Flash-Speicher im Fokus von Safety und Security

Sicherheitsrisiken erkennen und beseitigen

Ob Infotainment-oder Fahrerassistenzsysteme – Flash-Speicher kommen in vielfältigen Automotive-Applikationen zum Einsatz und müssen immer mehr Funktionen steuern. Wichtig ist: Die Komponenten müssen hohen Safety- und Security-Anforderungen Genüge tun.

Adrian Cosoroaba

© Winbond

Das Internet of Things (IoT) bringt neue Möglichkeiten, als deren Folge sich die Art und Weise, wie Menschen leben, arbeiten oder spielen grundlegend verändert. Die zunehmende Vernetzung des Alltagslebens sorgt allerdings ebenfalls dafür, dass die Risiken durch Hacker und andere Sicherheitsverletzungen mit jedem neu hinzukommenden IoT-Gerät zunehmen. Bei den Geräten, denen Nutzer:innen am meisten vertrauen – nämlich Smartphones und Laptops – ist den meisten sehr wohl bewusst, weshalb die Sicherheit einen so hohen Stellenwert hat. Dabei übersieht man allerdings häufig die vernetzte Intelligenz, die sich inzwischen in den Fahrzeugen befindet (**Bild 1**). Tatsächlich ist es so, dass diese Systeme für Sicherheitsverletzungen geradezu prädestiniert sind. Ein Beispiel: Das Model 3 von Tesla gilt als eines der intelligentesten Autos auf dem Markt. Im März 2019 hatten Hacker das Infotainment-System dieses Fahrzeugmodells im Visier und konnten es mithilfe eines JIT-Bugs im Renderer unter ihre Kontrolle bringen. Das geschah zugegebenermaßen im Rahmen eines Hacking-Events, sodass für die Fahrzeugbesitzer keine Gefahr bestand. Dennoch zeigte dieser Hack klar und deutlich, dass die Sicherheit von Automobilelektronik-Systemen eine klaffende Lücke aufweist. Wenn Fahrzeuge immer intelligenter und zunehmend mit der wachsenden IoT-Infrastruktur der Welt vernetzt werden, muss diese Schwachstelle unbedingt berücksichtigt und beseitigt werden.

Security und Safety immer wichtiger

E/E-Systeme werden zusehends intelligenter. Dazu kommen im gesamten Fahrzeug immer mehr hochentwickelte elektronische Funktionen hinzu, zu denen Fahrassistenzsysteme, der Antriebsstrang, das Infotainment (**Bild 2**) sowie V2V- und V2X-Applikationen gehören. All das sorgt für einen zunehmenden Bedarf an Security und Safety. Insbesondere auch in Hinblick auf den Flash-Speicher, der zu einer entscheidenden Komponente dieser Systeme geworden ist. Flash-Speicher sind seit Jahrzehnten gebräuchlich und kommen mittlerweile auch im Automobilbereich zum Einsatz. Das Problem an aktuellen Embedded-Flash-Lösungen sind ihre erheblichen Sicherheitsrisiken, weil sie auf althergebrachten Technologien und Architekturen beruhen, denen es schlicht an der erforderlichen Zertifizierung fehlt, um Security und Safety garantieren zu können.

In E/E-Systemen sind Safety und Se-

Bild 1: Moderne Fahrzeuge sind immer vernetzter und bieten dadurch mehr Einfallstore für Manipulationen und Cyber-Angriffe. © Winbond

curity jedoch unabdingbare Voraussetzungen, um ein tolerierbares Risiko im Sinne der Norm ISO 26262 garantieren zu können. Zwar widmen sich die Automobilhersteller und ihre Zulieferer diesen Risiken. Doch angesichts steigender Komplexität der Fahrzeugelektronik liegt die funktionale Sicherheit (Safety) ebenfalls in der Verantwortung der IC-Hersteller. Hierdurch wiederum sind auch die Flash-Speicher betroffen, in denen kritische Programme und Daten abgelegt werden. Hier können latente Fehler auftreten, wie eine Funktionsstörung der ECC-Engine. Das Fehlerprotokoll im Winbond-Serial-NAND (**Bild 3**) trägt dazu bei, potenziell schwache Zellen oder Blöcke zu erkennen.

Unter dem Begriff Security versteht man im Kontext eines Fahrzeugs das Verbergen und Verschlüsseln aller denkbaren Informationen, um Datenlecks durch ausgefeilte Mechanismen wie etwa Seitenkanäle von vorherein auszuschließen. Die im Flash-Speicher abgelegten Daten müssen chiffriert werden, und auch für den Kommunikationskanal ist eine wirkungsvolle Verschlüsselung erforderlich. Bei der Safety im Automobilbereich geht es um 100-prozentige Beobachtbarkeit, Fehlerdetektierung und maximale Offenlegung von Informationen. Die Daten sind zu validieren, und Tests sollten ein hohes Qualitätsniveau von ca. null DPPM gewährleisten. Hinzu kommt eine Defektanalyse, die eine Qualitätsverbesserung und das Finden der Fehlerursachen ermöglichen sollte.

Bild 2: In Infotainment-Systemen kommen vermehrt Flash-Speicher zum Einsatz. Diese Bausteine können sicherheitsanfällig sein. © Mercedes-Benz

Security kein Nice-to-have

Es ist zwingend notwendig, dass Automobilhersteller und -Zulieferer unangenehme Fragen stellen – und zwar jetzt, und nicht erst dann, wenn es tatsächlich zu einer Sicherheitsverletzung gekommen ist. Autobauer können wählen, welche Art von Flash-Technologie sie einsetzen wollen, und diese Entscheidung hat großen Einfluss darauf, ob ein Fahrzeug geschützt oder für Cyber-Angriffe und Manipulationen anfällig ist. Bevor also entschieden wird, auf welches Flash-Produkt gesetzt wird, sollte man sich kritisch mit folgenden Punkten auseinandersetzen:

- Ist die Flash-Technologie gemäß CC EAL5+ zertifiziert, und wenn ja, auf welchem Level?

Eine geschützte Lösung ist ohne Zertifizierung nicht wirklich sicher und verlässlich. Die Zertifizierung gemäß CC

EAL5+ bedeutet, dass der betreffende Flash-Speicher die höchsten Security-Anforderungen jeglicher Automobil-Anwendungen einschließlich V2V und V2X erfüllt. Mit diesem Security-Niveau kann die Architektur selbst die geringsten unbefugten Änderungen an den Daten erkennen und sie umgehend dem Host melden. Die gespeicherten Daten sind vor jeglichen nicht autorisierten Modifikationen geschützt, ganz gleich, ob diese mit Absicht herbeigeführt werden oder durch einen Fehler entstehen. Jede solche Modifikation wird sofort dem Host gemeldet, und dieser Melde-Mechanismus kann außerdem nicht blockiert werden. Darüber hinaus sollte das Flash-Array durch eine zusätzliche CRC-Ebene geschützt werden. Die Flash-Logik enthält ferner anspruchsvolle Funktionen zum Detektieren eines jeden falschen Betriebszustands. Das SPI-Interface schließlich verfügt über eine weitere Verschlüsselungs- und Fehlererkennungs-Ebene, die es schützt und vor Fehlern bewahrt.

- Ist das Werk, in der die Flash-Lösung produziert wird, gemäß ISO 26262 zertifiziert?

Die 2011 eingeführte ISO 26262 ist ein Zertifizierungs-Indikator, mit dem sich verifizieren lässt, ob ein Zulieferer die Automotive-Safety-Integrity-Level-Vorgaben (ASIL) erfüllt. Die Safety-Zertifizierung gemäß ISO 26262 umfasst das Management der funktionalen Sicherheit, die Konzeptphase, Designs und Verifikationen auf der System-, Hardware- und Software-Ebene, die Bereiche Fertigung, Betrieb und Wartung sowie Dekommissionierungs-Dienste, womit der gesamte Produktlebenszyklus abgedeckt wird. Die Stufe ASIL-D der Norm ISO 26262 verkörpert den höchsten Grad an Risikomanagement. Für ASIL-D entwickelte Komponenten oder Systeme entsprechen somit den strengsten Safety-Anforderungen. Flash-Bausteine, in denen der Code für kritische Funktionen eines Fahrzeugs hinterlegt ist, sollten höchsten Safety-Anforderungen entsprechen und zur Senkung der Sicherheitsrisiken beitragen, indem sie für eine hochgradig zuverlässige Code-Speicherung sorgen.

- Ist die Security-Implementierung Upgrade-fähig und programmierbar? Wie sieht die Root-of-Trust-Implementierung (RoT) aus? Zeichnet sich die Lösung durch Plattform-Resilienz aus?

ECC Status		Descriptions
ECC-1	ECC-0	
0	0	Entire data is ouput is **successful**, without any ECC correction.
0	1	Entire data is ouput is **successful**, with 1~4 bit/page ECC corrections in either a single page or multiple pages.
1	0	Entire data output contains **more than 4 bits errors only in a single page which cannot be repaired by ECC**. In the Continuous Read Mode, an additional command can be used to read out the Page Address(PA) which had the errors.
1	1	Entire data output contains **more than 4 bits errors/page in multiple pages.** In the Continuous Read Mode, the additional command can only provide the last Page Address(PA) that had failures, the user cannot obtain the PAs for other failure pages. **Data is not suitable to use.**

Bild 3: Fehlerprotokoll im Serial-Nand-Flash von Winbond. Damit lassen sich fehleranfällige Zellen oder Blöcke erkennen. © Winbond

Geschützte Lösungen müssen unbedingt ein gewisses Maß an Plattform-Resilienz aufweisen, damit sie im Laufe der Zeit weiterentwickelt und angepasst werden können, um das System so vor Sicherheitsverletzungen zu schützen. Kommen traditionelle ROM- oder Embedded-Flash-Konzepte mit Mikrocontrollern oder SoCs zum Einsatz, wird der RoT-Code der Software-Implementierung im ROM gespeichert. Solche Systeme sind nicht Upgrade-fähig und besitzen nicht die nötige Resilienz für künftige Attacken. Moderne Konzepte basieren dagegen auf Mikrocontrollern/SoCs und programmierbarem, geschütztem Flash-Speicher. Weil die Implementierung dieser Lösungen auf Software und abgesicherter Hardware beruht, sind sie programmierbar und Upgrade-fähig. Diese Art eines programmierbaren, Hardware-basierten RoT lässt sich fortlaufend aktualisieren, um mit einem breiter werden Spektrum an Bedrohungen fertig zu werden und für Plattform-Resilienz zu sorgen.

Sicheres Flash-Speicher-Konzept notwendig

Nicht nur die soeben beschriebenen Gründe machen es notwendig, auf ein modernes Flash-Speicher-Konzept zu setzen. Im Unterschied zu älteren Flash-Technologien auf dem Markt bedarf es einer neuen Technologie, die über einen kryptografisch abgesicherten, standardmäßigen SPI-Bus den Transfer von Code und Daten zwischen einem geschützten Bereich und einem SoC oder Mikrocontroller erlaubt. Es ist wahrscheinlich, dass diese besser geschützten Flash-Lösungen zwingend erforderlich sein werden, um die Sicherheitsrichtlinien und -standards zu erfüllen. Das gilt insbesondere angesichts der ständig an Häufigkeit und Raffiniertheit zunehmenden Cyber-Attacken. Zu erwarten ist ferner, dass die Vorschriften strenger werden, wodurch die Wichtigkeit von Security und funktionaler Sicherheit in Automobilapplikationen weiter zunehmen wird.

Das Fahrzeug der Zukunft

Elektronik spielt heute in nahezu jedem Bereich des Fahrzeugs eine tragende Rolle – von der Karosserie über den Antriebsstrang bis hin zum Infotainment-System. Zukünftige Fahrzeuge werden noch mehr elektronische Bauteile beinhalten, denn Fahrer und Insassen fragen vermehrt nach Safety-, Security-, Infotainment- und Komfort-Funktionen nach. Zudem werden Gesetzesvorgaben hinsichtlich des Kraftstoffverbrauchs strenger. Folglich wird es immer wichtiger, dass die zentrale Technologie, zu der Flash-Speicher gehören, hohe Security- und Safety-Standards erfüllt. Weil Hacker immer kreativer werden und nur eine Schwachstelle ausreichend ist, müssen Halbleiterhersteller Konzepte entwickeln, um diese Attacken schnell und effektiv abzuwehren. Wenn es um die Sicherheit des Fahrzeugs geht, sollten Security und Safety keine zusätzlichen Kostenfaktoren sein. ■ (eck)

www.winbond.com

Adrian Cosoroaba ist Technischer Marketing Manager für sichere Speicher bei Winbond. © Winbond