| Mögliche Safety-Risiken | Geeignete Safety-Schutzmaßnahmen |
|---|---|
| Inkompatibles Softwareupdate | **Übertragung und Vorab-Prüfung der vorhandenen Softwarekonfiguration** (*remote diagnosis*) im Hersteller-Backend mit geeigneter Kompatibilitäts- und Freigabedatenbank. |
| Unzureichendes Softwareupdate | **Software-Update-Packet-Management** (*package management*) zur Erkennung von Abhängigkeiten und Fehlkonfigurationen. |
| Unvollständige oder fehlerhafte Datenübertragung | **Download-Datenpuffer** zur Zwischenspeicherung bereits übertragener Daten bei sehr langsamen Verbindungen oder Verbindungsabbruch inklusive intelligenter Fehlerkorrektur (*corruption handling*) und Integritätsprüfung des gesamten Datenpakets nach Ende des Downloads. |
| Unzureichende Betriebsressourcen | **Vorab-Prüfung** aller notwendigen Betriebsressourcen wie Batterie und Speicher für den gesamten Updateprozess. |
| Ungeeignete Fahrzeugsituation | **Prüfung und Sicherstellung einer geeigneten Fahrzeugsituation** (z. B. Parkmodus) inkl. essentieller Notfunktionen (z. B. Türöffnung) während des gesamten Updateprozesses. |
| Flashspeicher wird durch häufige Schreibvorgänge fehleranfällig oder durch die Neuanordnung des Speicherabbilds verlangsamt (v. a. für Echtzeitanwendungen) | **Einsatz vielfach wiederbeschreibbarer Flashspeicher** mit z. B. mehr als 10.000 Schreibzyklen bei Fehlerraten kleiner 20 ppm über mindestens 20 Jahre. |
| Steuergerät kann/darf auch für ein Update nicht deaktiviert unterbrochen werden | **Redundanter Flashspeicher** und Redundanz aller weiteren ggf. unmittelbar vom Update betroffener Mikrocontroller-Ressourcen, um das Steuergerät im laufenden Betrieb zu aktualisieren und umzuschalten. |
| Benutzer ist mit Software-Update nicht einverstanden, möchte es abbrechen oder verschieben | Benutzer vorab über Art, Umfang und mögliche Folgen der Softwareaktualisierung sowie zur geschätzten Updatezeitrahmen informieren und wenn notwendig **Zustimmung einholen**. |
| Sonstige gezielte (z. B. durch den Benutzer in einer Notsituation) oder unvorhersehbare Abbrüche im laufenden Updateprozess | Erstellung eines lokalen **Notfall-Backups** im Fahrzeug und ggf. Wiederherstellung der Original-Software und/oder Integration eines (nicht überschreibbaren) Notbetriebsmodus. |

Tabelle 1: Übersicht möglicher Sicherheitsrisiken und geeigneter Schutzmaßnahmen für die effektive Absicherung der Funktionssicherheit (*safety*) für Over-the-Air-Software-Updates im Automobil. *Quelle: Escrypt*

| Mögliche Security-Risiken | Geeignete Security-Schutzmaßnahmen |
|---|---|
| Installation unautorisierter, manipulierter oder gefälschter Software | Absicherung und Prüfung aller Software-Updates über eine auf starker, etablierter Kryptografie (z. B. ECC-256) basierenden **digitalen Signatur** des Originalherstellers. |
| Ungewollte Installation ungewollter Software durch unautorisierte Personen | **Zwingende Zugriffskontrolle** (*mandatory access control*) des Updateprozesses mindestens basierend auf Zwei-Faktor-Authentifizierung, idealerweise inkl. Prüfung der physikalischer Präsenz (*physical presence*) des Fahrzeugbesitzers. |
| Datendiebstahl (*IP theft*) der Update-Daten | **Kryptografische Verschlüsselung** des Software-Updates mit etablierten kryptografischen Verfahren (z. B. AES-128), die nur vom und im Steuergerät selbst entschlüsselt werden kann. |
| Ausspähen der und ggf. böswilliger Eingriff in die Datenübertragung zwischen Backend und Fahrzeug | **Ende-zu-Ende-Verschlüsselung** des gesamten Kommunikationskanals mit etablierten kryptografischen Verfahren (z. B. TLS) mittels eines für jede Verbindung neu ausgehandelten, ausreichend langen kryptografischen Schlüssels (*session key*). |
| Missbrauch oder Manipulation (anderer) der Drahtlosschnittstelle oder anderer Fahrzeugelektronik über diese | Leistungsfähige **Embedded-Automotive-Firewall**, idealerweise mit dynamischem Regelwerk, geeigneter Heuristik, Paketfilterung und vollautomatischer Einbruchserkennung und Einbruchseindämmung (z. B. IDS bzw. IPS). |
| Abstreiten eines erfolgreich durchgeführten Software-Updates (z. B. Bezahl-Funktionen/Inhalte oder nach im späteren Fehler- oder Garantiefall) | Kryptografisch und redundant gesichertes **Log-Protokoll** aller durchgeführten Update-Vorgänge mind. mit Zeitpunkt/Nummerierung, Autorisation, Umfang und Ergebnis. Einsatz kryptografischer Zusatzfunktionen zur Nichtabstreitbarkeit (*non repudiation*) einer digitalen Transaktion – falls notwendig. |
| Manipulation, Deaktivierung, Umgehung oder Missbrauch der zur Absicherung verbauten Security-Mechanismen durch gezielte logische oder physische Eingriffe | Systematische **Evaluierung und Zertifizierung** aller Security-Mechanismen auf konzeptionelle Schwachstellen; regelmäßige Integritätsprüfung (z. B. via **Secure Boot**) aller Security-Mechanismen; strikte logische (z. B. via **Virtualisierung**) und physikalische Abschottung (z. B. via **Hardware Security Module**) aller Security-Komponenten während der Laufzeit; Möglichkeit zum sicheren **Update und Upgrade der Security-Funktionen** vorsehen (z. B. Krypto-Agilität). |

Tabelle 2: Übersicht möglicher Sicherheitsrisiken und geeigneter Schutzmaßnahmen für die effektive Absicherung der Informationssicherheit (*security*) für Over-the-Air-Software-Updates im Automobil. *Quelle: Escrypt*

Anmerkung: Die beiden Tabellen erheben keinen Anspruch auf Vollständigkeit und betrachten vor allem die technische Perspektive, ohne tiefer auf andere, beispielsweise organisatorische (wie geeignete Freigabeprozesse) oder rechtliche Risiken (wie unterschiedliche internationale Bestimmungen zum Datenschutz, Exportbestimmungen für Kryptografie) weiter einzugehen.