

Ursache 1.2: Benötigte Ressourcen nicht ausreichend festgelegt:

Beispiele:

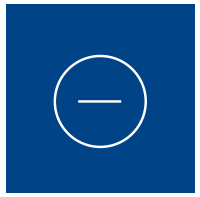
- Eine exakte Rollenverteilung innerhalb der Wartung fehlt, um die benötigte Wartung und Pflege der Software auch über längere Zeiträume sicherstellen zu können
- Unzureichende Zuteilung von langfristigen Ressourcen im Unternehmen / in der Lieferkette, um eine Unterstützung der Software-Wartung über lange Zeiträume anbieten zu können
- Langfristige Preisentwicklung wurde nicht genügend berücksichtigt für Wartung und Support

Prozessrisiko

Geeignete Risikoanalyseverfahren: z.B. „Simulation im V-Modell“ (siehe Projektbericht)

RF01 Wartungsvertrag hat Lücken bezgl. der Software-Pflege

Anwenden einer Vermeidungsstrategie (1/4)



Umsetzung (Beispiel)

- Verzicht auf externe (Software-)Lieferanten, Softwareentwicklung ausschließlich Inhouse (siehe z.B. Tesla), um Wartungsverträge zu vermeiden.

Bewertung

- Das eigentliche Problem der langfristigen Kalkulation der Wartungsaufwände wird nicht gelöst, die Komplexität ist allerdings geringer, als wenn die Softwareentwicklung in der Lieferkette realisiert wird.

Fazit

- Eine Konzentration auf die Inhouse-Entwicklung der Software ist wenig empfehlenswert, da das Problem der Kalkulierbarkeit weiterhin besteht. Das eigentliche Problem ist zwar weniger komplex als in der Lieferkette, besteht aber trotzdem weiter. Zudem kann Software nur dann Inhouse entwickelt werden, wenn entsprechendes Personal und Knowhow im Unternehmen in ausreichender Anzahl zur Verfügung stehen. In vielen Fällen gibt es weitere Gründe, die einer Softwareentwicklung Inhouse entgegenstehen.

RF01 Wartungsvertrag hat Lücken bezgl. der Software-Pflege

Anwenden einer Verminderungsstrategie (2/4)

Umsetzung (Beispiel)

- Langfristige Kalkulation der Wartungsaufwände mit Maßnahmenplanung in definierten Zeiträumen, basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen“, insbesondere sind die Punkte unter „1. Vertragsmanagement“ relevant.**

Bewertung

- Durch die genauere Planung und Kalkulation werden langfristige Wartungsaufwände vorhersehbarer und besser steuerbar.
- Allerdings erhöht dies die Komplexität und den Verwaltungsaufwand bei der Vertragsgestaltung durch z.B. unvorhergesehene Ereignisse wie Insolvenz, neue Regularien, etc.

Fazit

- Diese Strategie ermöglicht eine systematische und strukturierte Herangehensweise an die Wartung, reduziert das Risiko unvorhergesehener Kosten und fördert die Langzeitqualität der Software. Sie gilt als die sinnvollste Strategie in den meisten Fällen.

RF01 Wartungsvertrag hat Lücken bezgl. der Software-Pflege

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- OEM überträgt das Risiko durch vertragliche Regelungen an den Tier1-Lieferanten (bzw. TierX an TierX+1). Der Lieferant versucht, das Risiko in der Lieferkette weiterzugeben.

Bewertung

- Das Risiko wird nur verlagert und das Problem nicht gelöst. Während sich der OEM gegenüber dem Tier1 absichert, dass eine Wartung der Software über lange Zeiträume gewährleistet werden muss, geht der Softwarelieferant am Ende der Lieferkette so eine Verpflichtung oft nicht ein.

Fazit

- Diese Strategie kann zu instabilen Lieferketten führen, da der Tier1 oder ein nachgelagerter Lieferant das Risiko eventuell nicht tragen kann, was im schlimmsten Fall zur Insolvenz des Unternehmens führen könnte. Diese Konstellation gefährdet die Langzeitqualität und sollte daher vermieden werden. Stattdessen sollte das Problembewusstsein auf allen Ebenen der Lieferkette geschärft werden, um solche Risiken frühzeitig zu identifizieren und zu vermeiden.

RF01 Wartungsvertrag hat Lücken bezgl. der Software-Pflege

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Flexible Vereinbarungen zu Wartungsaufgaben werden zwischen Kunde und Lieferant im laufenden Betrieb getroffen und nicht über den Wartungsvertrag detailliert festgelegt.

Bewertung

- Das eigentliche Problem der fehlenden langfristigen Vereinbarungen zu den Wartungsaufwänden wird nicht gelöst, durch kurzfristige Vereinbarungen wird aber die Komplexität geringer.

Fazit

- Diese Strategie ist eher nicht empfehlenswert, da schwer kalkulierbare Kosten entstehen können. Sie kann jedoch in Situationen nützlich sein, in denen ein hohes Vertrauensverhältnis zwischen Kunde und Lieferant besteht, basierend auf einer langjährigen Zusammenarbeit. Kommt dazu ein schwer abschätzbarer Aufwand für langfristige Wartungsaufgaben, können entsprechende flexible Handhabung sowie Vereinbarungen der Wartungsaufgaben auch im laufenden Betrieb getroffen werden, besonders wenn für die Zukunft eine weitere enge Zusammenarbeit geplant ist.

RF02 Eingeschränkte Durchführbarkeit von (F)OTA-Updates

Mögliche Ursachen und Beispiele

Ursache 2.1 Schwächen im Design:

Beispiele:

- Die Fähigkeit zu (F)OTA-Updates wurde nicht konsequent ab Anfang an im Design jedes Bauteil mit Softwareinhalt beachtet
- Es wurde nicht sichergestellt, dass der Endkunde/Fahrer des Fahrzeugs wichtige (F)OTA-Updates nicht verhindern kann
- Ein Downgrade von Software ist nicht möglich, wodurch die Fehleranalyse eingeschränkt ist
- Die Dokumentation- und Updatestrategie ist nicht klar beschrieben und transparent umgesetzt

Technologisches Risiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, FTA (siehe Projektbericht)

RF02 Eingeschränkte Durchführbarkeit von (F)OTA-Updates

Mögliche Ursachen und Beispiele

AQI Automotive Quality Institute

Ursache 2.2 Fehlende oder lückenhafte Prozesse:

Beispiele:

- Einheitliche Prozesse und Schnittstellen in der Lieferkette für (F)OTA-Updates fehlen
- Es existiert kein Prozess, wie mit Fahrzeugen umgegangen wird, die sich dauerhaft/für einen langen Zeitraum in Regionen mit fehlender Funkverbindung befinden

Prozessrisiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, FTA (siehe Projektbericht)

RF02 Eingeschränkte Durchführbarkeit von (F)OTA-Updates

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Verzicht auf (F)OTA-Updates und Durchführung aller Software-Updates ausschließlich in der Werkstatt. Eine andere Vermeidungsstrategie ist schwierig, da (F)OTA-Updates in Fahrzeugen eine recht neue Technologie sind. Aufgrund der bisher noch begrenzten Erfahrungswerte ist es aktuell kaum möglich, Technologie und Prozesse so zu spezifizieren, dass (F)OTA-Updates unter allen denkbaren Bedingungen bei Bedarf durchgeführt werden können (auch wenn dies das langfristige Ziel sein sollte).

Bewertung

- Das Risiko wird vollständig vermieden, da keine (F)OTA-Updates durchgeführt werden.

Fazit

- Der Verzicht auf (F)OTA-Updates führt zu erheblich höheren Kosten durch notwendige Werkstattaufenthalte für jedes Software-Update. Zudem besteht ein erhöhtes Risiko für Verzögerungen bei sicherheitskritischen Updates, was potenziell zu Haftungsproblemen für den OEM führen kann, da für sicherheitskritische Updates ein deutlich größerer Zeitaufwand eingeplant werden muss. Zudem entsprechen (F)OTA-Updates inzwischen dem Stand der Technik, wodurch der Verzicht auf diese Technologie sogar zu rechtlichen Konsequenzen führen könnte, wenn es zu Schäden durch verspätete Sicherheitsupdates aufgrund notwendiger Werkstattaufenthalte kommt. Die Umsetzung ist daher nicht empfehlenswert.

RF02 Eingeschränkte Durchführbarkeit von (F)OTA-Updates

Anwenden einer Verminderungsstrategie (2/4)

Umsetzung (Beispiel)

- Implementierung von Technologien und Prozessen zur Erleichterung von (F)OTA-Updates basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „2. (F)OTA" relevant.**

Bewertung

- Reduziert das Risiko, indem wesentliche Voraussetzungen für (F)OTA-Updates geschaffen werden.
- Frühzeitige Berücksichtigung der Schnittstellen und Anforderungen im Entwicklungsprozess für stabile und sichere Implementierung von (F)OTA-Updates.

Fazit

- Durch die Implementierungen können teure Werkstattaufenthalte vermieden und der Aufwand für sicherheitskritische Updates reduziert werden, ohne jedoch den Anspruch zu erheben, das Risiko vollständig zu eliminieren. Dieser Ansatz stellt eine pragmatische Lösung dar, um die Vorteile von (F)OTA-Updates weitgehend zu nutzen und gleichzeitig die Risiken auf ein vertretbares Maß zu begrenzen.

RF02 Eingeschränkte Durchführbarkeit von (F)OTA-Updates

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- Weitergabe der Verantwortung für bestimmte Aspekte der (F)OTA-Updates an Lieferanten, indem vertraglich festgelegt wird, dass die Bauteile des Lieferanten bestimmte Voraussetzungen für (F)OTA-Updates erfüllen müssen. Bei Nichterfüllung haftet der Lieferant.

Bewertung

- Während das Risiko für bestimmte technische Aspekte auf den Lieferanten übertragen wird, bleibt die übergeordnete Verantwortung beim OEM, insbesondere aus Sicht des Endkunden.

Fazit

- Die Übertragung der Verantwortung für spezifische technische Anforderungen auf die Lieferanten kann eine sinnvolle Strategie sein, wenn bestimmte Bauteile nicht die vertraglich vereinbarten Voraussetzungen für (F)OTA-Updates erfüllen.
- Trotz dieser Maßnahme bleibt das Risiko beim OEM, da der Endkunde bei Bedarf eines zusätzlichen Werkstattbesuchs vermutlich den OEM verantwortlich machen wird. Deshalb ist diese Strategie nur bedingt empfehlenswert und sollte sorgfältig abgewogen werden.

RF02 Eingeschränkte Durchführbarkeit von (F)OTA-Updates

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Akzeptanz des Risikos eingeschränkter (F)OTA-Updates und Budgetierung für potenzielle Werkstattaufenthalte.

Bewertung

- Das eigentliche Problem wird nicht gelöst, da keine Präventivmaßnahmen ergriffen werden.

Fazit

- Verzögerungen oder Ausfälle bei (F)OTA-Updates haben für den OEM hohen Wartungskoste zur Folge, sowohl monetär durch Werkstattaufenthalte als auch nicht-monetär durch potenziellen Vertrauensverlust seitens der Kunden. Dennoch kann diese Strategie in bestimmten Situationen sinnvoll sein, z. B. wenn in einem Fahrzeug Bauteile verbaut sind, die keine (F)OTA-Updates unterstützen. Diese Strategie könnte auch in Fällen genutzt werden, in denen Bauteile erst nach der Fahrzeugauslieferung durch ein späteres Werkstatt-Update für (F)OTA-Updates tauglich gemacht werden können.

RF03 Keine langfristige Wartung durch Software-Lieferanten

Mögliche Ursachen und Beispiele

Ursache 3.1 Software-Lieferant (Unternehmen) existiert nicht mehr und kann nicht einfach ersetzt werden:

Beispiele:

- Es wurden keine Regelungen getroffen, damit nach der Insolvenz von Softwarelieferanten der Zugriff auf Quellcode, Dokumentation und Entwicklungstools der Software sichergestellt werden kann (z. B. über Escrow-Verträge)

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, Risikomatrix (siehe Projektbericht)

RF03 Keine langfristige Wartung durch Software-Lieferanten

Mögliche Ursachen und Beispiele

Ursache 3.2 Einsatz von Open-Source- oder Drittanbieter-Software ohne zusätzliche Maßnahmen für langfristige Wartung:

Beispiele:

- Es wurde freie oder Open-Source-Software eingesetzt, ohne sicherzustellen, dass langfristig eine zuverlässige und vertrauenswürdige Community für die Weiterentwicklung zur Verfügung steht
- Drittanbieter-Software/externe Bibliotheken werden nicht mehr vom Anbieter aktualisiert
- Bei Nutzung von lizenzierten Technologien/Anbietern kann die Software-Lizenz langfristig nicht verlängert werden

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, Risikomatrix (siehe Projektbericht)

RF03 Keine langfristige Wartung durch Software-Lieferanten

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Softwareentwicklung vollständig Inhouse durchführen, um die Abhängigkeit von einem externen Software-Lieferanten zu vermeiden und sicherzustellen, dass alle Ressourcen (Programmcode, Dokumentation, Entwicklungstools) im Unternehmen verfügbar sind.

Bewertung

- Das Risiko, dass ein externer Software-Lieferant die langfristige Wartung nicht übernimmt, wird vermieden.

Fazit

- Die Inhouse-Softwareentwicklung würde die Komplexität der langfristigen Wartung reduzieren, da alle notwendigen Ressourcen intern kontrolliert werden. Allerdings bleibt das Problem der langfristigen Wartung bestehen und muss intern gelöst werden, indem Mechanismen gefunden werden, die sicherstellen, dass eine langfristige Wartung mit kalkulierbarem Aufwand durchgeführt werden kann. Zudem erfordert die Inhouse-Entwicklung ausreichend qualifiziertes Personal und Know-how, was nicht immer verfügbar ist. Es gibt oft weitere Gründe, die gegen eine In-house-Entwicklung sprechen, wie zum Beispiel höhere Kosten oder fehlende spezialisierte Expertise.

RF03 Keine langfristige Wartung durch Software-Lieferanten

Anwenden einer Verminderungsstrategie (2/4)

Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen“, insbesondere sind die Punkte unter „1. Vertragsmanagement“, „5. Wartung & Pflege“ und „7. Zusammenarbeit in einer Tier-N-Lieferantenstruktur“ relevant.**

Bewertung

- Eine klare Regelung der Wartungsverpflichtungen minimiert das Risiko, dass Software unwartbar wird.
- Gleichzeitig bieten Escrow-Vereinbarungen zusätzliche Sicherheit.

Fazit

- Diese Strategie ermöglicht eine systematische und strukturierte Herangehensweise an die Wartung, reduziert das Risiko unvorhergesehener Kosten und fördert die Langzeitqualität der Software. Sie gilt als die sinnvollste Strategie in den meisten Fällen.

RF03 Keine langfristige Wartung durch Software-Lieferanten

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- OEM gibt das Risiko der langfristigen Softwarewartung vertraglich an den Tier1-Lieferanten weiter, der es möglicherweise an weitere Ebenen in der Lieferkette (TierX-Einkäufer der Software beim Softwarelieferenten) weitergibt.

Bewertung

- Das Risiko wird lediglich innerhalb der Lieferkette verlagert, bleibt aber bestehen.

Fazit

- Die Verlagerung des Risikos innerhalb der Lieferkette erweist sich als problematisch und ist daher nicht empfehlenswert. Diese Vorgehensweise kann die Stabilität der Lieferkette gefährden, da TierX-Lieferanten das Risiko möglicherweise nicht weitergeben können und es selbst tragen müssen. Besonders kleinere Unternehmen in der Lieferkette sind einem hohen Risiko ausgesetzt, das im schlimmsten Fall zu finanziellen Schwierigkeiten oder Insolvenz führen kann.

RF03 Keine langfristige Wartung durch Software-Lieferanten

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Akzeptanz des Risikos, dass der Softwarelieferant ab einem bestimmten Zeitpunkt keine Wartung mehr durchführt, und Ergreifen von Maßnahmen wie Minimierung, Abschaltung oder Ersetzung der betroffenen Funktionen und Dienste. Einplanung eines Budgets und entsprechender Ressourcen zur Reaktion auf das eintretende Risiko.

Bewertung

- Das Risiko kann erhebliche Auswirkungen auf die Funktionalität und Qualität der Software haben.

Fazit

- Meist nicht empfehlenswert. In bestimmten Situationen kann es jedoch sinnvoll sein, bewusste Funktionsverluste in Kauf zu nehmen, insbesondere wenn keine alternativen Anbieter für vergleichbare Softwareprodukte zu akzeptablen Preisen verfügbar sind oder wenn die Abschaltung oder Ersetzung der betroffenen Dienste möglich ist. Ein Beispiel hierfür wäre die Software eines Musik-Streaming-Dienstes: In diesem Fall könnte das Risiko akzeptiert werden, da der Dienst im Falle eines Marktrückzugs des Anbieters entweder abgeschaltet oder durch einen anderen Dienst ersetzt werden kann.

RF04 Kompetenz- & Wissensverlust während des Lifecycles

Mögliche Ursachen und Beispiele

Ursache 4.1: Langfristiger Wissenstransfer nicht ausreichend:

Beispiele:

- Maßnahmen zum Wissenstransfer und zur Erhaltung aller zur Softwarepflege und -wartung benötigten Kompetenzen und Tools (inklusive der notwendigen Software-Entwicklungstools und Artefakte) sind nicht ausreichend/strategisches Wissensmanagement unzureichend
- Die Zusammenarbeit hinsichtlich Kompetenzverteilung, Dokumentation, Know-how und Tools ist zwischen OEM und Zuliefern nicht klar geregelt

Menschliches Risiko | Prozessrisiko

Geeignete Risikoanalyseverfahren: z. B. SWOT-Analyse (siehe Projektbericht)

RF04 Kompetenz- & Wissensverlust während des Lifecycles

Mögliche Ursachen und Beispiele

Ursache 4.2: Beschränkung auf zukunftssichere Technologien bei der Softwareentwicklung unzureichend

Beispiele:

- Beschränkung auf zukunftssichere/State-of-the-Art Standards und Programmiersprachen wurde nicht konsequent (auch entlang der Lieferkette) umgesetzt

Prozessrisiko

Geeignete Risikoanalyseverfahren: z. B. SWOT-Analyse (siehe Projektbericht)

RF04 Kompetenz- & Wissensverlust während des Lifecycles

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Implementierung eines stetig fortlaufenden Schulungs- und Wissensmanagementsystems, welches sicherstellt, dass Kompetenzen und Wissen über lange Zeiträume (bis EoL der Fahrzeuge) hinweg erhalten bleiben.

Bewertung

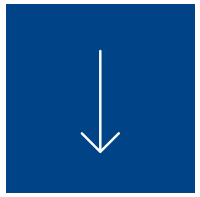
- Ein Schulungs- und Wissensmanagementsystems kann Wissen und Kompetenzen für eine bestimmte Zeit aufrechterhalten, aber langfristig wird dies immer schwieriger, da sich Technologien und Programmiersprachen weiterentwickeln und ältere Fachkenntnisse zunehmend verloren gehen.

Fazit

- Der Versuch den potenziell drohenden Wissensverlust präventiv zu adressieren ist grundsätzlich erstrebenswert, allerdings praktisch nur für begrenzte Zeiträume umsetzbar.
- Mit der fortschreitenden technischen Entwicklung wird es zunehmend schwieriger, die erforderlichen Kompetenzen aufrechtzuerhalten, z. B. ältere Programmiersprachen und Tools geraten in Vergessenheit, da Studium und Ausbildung von IT-Fachkräften auf den aktuellen Stand der Technik ausgerichtet sind.
- Daher ist die Vermeidungsstrategie, obwohl sinnvoll, nur begrenzt wirksam. Für sehr lange Zeiträume ist die Strategie der Reduzierung oder Begrenzung der Risiken besser geeignet.

RF04 Kompetenz- & Wissensverlust während des Lifecycles

Anwenden einer Verminderungsstrategie (2/4)



Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „5. Wartung & Pflege" relevant.**

Bewertung

- Der drohende Verlust von Kompetenz und Wissen kann minimiert werden.

Fazit

- Die Strategie bietet die Grundlage, um den Verlust von Wissen und Kompetenz über den Lifecycle zu minimieren.

RF04 Kompetenz- & Wissensverlust während des Lifecycles

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- Verpflichtung des Software-Lieferanten, notwendige Kompetenzen und Wissen langfristig zu erhalten, während das eigene Unternehmen diese Verantwortung weitgehend abgibt.

Bewertung

- Das Risiko des Wissensverlusts wird auf den Lieferanten übertragen, wodurch das Unternehmen selbst entlastet wird.

Fazit

- Ein kompletter Transfer der Verantwortung birgt ein erhebliches Risiko, da das Unternehmen stark abhängig vom Lieferanten wird.
- Wenn die internen Kompetenzen und das Wissen verloren gehen, fehlt dem Unternehmen die Fähigkeit, eigenständig Wartungen oder Anpassungen vorzunehmen.
- Zudem ist der Software-Lieferant bezüglich Erhaltung von Kompetenzen und Wissen mit den gleichen Problemen konfrontiert, wie das Unternehmen selbst.
- Bei einer möglichen Umsetzung muss sich das Unternehmen bewusst sein, dass der Transfer weitere Risiken hervorrufen kann.

RF04 Kompetenz- & Wissensverlust während des Lifecycles

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Akzeptanz des Risikos, dass Kompetenzen und Wissen mit zunehmendem technologischem Fortschritt verloren gehen, ohne aktiv dagegen vorzugehen. Insbesondere in Fällen, in denen der Wissenserhalt zu kostspielig wäre und die betroffene Software nicht unbedingt langfristig benötigt wird.

Bewertung

- Das Risiko wird bewusst in Kauf genommen, insbesondere für weniger kritische Softwarekomponenten.

Fazit

- Ein drohender Wissensverlust ohne entsprechende Gegenmaßnahmen kann zu langfristig zu hohen Kosten führen, wenn die Software neu entwickelt oder angepasst werden muss.
- In einigen Fällen jedoch sinnvoll, insbesondere wenn die Kosten für den Wissenserhalt unverhältnismäßig hoch sind und die betreffende Software keine kritische Funktion erfüllt.
- Ein Beispiel wäre die Akzeptanz des Risikos für Softwarekomponenten im Entertainmentsystem, wie etwa Musik-Streaming-Diensten. Hier kann der Endkunde beim Verlust der Funktionalität im Fahrzeug sein Smartphone als eine alternative Wiedergabequelle nutzen. Diese Komponenten können bei Bedarf abgeschaltet werden, ohne die wesentlichen Funktionen des Fahrzeugs zu beeinträchtigen.

RF05 Modularität & Abschaltbarkeit von Komponenten nicht ausreichend umgesetzt

Mögliche Ursachen und Beispiele

Ursache 5.1: Modulares Design nicht genügend berücksichtigt:

Beispiele:

- Strategie zur Abschaltbarkeit und zum Austausch von Funktionen und Softwarekomponenten sowie deren Umsetzung lückenhaft

Prozessrisiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, FTA (siehe Projektbericht)

RF05 Modularität & Abschaltbarkeit von Komponenten nicht ausreichend umgesetzt

Mögliche Ursachen und Beispiele

Ursache 5.2 Kommunikation gegenüber dem Endkunden über ggf. erfolgende Abschaltung von Funktionen nicht ausreichend

Beispiele:

- Gegenüber dem Endkunden wurde nicht klar und transparent kommuniziert, dass nicht alle im Neufahrzeug angebotenen Funktionen und Dienste kostenfrei bis End-of-Life des Fahrzeugs zur Verfügung stehen.
- Kommunikationsstrategie gegenüber dem Endkunden fehlt, welche Features des Fahrzeugs über den gesamten Lebenszyklus zur Verfügung gestellt werden und welche Features ein Enddatum haben und danach nur gegen Bezahlung oder gar nicht angeboten werden.

Prozessrisiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, FTA (siehe Projektbericht)

RF05 Modularität & Abschaltbarkeit von Komponenten nicht ausreichend umgesetzt

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Konsequent alle nicht gesetzlich vorgeschriebenen und verzichtbaren Komponenten, Dienste und Funktionen im Fahrzeug so gestalten, dass sie abschaltbar sind, ohne dass das Fahrzeug nicht mehr sinnvoll genutzt werden kann.
- Entsprechende Komponenten werden abgeschaltet, wenn der Wartungsaufwand mit dem Alter der Fahrzeuge stark ansteigt.

Bewertung

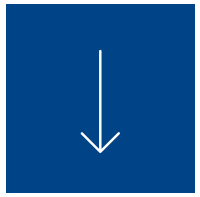
- Aus Sicht des OEM könnten steigende Wartungskosten bei alternden Fahrzeugen deutlich reduziert werden, indem nicht essenzielle Komponenten gezielt abgeschaltet werden, was den Aufwand und die Kosten für Wartung und Software-Updates minimiert.

Fazit

- Die Umsetzung ist zwar wünschenswert, aber in der Praxis oft schwer vollständig umzusetzen, da bestehende Fahrzeugarchitekturen oft nicht einfach angepasst werden können, und die Entwicklung neuer Architekturen, die eine umfassende Abschaltbarkeit ermöglichen, komplex und ressourcenintensiv ist.
- Eine Abschaltung einzelner Komponenten ist aufgrund vertraglicher Verpflichtungen gegenüber dem Endkunden nicht immer möglich. In einigen Fällen könnten dem Endkunden Entschädigungszahlungen zustehen, um den Verlust von Funktionalitäten auszugleichen.

RF05 Modularität & Abschaltbarkeit von Komponenten nicht ausreichend umgesetzt

Anwenden einer Verminderungsstrategie (2/4)



Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „4. Kompatibilität & Modulare Bauweise" relevant.**

Bewertung

- Diese Strategie trägt dazu bei, Modularität & Abschaltbarkeit im Rahmen der wirtschaftlich und technisch vertretbaren Möglichkeiten umzusetzen.

Fazit

- Geeignete Strategie zur Umsetzung von Modularität & Abschaltbarkeit.

RF05 Modularität & Abschaltbarkeit von Komponenten nicht ausreichend umgesetzt

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- Verpflichtung der Lieferanten, Modularität und Abschaltbarkeit in ihren bereitgestellten Komponenten, Diensten und Funktionen zu gewährleisten.

Bewertung

- Lieferanten tragen zur Risikominimierung bei, allerdings bleibt eine Restverantwortung beim OEM, der ebenfalls Maßnahmen zur Modularität und Abschaltbarkeit umsetzen muss.

Fazit

- Ein kompletter Transfer des Risikos ist nicht möglich, da der OEM oder der Lieferant, gegenüber seinen Unterlieferanten, in der Lieferkette weiterhin für die Gesamtkonzeption und die Implementierung von Modularität und Abschaltbarkeit verantwortlich bleiben.
- Daher ist diese Maßnahme eher als Teil der Strategie Verminderung/Begrenzung umzusetzen. Die Verpflichtung von Lieferanten kann sinnvoll sein, entlastet aber den OEM nicht vollständig von der Verantwortung.

RF05 Modularität & Abschaltbarkeit von Komponenten nicht ausreichend umgesetzt

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Akzeptanz des Risikos, dass Fahrzeugkomponenten aufgrund der aktuellen Fahrzeugarchitekturen nicht abgeschaltet werden können.
- Sicherstellung eines Mindestmaßes an Softwarewartung, einschließlich der Behebung von Sicherheitslücken, und Bereitstellung kompatibler Schnittstellen im Backend für vernetzte Systeme, die weiterhin funktionieren müssen.

Bewertung

- In aktuellen Fahrzeugarchitekturen können zahlreiche Komponenten nicht abgeschaltet werden. In diesem Fall gibt es für diese Komponenten keine andere sinnvolle Strategie außer die Akzeptanzstrategie.

Fazit

- Für nicht abschaltbare Komponenten die sinnvollste Strategie. Es muss allerdings in diesem Fall sichergestellt werden, dass eine notwendige Softwarewartung (z. B. Behebung von Sicherheitslücken) für diese Komponenten weiterhin möglich ist.

RF06 Software-basiertes Design von Komponenten nicht ausreichend umgesetzt

Mögliche Ursachen und Beispiele

Ursache 6.1: Hardware-basierte Realisierung von Funktionalität anstatt Software-basierte Umsetzung:

Beispiele:

- Für die externe Kommunikation notwendige Komponenten (z. B. Funkmodem) wurde nicht konsequent in Software realisiert, so dass auf Technologieänderungen (z. B. Abschaltung einer Mobilfunktechnologie) nicht einfach reagiert werden kann

Technologisches Risiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, SWOT-Analyse (siehe Projektbericht)

RF06 Software-basiertes Design von Komponenten nicht ausreichend umgesetzt

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Sämtliche hardwarebasierte Funktionalitäten werden durch softwarebasierte Lösungen ersetzt, um die Anpassbarkeit zu erhöhen.

Bewertung

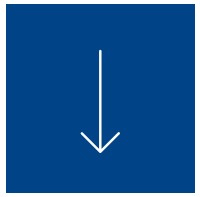
- Während eine vollständige Umstellung auf softwarebasierte Lösungen die Anpassbarkeit erleichtern könnte, ist dies in der Praxis weder vollständig möglich noch sinnvoll.
- Hardware hat in einigen Situationen auch spezifische Vorteile, wie höhere Sicherheit und Robustheit, die durch reine Softwarelösungen nicht immer gewährleistet werden können.

Fazit

- Eine vollständige Vermeidung durch reine Softwarelösungen ist in der Praxis nicht realisierbar.
- Softwarebasierte Lösungen erleichtern die Anpassbarkeit, erhöhen jedoch das Risiko von Cyberangriffen im Vergleich zu Hardwarekomponenten.
- Es sollte für jede Komponente abgewogen werden, ob eine softwarebasierte Lösung im Sinne der langfristigen Wartung sinnvoller ist. Beispielsweise könnte die Funktionalität eines Funkmodems softwarebasiert umgesetzt werden, um zukünftige Mobilfunkstandards zu unterstützen, während andere Komponenten besser in Hardware verbleiben. Diese Abwägung fällt eher unter die Strategie der Verminderung/Begrenzung.

RF06 Software-basiertes Design von Komponenten nicht ausreichend umgesetzt

Anwenden einer Verminderungsstrategie (2/4)



Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „4. Kompatibilität & Modulare Bauweise" relevant.**

Bewertung

- Funktionen werden, wenn möglich, konsequent in Software realisiert, um auf technologische Änderungen (wie z. B. Mobilfunkstandardabschaltungen) flexibel reagieren zu können, z. B. durch (F)OTA-Updates anstelle von Hardwareanpassungen.

Fazit

- Geeignete Strategie, um Software-basierte Lösungen überall dort einzusetzen, wo es technisch und wirtschaftlich sinnvoll ist.
- Es sollte für jede Komponente abgewogen werden, ob eine softwarebasierte Lösung im Sinne der langfristigen Wartung sinnvoller als eine Realisierung der Funktionalität in Hardware ist.

RF06 Software-basiertes Design von Komponenten nicht ausreichend umgesetzt

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- Verpflichtung der Lieferanten, bestimmte Funktionalitäten von Bauteilen und Komponenten durch softwarebasierte Lösungen, statt durch Hardware zu realisieren.

Bewertung

- Indem Lieferanten dazu angehalten werden, mehr softwarebasierte Lösungen zu entwickeln, kann die Anpassbarkeit und Wartungsfähigkeit verbessert werden.
- Allerdings bleibt eine Restverantwortung beim OEM, der ebenfalls eigene Maßnahmen zur Implementierung von softwarebasierten Lösungen umsetzen muss.

Fazit

- Ein kompletter Transfer des Risikos ist nicht möglich, da der OEM oder der Lieferant gegenüber seinen Unterlieferanten, in der Lieferkette weiterhin für die Gesamtkonzeption und die Implementierung von softwarebasierten Lösungen verantwortlich bleibt.
- Daher ist diese Maßnahme eher als Teil der Strategie Verminderung/Begrenzung zu betrachten.

RF06 Software-basiertes Design von Komponenten nicht ausreichend umgesetzt

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Akzeptieren des Risikos, dass in Hardware realisierte Funktionen nicht anpassbar sind, und Entwicklung einer Strategie zum langfristigen Umgang mit dieser Einschränkung (z. B. durch Lobbyarbeit zur Verzögerung der Abschaltung alter Mobilfunkstandards oder Budgetierung für den Hardwareaustausch).

Bewertung

- Das eigentliche Problem wird nicht gelöst, da die Hardware weiterhin nur eingeschränkte Anpassungsmöglichkeiten bietet und zusätzliche Maßnahmen notwendig werden, um den Betrieb langfristig sicherzustellen.

Fazit

- Zusätzliche Maßnahmen bringen sowohl erheblichen Extraaufwand als auch Kosten mit sich und sollten daher nur in spezifischen Fällen in Erwägung gezogen werden, wenn eine softwarebasierte Lösung entweder nicht möglich oder nicht sinnvoll ist.
- In Fällen, in denen eine hardwarebasierte Umsetzung erforderlich wird, sollten präventive Maßnahmen eingeplant werden. Dazu gehören die Budgetierung für zukünftige Hardwareaustausche sowie die Entwicklung von Strategien zur Abschaltung oder zum Ersatz der Hardwarekomponenten.

RF07 Ab- & Aufwärtskompatibilität der Soft- & Hardware nicht gewährleistet

Mögliche Ursachen und Beispiele

Ursache 7.1: Zu geringe „Überdimensionierung“ der Hardware:

Beispiele:

- Es wurde keine zum Auslieferungszeitpunkt überdimensionierte HW (z. B. leistungsstärkerer Prozessor oder größerer Speicher als nötig) verbaut, so dass längerfristig aufgrund der HW-Begrenzung nicht die aktuellste SW-Versionen eingespielt werden kann und somit die vorhandene ältere SW-Versionen separat mit Updates versorgt werden muss
- Zu verarbeitende und zu übertragende Datenmengen nehmen längerfristig stark zu und sind somit längerfristig zu hoch für die verbaute HW, so dass die Ausführung der aktuellen Funktionen und Dienste längerfristig träge wird bzw. nicht mehr möglich ist

Technologisches Risiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, FTA (siehe Projektbericht)

RF07 Ab- & Aufwärtskompatibilität der Soft- & Hardware nicht gewährleistet

Mögliche Ursachen und Beispiele

Ursache 7.2: Abwärtskompatibilität der entwickelten Software:

Beispiele:

- Neue SW-Stände sind nicht abwärtskompatibel zu älteren SW-Ständen, z. B. weil neue Features realisiert werden sollen, die eine Abwärtskompatibilität verhindern. Dies erhöht den Wartungsaufwand, weil ältere und neuere SW-Stände parallel gepflegt werden müssen.

Technologisches Risiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, FTA (siehe Projektbericht)

RF07 Ab- & Aufwärtskompatibilität der Soft- & Hardware nicht gewährleistet

Anwenden einer Vermeidungsstrategie-Aufwärtskompatibilität (1/4)

Umsetzung (Beispiel)

- Implementierung von Hardware, die zum Zeitpunkt der Inbetriebnahme des Fahrzeugs deutlich leistungsstärker als notwendig ist (leistungsstärkere Prozessoren und größere Speicherkapazitäten). Dabei müsste die Überdimensionierung so deutlich ausfallen, dass alle zukünftigen Softwareversionen problemlos unterstützt werden können.

Bewertung

- Eine solche Hardware-Überdimensionierung wird in vielen Fällen wirtschaftlich nicht sinnvoll sein, da teurere und leistungsstärkere Hardwarekomponenten eingesetzt werden müssen.
- Weiter schreitet die technologische Entwicklung in Bereichen wie Speicher und Prozessoren so schnell voran, dass die zum Zeitpunkt der Fahrzeugproduktion aktuelle Hardware wenige Jahre später bereits veraltet sein könnte. Dadurch kann der Vorteil der Überdimensionierung verloren gehen.

Fazit

- Aufgrund hoher Kosten und der technischen Einschränkungen ist die Umsetzung weder praktikabel noch empfehlenswert.
- Eine sinnvollere Herangehensweise wäre die Strategie der Verminderung/Begrenzung, bei der geeignete Maßnahmen zur Risikoabmilderung und zu einem ausgewogenen Verhältnis zwischen Kosten und Kompatibilität gefunden werden.

RF07 Ab- & Aufwärtskompatibilität der Soft- & Hardware nicht gewährleistet

Anwenden einer Vermeidungsstrategie - Abwärtskompatibilität (1/4)

Umsetzung (Beispiel)

- Sicherstellung, dass alle neuen Softwareversionen zu den in älteren Fahrzeugen verbauten Hardwarekomponenten vollständig kompatibel sind.

Bewertung

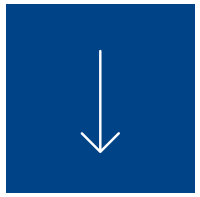
- Die Entwicklung neuer Softwareversionen wird erheblich eingeschränkt, da die Software auch generell ältere Hardware unterstützen muss. Dies würde in der Praxis dazu führen, dass innovative Features und technische Fortschritte in neuen Softwareversionen nur begrenzt oder gar nicht eingeführt werden können.
- In aktuellen Fahrzeugmodellen könnte dies zu einer veralteten und wenig attraktiven Software führen, was zu Unzufriedenheit bei den Endkunden führen könnte.

Fazit

- Es droht, dass sowohl Innovationsfähigkeit als auch Kundenzufriedenheit eingeschränkt werden. Daher ist das eine Umsetzung nicht empfehlenswert.

RF07 Ab- & Aufwärtskompatibilität der Soft- & Hardware nicht gewährleistet

Anwenden einer Verminderungsstrategie (2/4)



Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „4. Kompatibilität & Modulare Bauweise" relevant.**

Bewertung

- Die Ab- und Aufwärtskompatibilität sind strategisch berücksichtigt und implementiert. Eine Wirtschaftlichkeitsrechnung zur Bewertung von Kosten und Nutzen der Ab- und Aufwärtskompatibilität wird durchgeführt und berücksichtigt im strategischen Entscheidungsprozess.

Fazit

- Geeignete Strategie, um einen sinnvollen wirtschaftlichen und technischen Kompromiss bezüglich einer langfristigen Ab- und Aufwärtskompatibilität zu finden.

RF07 Ab- & Aufwärtskompatibilität der Soft- & Hardware nicht gewährleistet

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- Lieferanten werden vertraglich verpflichtet, sowohl die Abwärtskompatibilität der Software als auch die Aufwärtskompatibilität der Hardware sicherzustellen.

Bewertung

- Ein vollständiger Transfer des Risikos ist nicht möglich, da der OEM weiterhin eigene Maßnahmen, hinsichtlich der Sicherstellung und der Integration neuer und alter Technologien, implementieren muss, um die Kompatibilität sicherzustellen.

Fazit

- Die vertragliche Weitergabe von Maßnahmen seitens des OEMs an die Lieferanten kann eine geeignete und sinnvolle Ergänzung im Rahmen einer eigenen Strategie zur Risikominderung darstellen.

RF07 Ab- & Aufwärtskompatibilität der Soft- & Hardware nicht gewährleistet

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Akzeptanz, dass Software-Versionen neuerer Modelle nicht mehr in älteren Fahrzeugen installiert werden können, da die Hardware der älteren Fahrzeuge dafür nicht ausreichend und/oder die neue Software zu den älteren Modellen nicht mehr kompatibel ist.
- Daher Entwicklung einer Kommunikationsstrategie, um Kunden frühzeitig darüber zu informieren, dass Software-Updates mit neuen Funktionen für Fahrzeuge nur über einen begrenzten Zeitraum zu Verfügung stehen, und Sicherstellung, dass ältere Softwarestände weiterhin Sicherheitsupdates und Fehlerbehebungen gestellt bekommen.

Bewertung

- Das eigentliche Problem der fehlenden Abwärts- und Aufwärtskompatibilität wird nicht gelöst.

Fazit

- Eine Verminderung/Begrenzung-Strategie wäre vorzuziehen. In bestimmten Situationen, in denen keine Alternativen existieren, kann die Akzeptanz-Strategie jedoch notwendig sein.

RF08 Anforderungen der Fehleranalyse für im Feld befindliche Fahrzeuge nicht im Design beachtet

Mögliche Ursachen und Beispiele

Ursache 8.1 Unzureichende Dokumentation der Analysefähigkeit:

Beispiele:

- Standardisierte SBOM-Listen sind nicht Bestandteil der Dokumentation bzw. werden nicht regelmäßig gepflegt → Es ist nicht klar, welche Softwarebestückung (Versionsnummern aller Softwarekomponenten im Fahrzeug) in einem Fahrzeug, in dem ein Fehler auftritt, vorhanden ist

Prozessrisiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, HAZOP (siehe Projektbericht)

RF08 Anforderungen der Fehleranalyse für im Feld befindliche Fahrzeuge nicht im Design beachtet

Mögliche Ursachen und Beispiele

AQI Automotive Quality Institute

Ursache 8.2: Prozesse und Methoden zur Fehleranalyse lückenhaft

Beispiele:

- Teststrategien bzw. -umgebungen inkl. „Lagerung“ sind nicht ausreichend festgelegt und transparent geregelt
- Testumgebung (z.B. Fahrzeug mit bestimmter Hardware-/ Softwareausstattung) und Testzyklen inkl. der jeweiligen Verantwortlichkeiten sind nicht hinreichend festgelegt
- Vertragliche Regelungen zur Analyse- und Updatefähigkeit sind in der Lieferkette nicht ausreichend definiert (Umfänge, Zeiträume)

Prozessrisiko

Geeignete Risikoanalyseverfahren: z. B. FMEA, HAZOP (siehe Projektbericht)

RF08 Anforderungen der Fehleranalyse für im Feld befindliche Fahrzeuge nicht im Design beachtet

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Die Anforderungen für die Fehleranalyse werden bereits in den ersten Spezifikationen zur Umsetzung berücksichtigt, sodass das Thema Fehleranalyse konsequent im Design integriert wird.

Bewertung

- Diese Maßnahme trägt effektiv dazu bei, Probleme bei der späteren Fehlerbehebung zu vermeiden, indem sie sicherstellt, dass die Fehleranalyse der Software im Fahrzeug oder in vernetzten Systemen von Anfang an berücksichtigt wird. Allerdings kann die Umsetzung in der Praxis schwierig sein. Aufgrund der Komplexität könnten Lücken im Design erst dann entdeckt werden, wenn die Fahrzeuge bereits im Feld unterwegs sind und erste Probleme auftauchen.
- Es besteht auch nicht immer die Möglichkeit, bei allen beteiligten Stakeholdern durchzusetzen, dass die notwendigen Maßnahmen für eine umfassenden Fehleranalyse umgesetzt werden. Anbieter von Ladeinfrastruktur für E-Fahrzeuge werden wahrscheinlich nur eingeschränkt bereit sein, dem Fahrzeughersteller ihre Daten zu fehlerhaften Ladevorgängen zur Verfügung zu stellen.

Fazit

- Die Vermeidungsstrategie ist sehr empfehlenswert, um eine effiziente Fehleranalyse sicherzustellen.
- In der Praxis gibt es allerdings Hürden, die eine konsequente Umsetzung nicht immer möglich machen, weshalb häufig nur eine Strategie zum Vermindern/Begrenzen des Risikos möglich ist.

RF08 Anforderungen der Fehleranalyse für im Feld befindliche Fahrzeuge nicht im Design beachtet

Anwenden einer Verminderungsstrategie (2/4)

Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „3. Testing & Analyse" und „Zusammenarbeit in einer Tier-N-Lieferantenstruktur" relevant.**

Bewertung

- Eine Umsetzung der Maßnahmen kann dabei helfen, die kontinuierliche Fehleranalyse und -behebung zu verbessern.

Fazit

- In den meisten Fällen die sinnvollste Strategie, um die Anforderungen der Fehleranalyse umfassend umzusetzen.

RF08 Anforderungen der Fehleranalyse für im Feld befindliche Fahrzeuge nicht im Design beachtet

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- Um die Anforderungen für die Fehleranalyse von Anfang an konsequent im Design zu berücksichtigen, muss nicht nur das Gesamtfahrzeug, sondern auch alle verbauten Bauteile, Komponenten und die eingesetzte Software/Dienste mit einbezogen werden.
- Lieferanten sollten klare Vorgaben erhalten, um diese Anforderungen sicherzustellen.

Bewertung

- Diese Maßnahme entlastet den OEM oder den Lieferanten gegenüber seinen Unterlieferanten nicht davon, eigene Maßnahmen zur Risikominimierung umzusetzen. Ein vollständiger Transfer des Risikos ist somit nicht möglich.

Fazit

- Die Transfer-Strategie bezüglich der Lieferanten ist eine sinnvolle Ergänzung zur eigenen Risikominderungsstrategie und sollte auch verpflichtend an die Lieferanten weitergegeben und angewendet werden.

RF08 Anforderungen der Fehleranalyse für im Feld befindliche Fahrzeuge nicht im Design beachtet

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Wird dieses Risiko akzeptiert, bedeutet das, dass der Fehlerabstellprozess langsam und aufwendig verläuft und somit nicht nur die Kosten steigen, sondern auch die Kundenzufriedenheit sinkt.
- Für die Analyse und Behebung von Fehlern muss zudem zusätzliche Ressourcen eingeplant werden. Zudem sollte eine Strategie entwickelt werden, um unter anderen mit der daraus resultierenden Kundenunzufriedenheit umzugehen.

Bewertung

- In der Praxis kann es vorkommen, dass die Mängel in der Fehleranalyse erst entdeckt werden, wenn die Fahrzeuge bereits im Feld sind.
- Sollte zu diesem Zeitpunkt keine Risikominimierung mehr möglich sein, könnte die Akzeptanz-Strategie die einzige verbleibende Option sein, auch wenn sie zusätzliche Kosten und potenzielle Kundenschäden verursacht.

Fazit

- Diese Strategie sollte vermieden werden, sie muss jedoch in Betracht gezogen werden, wenn die anderen Strategien nicht anwendbar sind. Priorität sollte immer auf Maßnahmen zur Risikominderung und Begrenzung gelegt werden.

RF09 Änderungen im normativen, rechtlichen Rahmenwerk oder im Stand der Technik

Mögliche Ursachen und Beispiele

AQI Automotive Quality Institute

Ursache 9.1 Vorkehrungen bezüglich des normativen, rechtlichen Rahmenwerks sind lückenhaft

Beispiele:

- Dass langfristige Softwareanpassungen aufgrund von Gesetzesänderungen, Gerichtsurteilen, neuen Regulierungen oder neuen Normen/Standards notwendig werden können, wurde nicht ausreichend in der Planung (auch in der Lieferkette) berücksichtigt
- Verantwortungsbereich für die Aktualisierung von Softwarekomponenten aufgrund von Gesetzesänderungen, Gerichtsurteilen, neuen Regulierungen oder neuen Normen/Standards etc. wurde für die Lieferkette nicht sauber definiert
- Ein weltweites Screening, welche Gesetzesänderungen, Gerichtsurteilen, neuen Regulierungen oder neuen Normen/Standards etc. mittel- und langfristig anstehen könnten, ist nicht aus ausreichend erfolgt

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. Szenariotechnik, Gap-Analyse, PESTEL-Analyse (siehe Projektbericht)

RF09 Änderungen im normativen, rechtlichen Rahmenwerk oder im Stand der Technik

Mögliche Ursachen und Beispiele

Ursache 9.2: Vorkehrungen bezüglich Änderungen beim Stand der Technik (z. B. E-Roller als häufig anzutreffendes Verkehrsmittel) lückenhaft:

Beispiele:

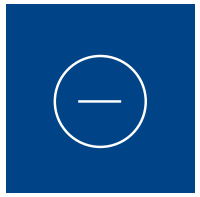
- Dass langfristige Softwareanpassungen aufgrund von Änderungen beim Stand der Technik notwendig werden können, wurde nicht ausreichend in der Planung (auch in der Lieferkette) berücksichtigt
- Verantwortungsbereich für die Aktualisierung von Softwarekomponenten aufgrund Änderungen beim Stand der Technik wurde für die Lieferkette nicht sauber definiert
- Ein Screening, welche Änderungen beim Stand der Technik mittel- und langfristig anstehen könnten, ist nicht aus ausreichend erfolgt

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. Szenariotechnik, Gap-Analyse, PESTEL-Analyse (siehe Projektbericht)

RF09 Änderungen im normativen, rechtlichen Rahmenwerk oder im Stand der Technik

Anwenden einer Vermeidungsstrategie (1/4)



Umsetzung (Beispiel)

- Eine Vermeidungsstrategie ist nicht möglich, da es sich bei Änderungen im normativ rechtlichen Rahmenwerk oder im Stand der Technik um externe Faktoren handelt, auf die ein Hersteller wenig Einfluss nehmen kann.
- Änderungen sind meist verbindlich und müssen eingehalten werden, beispielsweise kann es ein Hersteller in der Regel nicht vermeiden, bei Gesetzesänderungen die neuen Vorgaben umzusetzen.

RF09 Änderungen im normativen, rechtlichen Rahmenwerk oder im Stand der Technik

Anwenden einer Verminderungsstrategie (2/4)

Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „6. Risikomanagement" relevant.**

Bewertung

- Eine systematische Überwachung und Anpassung reduziert das Risiko, dass das Unternehmen unvorbereitet auf neue gesetzliche Anforderungen oder technische Entwicklungen trifft, erfordert jedoch entsprechende Investitionen in Personal und Prozesse.

Fazit

- Obwohl diese Strategie ressourcenintensiv ist, gewährleistet sie die Fähigkeit, schnell auf neue Anforderungen zu reagieren und mögliche Sanktionen oder Marktnachteile zu vermeiden.

RF09 Änderungen im normativen, rechtlichen Rahmenwerk oder im Stand der Technik

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- Vertragliche Weitergabe des Risikos bei Änderungen im rechtlichen Rahmen oder Stand der Technik vom OEM an Lieferanten oder Unterlieferanten.
- Der Lieferant muss in solchen Fällen Lösungen für die Änderungen bereitstellen.

Bewertung

- Für kleinere Lieferanten kann eine solche Verpflichtung existenzbedrohend sein, was zu instabilen Lieferketten führen könnte. Daher ist ein Risiko-Transfer mit Vorsicht zu betrachten und sollte nicht ohne eine sorgfältige Bewertung der Auswirkungen auf die gesamte Lieferkette erfolgen.

Fazit

- Ein Transfer des Risikos sollte nur mit Bedacht und vorzugsweise als Teil einer umfassenderen Verminderungsstrategie erfolgen, die das Unternehmen selbst ebenfalls verfolgt. Dies minimiert das Risiko von negativen Folgen für die Stabilität der Lieferkette.

RF09 Änderungen im normativen, rechtlichen Rahmenwerk oder im Stand der Technik

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Änderungen im rechtlichen Rahmenwerk oder Stand der Technik sind unvermeidlich und erwartbar, da diese Faktoren extern sind und daher wenig beeinflussbar, weshalb Unternehmen sie meist akzeptieren müssen.
- Unternehmen müssen Rücklagen bilden, um bei Änderungen schnell auf mögliche Risiken reagieren zu können.

Bewertung

- In der Praxis wird diese Strategie häufig angewendet. Ein Beispiel ist, wenn ein Gerichtsurteil den Hersteller verpflichtet, ältere Fahrzeuge umzurüsten. Der Hersteller veranlasst dann die Umrüstung in der Werkstatt und übernimmt die Kosten.

Fazit

- In Fällen, in denen externe Faktoren, wie gesetzliche Änderungen, nicht beeinflussbar, jedoch möglich sind, ist das Akzeptieren eine praktikable Lösung, um auf unvorhergesehene gesetzliche oder technische Änderungen zu reagieren. Diese Strategie erfordert jedoch eine entsprechende finanzielle Planung, um im Falle des Eintritts des Risikos schnell und effektiv die notwendigen Ressourcen bereitstellen zu können.

RF10 Einzelne Elemente in der Lieferkette fallen (zeitweise) aus

Mögliche Ursachen und Beispiele

Ursache 10.1: Normalerweise robuste Lieferketten werden in Extremsituationen unterbrochen und es kommt zu Engpässen in der SW-Wartung & -Pflege

Beispiele:

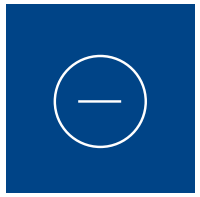
- Politische Konflikte, z. B. israelische Security-Experten werden in die Armee eingezogen und stehen nicht mehr zur Verfügung
- Sanktionen, Einfuhr- oder Ausfuhrbeschränkungen, Handelskriege
- Pandemie
- Blockierte oder eingeschränkte Schiffsrouten

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. Risikoanalyse entlang der gesamten Lieferkette (siehe Projektbericht)

RF10 Einzelne Elemente in der Lieferkette fallen (zeitweise) aus

Anwenden einer Vermeidungsstrategie (1/4)



Umsetzung (Beispiel)

- Verzicht auf externe (Software-)Lieferanten, Softwareentwicklung ausschließlich Inhouse (siehe z. B. Tesla).

Bewertung

- Eine Inhouse-Entwicklung von Software erfordert umfangreiches Personal und spezifisches Knowhow, das in ausreichender Menge im Unternehmen vorhanden sein muss.
- Jedoch fehlen oft diese Ressourcen, und es gibt zusätzliche Gründe, die einer internen Softwareentwicklung entgegenstehen.

Fazit

- Die vollständige Vermeidung von externen (Software-)Lieferanten kann theoretisch eine Lösung für das Risiko von Lieferkettenausfällen bieten, jedoch ist diese Strategie in der Praxis häufig nicht realisierbar und daher nicht empfehlenswert.

RF10 Einzelne Elemente in der Lieferkette fallen (zeitweise) aus

Anwenden einer Verminderungsstrategie (2/4)

Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „7. Zusammenarbeit in einer Tier-N-Lieferantenstruktur" relevant.**

Bewertung

- Robuste Notfallpläne und Risikoanalysen werden etabliert, um auf Engpässe in der Software-Wartung und -Pflege aufgrund von Extremsituationen wie politischen Konflikten, Umwelteinflüsse oder blockierten Handelsrouten schnell reagieren zu können.

Fazit

- In den meisten Fällen die sinnvollste Strategie, um die Auswirkungen von Ausfällen in der Lieferkette minimieren zu können.

RF10 Einzelne Elemente in der Lieferkette fallen (zeitweise) aus

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- OEM gibt das Risiko vertraglich an einen Lieferanten (bzw. Lieferant an einen Unterlieferanten) weiter, sodass dieser bei Ausfällen in der Lieferkette für eine Lösung sorgen oder für den Schaden haften muss.

Bewertung

- Diese Maßnahme kann kleinere Lieferanten in eine existenzbedrohende Lage bringen und somit zu instabilen Lieferketten führen, weshalb ein Risikotransfer riskant ist.

Fazit

- Ein Risikotransfer sollte immer mit Bedacht und eher im Rahmen einer Verminderungsstrategie erfolgen, die das Unternehmen auch selbst umsetzt.
- Eine vollständige Risikoübertragung ist nicht empfehlenswert, da sie die Stabilität der Lieferkette gefährden kann.
- Weiterhin kann beim Endkunden ein Reputationsverlust auftreten, der hauptsächlich den OEM trifft (wenn z. B. Ersatzteile für die Reparatur des Autos fehlen).

RF10 Einzelne Elemente in der Lieferkette fallen (zeitweise) aus

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Akzeptanz von temporären Wartungsausfällen und Entwicklung von Notfallplänen.

Bewertung

- Grundsätzlich ist diese Strategie nicht empfehlenswert, da es sinnvoller ist, im Rahmen einer Minderungsstrategie die Auswirkungen solcher Ausfälle zu reduzieren.
- In bestimmten Fällen kann die Akzeptanzstrategie jedoch notwendig sein, etwa wenn die Entwicklung und Wartung einer Software spezielles Wissen erfordert, das nur bei einem einzelnen Unternehmen vorhanden ist.

Fazit

- In Ausnahmefällen können einzelne Wartungsausfälle akzeptiert werden. Das Unternehmen muss sich jedoch der Auswirkungen bewusst sein und entsprechende Vorsichtsmaßnahmen ergreifen. Eine solche Konstellation sollte nach Möglichkeit vermieden werden.

RF11 Nichtverfügbarkeit von Infrastruktur/Diensten

Mögliche Ursachen und Beispiele

Ursache 11.1 Infrastruktur und Dienste, die als verfügbar und zuverlässig gelten, werden temporär gestört oder unterbrochen:

Beispiele:

- GPS-Störungen (z. B. durch atmosphärische Störungen oder Störsender)
- Ausfall von Mobilfunknetzen

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. Kritikalitätsanalyse, Szenarioentwicklung (siehe Projektbericht)

RF11 Nichtverfügbarkeit von Infrastruktur/Diensten

Mögliche Ursachen und Beispiele

Ursache 11.2 Infrastruktur und Dienste, die als verfügbar und zuverlässig gelten, werden eingestellt

Beispiele:

- Genutzte Protokolle (z. B. zur Datenübertragung, Verschlüsselung etc.) werden nicht mehr unterstützt
- Genutzter Mobilfunkstandard wird eingestellt

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. Kritikalitätsanalyse, Szenarioentwicklung (siehe Projektbericht)

RF11 Nichtverfügbarkeit von Infrastruktur/Diensten

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Bei der Entwicklung von Fahrzeugen und Baureihen wird darauf geachtet, dass alle Dienste und Funktionen im Fahrzeug ohne Vernetzung funktionieren und keine Abhängigkeit von Infrastruktur und Diensten außerhalb des Fahrzeugs besteht.

Bewertung

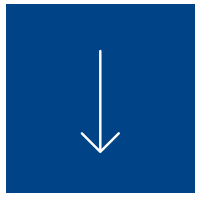
- Durch die Digitalisierung sind moderne Fahrzeuge zunehmend auf Vernetzung und externe Dienste angewiesen, um Daten aus verschiedenen Quellen zu beziehen und zu verarbeiten.
- Die vernetzten Dienste und Funktionen stellen den aktuellen Stand der Technik dar und werden auch von den Endkunden gewünscht. Ein Verzicht auf diese Vernetzung ist darum nur in Ausnahmefällen umsetzbar, beispielsweise für Spezialfahrzeuge, in denen der Einsatz von vernetzten Diensten und Funktionen keinen nennenswerten Mehrwert bringt.

Fazit

- Der Verzicht auf die Vernetzung von Fahrzeugen ist sehr selten sinnvoll und entspricht nicht dem Stand der Technik. Stattdessen ist eine Verminderungsstrategie deutlich sinnvoller, die darauf abzielt, die Auswirkungen der oben beschriebenen Ausfälle zu minimieren.

RF11 Nichtverfügbarkeit von Infrastruktur oder Diensten

Anwenden einer Verminderungsstrategie (2/4)



Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen", insbesondere sind die Punkte unter „6. Risikomanagement" relevant.**

Bewertung

- Maßnahmen zur Risikominimierung bei temporären Störungen von Infrastruktur und Diensten, wie GPS-Ausfällen oder Mobilfunkunterbrechungen, werden etabliert, um die Funktionsfähigkeit der Software zu gewährleisten.

Fazit

- In den meisten Fällen die sinnvollste Strategie, um die Auswirkungen von Nichtverfügbarkeit von Infrastruktur oder Diensten minimieren zu können.

RF11 Nichtverfügbarkeit von Infrastruktur/Diensten

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- In bestimmten Fällen kann ein OEM das Risiko vertraglich an einen Lieferanten (bzw. ein Lieferant an seinen Unterlieferanten) weitergeben, insbesondere wenn der Lieferant die Komponente herstellt, die auf die ausgefallene Infrastruktur oder den ausgefallenen Dienst angewiesen ist. In solchen Fällen muss der (Unter-)Lieferant eine Lösung bereitstellen oder für den entstandenen Schaden haften.

Bewertung

- Während diese Strategie für den OEM auf den ersten Blick vorteilhaft sein kann, kann sie für kleinere Lieferanten existenzbedrohend sein und zu instabilen Lieferketten führen.

Fazit

- Ein Transfer des Risikos sollte mit Bedacht umgesetzt werden und eher als Teil einer umfassenderen Verminderungsstrategie umgesetzt werden, die das Unternehmen auch selbst verfolgt.
- Bei nicht-verfügbaren Diensten im Fahrzeug kann beim Endkunden ein Reputationsverlust auftreten, der hauptsächlich den OEM trifft.

RF11 Nichtverfügbarkeit von Infrastruktur/Diensten

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Unternehmen akzeptieren, dass Infrastruktur und Dienste, aufgrund schwer beeinflussbarer oder unvermeidlicher Entwicklungen, bspw. durch die Abschaltung von Mobilfunkstandards, irgendwann nicht mehr zur Verfügung stehen werden.

Bewertung

- In bestimmten Situationen kann dies sinnvoll sein, insbesondere wenn Minderungsstrategien nicht anwendbar sind. Dennoch sollte immer versucht werden, die Auswirkungen durch Minderungsstrategien zu reduzieren.
- Es ist wichtig, Maßnahmen zu planen, die im Falle eines solchen Ausfalls zur Anwendung kommen können, wie beispielsweise die Abschaltung von Diensten und Funktionen, die auf Funkkommunikation angewiesen sind.

Fazit

- Eine Akzeptanzstrategie kann in manchen Fällen erforderlich sein, sie sollte jedoch nicht immer die bevorzugte Wahl sein.
- Eine Minderungsstrategie sollte, wo möglich, vorgezogen werden, um die Auswirkungen eines Infrastrukturausfalls zu minimieren (siehe auch Risikofaktor 5).

RF12 Akzeptanzverlust von Technologien & „Verhaltensweisen“ beim Endkunden

Mögliche Ursachen und Beispiele

Ursache 12.1 Das Wertesystem der Endkunden verändert sich:

Beispiele:

- Bisher akzeptierte Datenerhebung durch Fahrfunktionen etc. wird durch gestimmte Ereignisse (Presseberichte, Sicherheitsvorfälle, …) vom Endkunden als Überwachung wahrgenommen
- Bestimmte Nutzerinteraktion der Software gelten im Laufe der Zeit als diskriminierend
- Umweltfreundliches Verhalten/Energiesparen wird vom Endkunden im Laufe der Zeit viel kritischer eingefordert
- User Experience/User Interface nicht mehr an aktuelle Gewohnheiten angepasst

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. Szenariotechnik, SWOT-Analyse (siehe Projektbericht)

RF12 Akzeptanzverlust von Technologien & „Verhaltensweisen“ beim Endkunden

Mögliche Ursachen und Beispiele

Ursache 12.2 Der aktuelle Stand der Technik erzeugt beim Endkunden höhere Ansprüche:

Beispiele:

- User Experience/User Interface entspricht nicht mehr den aktuellen Gewohnheiten der Endkunden und wird als zu stark einschränkend wahrgenommen

Externes Risiko

Geeignete Risikoanalyseverfahren: z. B. Szenariotechnik, SWOT-Analyse (siehe Projektbericht)

RF12 Akzeptanzverlust von Technologien & „Verhaltensweisen“ beim Endkunden

Anwenden einer Vermeidungsstrategie (1/4)

Umsetzung (Beispiel)

- Aufgrund der fortschreitenden Digitalisierung und der damit einhergehenden technologischen Fortschritte kommt es im Laufe der Produktlebenszyklen immer wieder zu veränderten Anforderungen hinsichtlich des Kundenerlebnisses und der Usability. Dies führt dazu, dass Software-Funktionen oder -Designs, die zu Beginn des Lebenszyklus noch als modern und benutzerfreundlich galten, im Laufe der Zeit möglicherweise nicht mehr den aktuellen Erwartungen der Nutzer entsprechen.

Bewertung

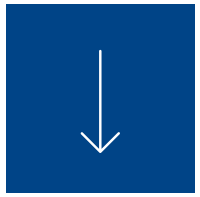
- Externe Faktoren, wie technologischem Fortschritt, sich wandelnden Nutzererwartungen oder Marktveränderungen, liegen meist nicht im Einflussbereich der Hersteller.

Fazit

- Das Risiko zu umgehen ist schwierig. Daher ist eine Vermeidungsstrategie für das Risiko, dass Technologien und „Verhaltensweisen“ von Software mit der Zeit beim Endkunden an Akzeptanz verlieren, in der Regel nicht umsetzbar. Stattdessen sollten Strategien zum Vermindern/Begrenzen des Risikos eingesetzt werden.

RF12 Akzeptanzverlust von Technologien & „Verhaltensweisen“ beim Endkunden

Anwenden einer Verminderungsstrategie (2/4)



Umsetzung (Beispiel)

- Mechanismen zur Reduktion des Risikos implementieren basierend auf der **Checkliste des AQI-Projekts „Langzeitqualität von Software-intensiven Systemen“, insbesondere sind die Punkte unter „6. Risikomanagement und 7. Zusammenarbeit in einer Tier-N-Lieferantenstruktur “ relevant.**

Bewertung

- Das Verhalten der Endkunden, beispielsweise in Bezug auf Datenschutz, Nutzerinteraktion und Umweltbewusstsein, wird regelmäßig analysiert, um frühzeitig auf veränderte Erwartungen reagieren zu können. Die User Experience und das User Interface der Software werden nach Möglichkeit angepasst.

Fazit

- In den meisten Fällen die sinnvollste Strategie, um Akzeptanzverlust zu verhindern und moderne Benutzeranforderungen zu erfüllen.

RF12 Akzeptanzverlust von Technologien & „Verhaltensweisen“ beim Endkunden

Anwenden einer Transferstrategie (3/4)

Umsetzung (Beispiel)

- OEM legt vertraglich fest, dass Lieferanten für die kontinuierliche Anpassung der Software verantwortlich sind, um sicherzustellen, dass diese den sich ändernden Kundenanforderungen etc. entspricht.

Bewertung

- Einen Transfer des Risikos an den Lieferanten wird ein OEM wahrscheinlich nur für einen begrenzten Zeitraum durchsetzen können.
- Endkunden nehmen dagegen wahrscheinlich den OEM als Verantwortlichen wahr, die Fahrzeugtechnologien und „Verhaltensweisen“ der implementierten Software auf den aktuellen Stand der Technik zu halten. Somit kann beim Endkunden ein Imageverlust bezüglich des OEMs entstehen, auch wenn dieser versucht, das Risiko zu einem Lieferanten zu transferieren.

Fazit

- Ein Risiko-Transfer auf den Lieferanten ist nicht sinnvoll.

RF12 Akzeptanzverlust von Technologien & „Verhaltensweisen“ beim Endkunden

Anwenden einer Akzeptanzstrategie (4/4)

Umsetzung (Beispiel)

- Unternehmen akzeptieren, dass der Endkunde die Fahrzeugtechnologien und „Verhaltensweisen“ der implementierten Software, die zu Beginn des Lebenszyklus noch als modern und benutzerfreundlich galten, ggf. als nicht mehr akzeptabel ansieht.

Bewertung

- Wenn die Auswirkungen dieses Risikos als gering eingeschätzt werden, können Unternehmen einen möglichen Akzeptanzverlust beim Endkunden bezüglich der in älteren Fahrzeugen eingesetzten Technologien durchaus akzeptieren.

Fazit

- Es sollte allerdings trotzdem versucht werden, im Rahmen einer Minderungsstrategie die Auswirkungen zu reduzieren (z.B. durch eine lange Bereitstellung von aktuellen Software-Updates), anstatt nur auf eine Akzeptanzstrategie zu setzen.
- Eine geeignete Kommunikation gegenüber dem Endkunden kann zudem dafür sorgen, dass keine Erwartungshaltung beim Endkunden entsteht, dass auch ein älteres Fahrzeug des Herstellers per Software-Update immer auf den aktuellen Stand der Technik gebracht wird (ähnlich zum Risikofaktor 5).