EMBEDDED SYSTEMS

Dual Banking für reibungslose **SOTA-Updates**

Upgrades für Fahrzeugfunktionen sind im Zusammenhang mit autonomen und vernetzten Automobilen von entscheidender Bedeutung. SOTA (Software Over the Air) Updates werden zukünftig der Standard bei Bugfixes, Erweiterungen und neuen Funktionsmerkmalen sein. Dual Banking ist in einem solchen Szenario für ein positives Kundenerlebnis unverzichtbar.

Bei Dual Banking ist der Speicherbedarf für updatefähige Softwarekomponenten in der ECU doppelt so hoch wie gewöhnlich. Der Speicher wird in zwei als Bank-A und Bank-B bezeichnete gleich große Partitionen aufgeteilt. Von den zwei Bänken ist zu jedem Zeitpunkt jeweils immer eine aktiv und die andere inaktiv. Die neue Software wird laufend in die inaktive Speicherbank heruntergeladen. Nach einem erfolgreichen Software-Update kann die neue Software dann durch Umschalten der Speicherbank ausgeführt werden. Die Funktionsmerkmale des Dual Banking sind in Bild 1 dargestellt.

Hintergrundprogrammierung

Während das Fahrzeug läuft, also während Software aus der aktiven Bank ausgeführt wird, kann das Telematiksteuergerät (TCU) im Fahrzeug die neuen Software-Updates empfangen, die dann in die inaktive Speicherbank der Ziel-ECU geladen werden. Dies wird als Hintergrundprogrammierung bezeichnet, und es gibt dabei keine Fahrzeugausfallzeiten aufgrund eines Software-Updates. Normalerweise wird die Software digital signiert und in die Ziel-ECU heruntergeladen, um nicht authentifizierte Updates zu vermeiden. Auch eine Fahrzeugdiagnose ist während der Hintergrundprogrammierung möglich.

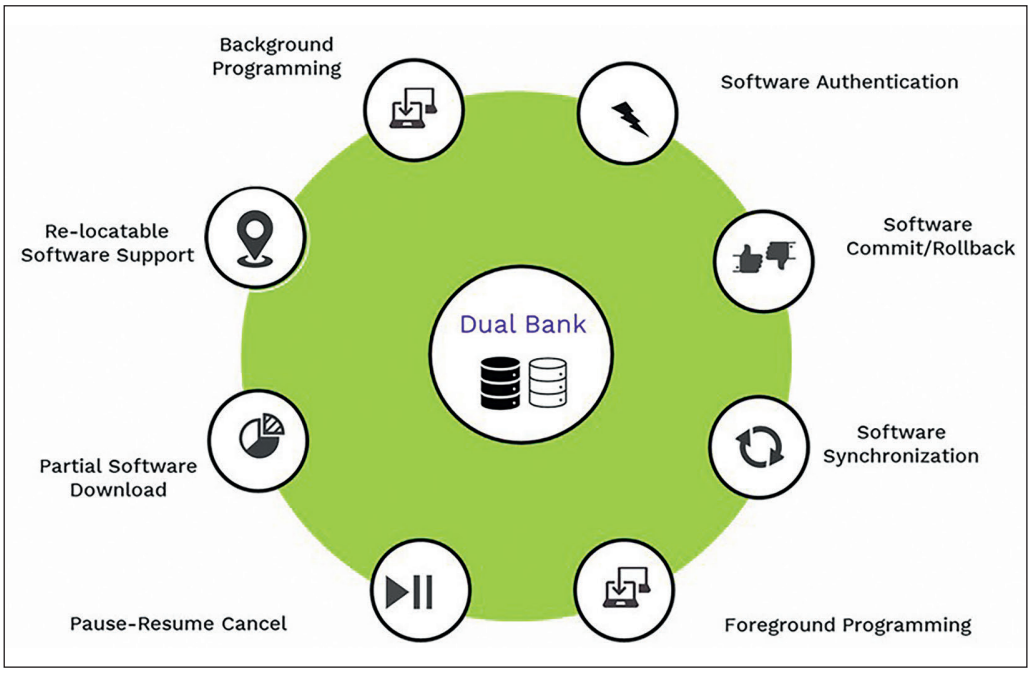

Bild 1: Dual Banking-Funktionen © KPIT Technologies

Software-Teildownload

Mit der Software-Teildownloadfunktion ist es nicht erforderlich, bei jedem Software-Update alle Softwarekomponenten einer ECU herunterzuladen. Es besteht die Möglichkeit, nur die überarbeiteten Softwarekomponenten einzeln herunterzuladen, um die Gesamtdauer des Updates zu verkürzen und die damit verbundenen Übertragungskosten zu reduzieren.

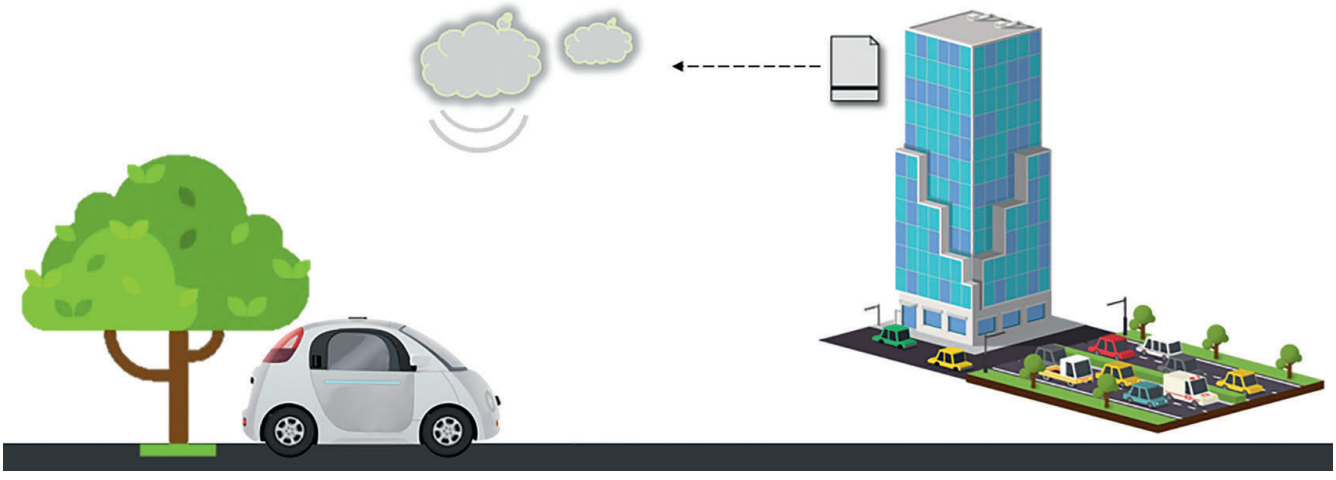

Bild 2: Software-Update bei laufendem Fahrzeug. © KPIT Technologies

Pause, Wiederaufnahme und Abbruch

Während der Hintergrundprogrammierung kann das Software-Update unterbrochen werden, wenn die ECU oder der Server offline geht und dann später bei erneuter Verfügbarkeit fortgesetzt oder abgebrochen werden. Auf diese Weise lassen sich die Gesamtdauer des Software-Updates und die entsprechenden Datenkosten reduzieren. Das unterbrochene/abgebrochene Software-Update wirkt sich in keiner Weise auf die ECU aus, da es sich in der inaktiven Speicherbank befindet.

Nach einem erfolgreichen Software-Update wird die aktualisierte Software beim nächsten Fahrzeugstart aus der Download-Speicherbank ausgeführt. Der Kunde kann die aktualisierte Software in ein paar Probeläufen nutzen und sie dann aktivieren, wenn er mit der Leistung der aktualisierten Version zufrieden ist.

Nach der Aktivierung der Software wird die aktive Speicherbank inaktiv und die Probelauf-Speicherbank aktiv. Ist der Kunde mit der Leistung der aktualisierten Software nicht zufrieden, kann er die vorherige Version der Software wiederherstellen, indem er einfach die Speicherbank umschaltet, sodass er von der neuen Version nicht betroffen ist.

Softwaresynchronisation

Sobald das Software-Update aktiviert ist, die frühere Version wiederhergestellt oder auch das Update abgebrochen ist, wird die Software bei laufendem Fahrzeug aus der aktiven Bank in die inaktive Bank kopiert. Dieser Vorgang wird als Softwaresynchronisation bezeichnet und ist nützlich, um zulässige Software in beiden Bänken der ECU sicherzustellen. Ist die Software in der aktiven Speicherbank aus irgendeinem Grund beschädigt, kann die Software aus der inaktiven Bank verwendet werden. In diesem Fall wird die aktive Bank zur inaktiven und die inaktive Bank zur aktiven, und die Software aus der neuen aktiven Speicherbank wird ausgeführt. Dies hilft, einen ECU-Ausfall zu verhindern und das Fahrzeug am Laufen zu halten.

Vordergrundprogrammierung

In Servicestellen kann die ECU per OBD neu programmiert werden, um den Bootloader bei Bugfixes, Erweiterungen und neuen Funktionen zu aktualisieren. Dies verbessert die SOTA-Updatefähigkeit des Fahrzeugs und trägt somit dazu bei, Stillstandszeiten zu vermeiden. Auch ist es immer möglich, mit einer solchen Vordergrundprogrammierung Komponenten der Anwendungssoftware zu aktualisieren.

Schnellere Umschaltung

Wenn der Ziel-Mikrocontroller in der ECU die Neuzuordnung logischer Adressen zu physikalischen Adressen unterstützt, kann die ECU-Software mit logischen Adressen aufgebaut werden, die sich aus einer beliebigen Bank ausführen lassen. Dies erleichtert eine schnellere Speicherbankumschaltung bei jedem neuen Software-Update und verhindert so mögliche Fahrzeugstartverzögerungen nach einem neuen Software-Update.

SW-Authentifizierung

Das SOTA-Update ist anfällig für Hacker-Angriffe. Um nicht authentifizierte Software-Updates zu vermeiden, muss die ECU-Software mit Signaturalgorithmen wie ECDSA, RSA und anderen digital signiert werden. Während des Software-Updates berechnet die ECU den Hash-Wert und verifiziert die Signatur der heruntergeladenen Software anhand des in der ECU gespeicherten öffentlichen Schlüssels/Zertifikats. Die heruntergeladene Software wird als gültig behandelt, wenn die Signaturverifizierung erfolgreich ist. Dieser sichere Download der Software hilft, die Programmierung nicht authentifizierter Software und somit Fahrzeug-Stillstandszeiten zu vermeiden.

Fazit

Es ist offensichtlich, dass Dual Banking durch die oben erläuterten Funktionen zur Verbesserung des Kundenerlebnisses beiträgt. Des Weiteren können auch Fahrzeugrückrufe wegen Software-Updates und die damit verbundenen Kosten vermieden werden. Eine problemlose Wartung, Software-Updates und -erweiterungen verbessern die Sicherheit und Leistungsfähigkeit des Fahrzeugs. Dies wiederum führt zu einem besseren Kundenerlebnis ohne Stillstandszeiten während der Software-Updates. ■ (oe)

www.kpit.com

Prabakaran Chinnasamy
ist Senior Solution Architect bei KPIT Technologies.