Sicherheit in Industrie 4.0-Anwendungen

Wenn Mikrocontroller-basierte Sicherheit nicht mehr ausreicht

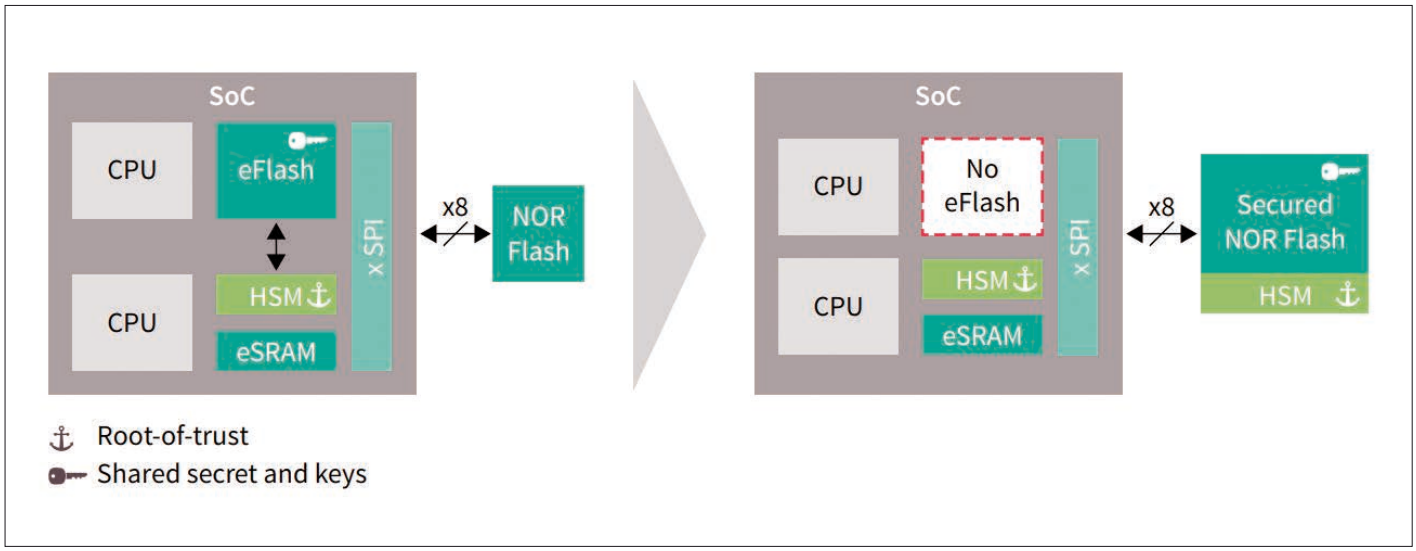
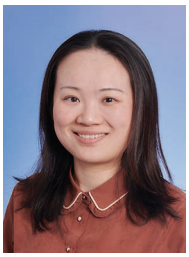


Bild 1: De-Integration von embedded Flash (eFlash) aus dem SoC. Alle Bilder © Infineon



Autoren:
Chen Grace Wang
Corporate Product Manager Digital
Rutronik Elektronische Bauelemente GmbH
www.rutronik.com

Slaven Dekic
Field Application Engineer Memory Solutions
Infineon Technologies
www.infineon.com

Eine Folge der Miniaturisierung von System-on-Chips ist es, dass der Flash-Speicher immer häufiger extern realisiert werden muss. Das bringt neue Sicherheitsanforderungen mit sich, die vor allem in unternehmenskritischen vernetzten Systemen dringend zu erfüllen sind.

Die rasante Zunahme vernetzter Systeme auf der ganzen Welt führt zu einem immer größeren Bedarf an Systemsicherheit. Denn jedes vernetzte intelligente Gerät ist ein potenzielles Ziel für Cyberangriffe. Gleichzeitig treiben die Fortschritte bei System-on-Chips (SoC) die Fertigungstechnologien auf die kleinsten sinnvollen Prozessknoten, um die für rechenintensive Anwendungen erforderliche Energie und Leistung zu erreichen. Die Integration von nichtflüchtigem Speicher (Non-Volatile Memory, NVM) wird mit der Verkleinerung der Prozessknoten auf 22 nm und darunter jedoch immer schwieriger. Insbesondere embedded NOR-Flash ist für die Implementierung in diese kleinen Knoten unerschwinglich geworden. Daher benötigen Systeme, die hochleistungsfähige SoCs verwenden, eine Alternative zu embedded Flash und kehren zu externen On-Board-Speichern zurück (Bild 1).

Modernste SoCs erfordern externen Flash-Speicher

Jahrzehntelang bestand die Strategie für die Entwicklung von elektronischen Systemen unabhängig von der Branche in der Regel darin, mehr Funktionen – inklusive größerer Speicherkapazität – in weniger Chips zu integrieren. Dieser Trend führte zu SoC-Architekturen, die komplexe Embedded-Systeme auf einem einzigen Chip ermöglichen. Um deren Leistung zu steigern und die Kosten zu senken, haben sich SoC-Anbieter auf innovative Fertigungs-Prozessknoten verlassen. Die Fortschritte in der Halbleitertechnologie haben jedoch dazu geführt, dass es immer schwieriger ist, Flash-Speicher in ein SoC einzubetten. Dies zwingt Systementwickler dazu, den kritischen Code und die Systemdaten in einem externen Flash zu speichern.

Vorteile

Das Design mit externem Flash bringt aber auch Vorteile mit sich: Das SoC kann allein aufgrund seiner Leistung gewählt werden. Die geeignete Flash-Dichte für das spezifische Design lässt sich unabhängig davon bestimmen.

Der Code wird immer größer und aktuelle Anwendungen speichern und verarbeiten mehr Daten als je zuvor. Selbst wenn ein SoC embedded NVM enthält, wird in vielen Fällen zusätzliche externe Speicherkapazität benötigt. Kann die am besten geeignete Kapazität des externen Flash-Speichers frei gewählt werden, reduzieren sich die Systemkosten und die Effizienz des Gesamtsystems wird optimiert.

Externe Speicher stellen andere Sicherheitsanforderungen

Der On-Chip-Speicher ist eng mit dem Rest des SoCs verbunden, in dem er sich befindet und gilt als grundsätzlich vertrauenswürdiger als herkömmlicher externer Speicher. Denn dieser ist als eigenständiges Gerät anfälliger für physische Angriffe. Selbst verschlüsselte Daten, die im externen Flash-Speicher gespeichert sind, können ein leichtes Ziel für bestimmte Angriffe sein. Zu den wichtigsten Bedrohungen, die bei der Sicherung von externem Flash-Speicher zu berücksichtigen sind, gehören:

- Nachahmung von Transaktionen in den Flash oder aus dem Flash ohne Autorisierung

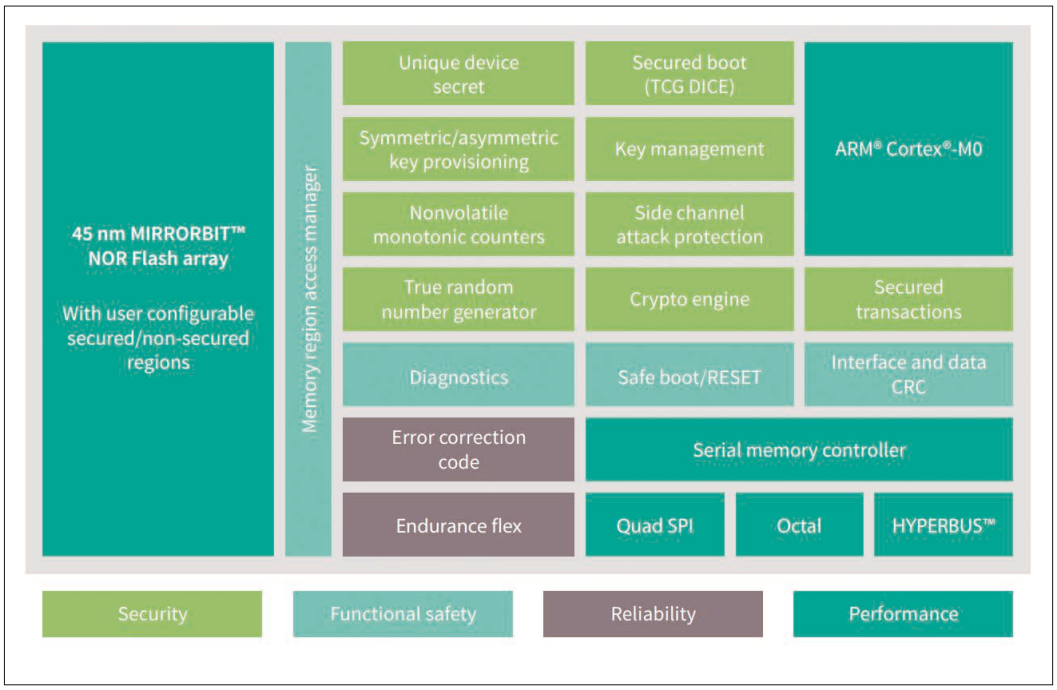


Bild 2: Mit SEMPER Secure NOR-Flash bietet Infineon den nach Herstellerangaben fortschrittlichsten, sichersten und zuverlässigsten Flash-Speicher der Branche.

- Manipulation des gespeicherten Codes, von gespeicherten Daten, Parametern und Protokollen
- Wiederholung von Transaktionen, um den Inhalt des Flash-Speichers auf alte, unsichere Versionen zurückzusetzen
- Beschaffung von Schlüsseln während der Bereitstellung in einer unsicheren Umgebung
- Snooping-Angriffe (Man-in-the-Middle) bei Transaktionen von/zu Flash-Geräten
- Durchführung von Seitenkanalangriffen auf Flash-Speicher, um dessen Inhalt zu beobachten oder sich diesen zu verschaffen

Lösungen

Um all diese Bedrohungen und andere Sicherheitsschwachstellen eines externen Flash-Speichers zu beseitigen, muss das Gerät folgende Funktionen bieten:

- Einen hardwarebasierten Vertrauensanker (Root-of-Trust), um eine Veränderung oder Manipulation, das Kopieren oder andere Auswirkungen eines Angriffs auf den im Flash-Speicher gespeicherten Code und/oder die Daten zu verhindern
- Sichere Updates vom Mikrocontroller oder der Cloud durch eine Kombination aus End-to-End-Schutz mit authentifizierten und verschlüsselten Transaktionen über den Bus, sicheren Regionen mit Lese-/Schreibzugriffsmethoden, sicherem Schlüsselspeicherplatz sowie nichtflüchtigen monotonen Zählern
- Geringe Kosten, weil keine zusätzlichen Sicherheitsvorrichtungen (z. B. ein Trusted Platform Module) erforderlich und keine Änderungen an den Leiterplatten nötig sind, inklusive der Unterstützung für gängige serielle Flash-Schnittstellen. Bild 2 zeigt das SEMPER Secure NOR-Flash. Damit bietet Infineon den nach Herstellerangaben fortschrittlichsten, sichersten und zuverlässigsten Flash-Speicher der Branche. Er ist auf funktionale Sicherheit ausgelegt, führt Diagnosen und Datenkorrekturen durch und entspricht den Anforderungen der ISO 26262. Auf dieser Basis fügt SEMPER Secure ein Hardware-Root-of-Trust sowie Optionen für asymmetrische oder symmetrische Kryptografie hinzu.

Sicherer Flash-Speicher für unternehmenskritische Anwendungen

Externe Flash-Speicher sind über eine serielle Speicherschnittstelle und einen Bus mit dem Host-SoC verbunden. Das macht sie anfällig für Replay-Angriffe und Man-in-the-Middle-Attacken. Weil kritische Daten zwischen mehreren Halbleiterbausteinen ausgetauscht werden, reicht es nicht aus, nur den Host-SoC zu schützen. Auch der externe Flash-Speicher und die bidirektionale Kommunikation zwischen beiden müssen gesichert werden.

SEMPER Secure (Bild 3) erweitert die sichere Verarbeitungsumgebung über den Host-SoC hinaus auf den externen NOR-Flash, indem er verschiedene Arten gesicherter Transaktionen unterstützt, darunter authentifiziertes Lesen, Programmieren und Löschen sowie verschlüsseltes Lesen, Programmieren und Löschen.

Lösen lässt sich dieses Problem durch Authentifizierung und/oder Verschlüsselung von Transaktionen zwischen dem Host-SoC und dem Speicher. So gewährleistet er Authentizität, Vertraulichkeit und Datenintegrität, schützt vor Replay-Angriffen und wird damit zur sicheren Lösung für unternehmenskritische Anwendungen.

Wer schreibt

Die Rutronik Elektronische Bauelemente GmbH feierte 2023 unter dem Motto „Committed to celebrate“ 50-jähriges Firmenjubiläum. Als unabhängiges Familienunternehmen steht der Distributor für ein nachhaltiges Wachstum mit Fokus auf Zukunftsmärkten, welche die Welt der Elektronik von morgen prägen werden: Advanced Materials, Advanced Measurement, Processing & Analytics, Advanced Robotics, Automation, Biotechnology, Energy & Power, Future Mobility, IIoT & Internet of everything, Industry 4.0, Medical & Healthcare sowie Transportation, Logistics & Supply Chain. ◄

Bild 3: SEMPER Secure erweitert die sichere Verarbeitungsumgebung über den Host-SoC hinaus auf den externen NOR-Flash.