MICRO CONSULT

Datensicherheit als Schlüsselkriterium für moderne mobile Systeme

Mit den neuen Generationen von Multicore-Mikrocontrollern können höchste Anforderungen an vernetzte Systeme und Datensicherheit erfüllt werden. Doch Entwickler brauchen von den Anforderungen bis hin zur Implementierung das richtige Wissen, um Daten in dieser Umgebung effizient zu schützen.

Selbst Smartphone-Modelle im Einsteigerbereich für um die 200 Euro verfügen heute bereits über einen Prozessor mit acht Kernen. Die neuen 32-Bit-Multicore-Mikrocontroller haben bei einer vergleichsweise geringen Taktzahl ein Vielfaches der Leistungsfähigkeit ihrer Singlecore-Vorfahren. Insgesamt steigt die **Leistungsfähigkeit** des Prozessors mit jedem weiteren Rechenkern. In Multicore-Systemen kann ein einzelnes Programm in kürzerer Zeit auf mehreren CPUs verarbeitet werden, oder es lassen sich mehrere Softwareaufgaben parallel ausführen.

Auch wenn die Leistungsfähigkeit ein wichtiger Treiber für die Entwicklung zu mehr Kernen war, spielt in mobilen Endgeräten die Ausdauer und damit die **Energieeffizienz** ebenfalls eine wichtige Rolle: Wie lange steht mir das Gerät mit nur einer Batterieladung zur Verfügung, bis ich es wieder ans Netzteil anschließen muss?

Bei einem mobilen Endgerät, das sich üblicherweise in unterschiedlichen Netzwerk-Umgebungen befindet und ununterbrochen Daten von Cloud Services über E-Mail, Social Media und Nachrichten-Apps empfängt, spielt ist die Datensicherheit essentiell. Das Smartphone ist heute identitätskritischer Bestandteil unseres Lebens und hat deshalb einen besonders genauen Blick auf die **Datensicherheit** verdient. Das mobile Multicore-System bedarf deshalb einer Krypto-Hardware mit hohen Anforderungen an die Verschlüsselung von gespeicherten Daten und Sendedaten. Je höher die Datensicherheit sein soll, desto aufwendiger sind die Verschlüsselungsmechanismen.

Zusammenfassend ist folgendes Dreigestirn für zuverlässige mobile Kommunikationssysteme von heute unabdingbar:

Leistungsfähigkeit + Energieeffizienz + Datensicherheit
= Moderne zuverlässige Mobilität

Wie ist ein moderner 32-Bit-Multicore-Mikrocontroller aufgebaut, und welche Bereiche sind besonders mit Verschlüsselung zu schützen?

1. Die **Bussysteme** verbinden die CPU mit Programm- und Datenspeicher und Peripherie-Modulen.
2. Im **Programmspeicher** werden die Ablaufsteuerungssequenzen (Programme) der unterschiedlichen Prozesse gespeichert.

3. Im **Datenspeicher** werden die Daten gespeichert, die während der Verarbeitung der Steuerungsabläufe entstehen.

Dazu kommen die **Peripherie-Module**:

- **Timer** für die zeitliche Steuerung und Überwachung von Programm- und Signalabläufen
- **Serielle Interfaces,** wie SPI-Interfaces zur Kommunikation mit Displayeinheiten, sowie USB-Module für die Kommunikation zu anderen USB-Geräten zur Speicherung von Daten über das USB-Protokoll (auf USB-Sticks o.ä.).
- **PWM-Units** zur Generierung von PWM-Signalen, z.B. zur Steuerung von Motoren, Helligkeit von LEDs usw.

Die richtige Speicher-Partitionierung – der Schlüssel zum Erfolg

Ein fehlerfrei funktionierendes System, das unterschiedliche Aufgaben gleichzeitig lösen und bearbeiten und dabei ohne Datenverlust oder ohne unbeabsichtigte Datenmanipulation auf gemeinsam verwendete Ressourcen (wie Programm-/Datenspeicher) zugreifen soll, benötigt strikt getrennte Speicherpartitionen bzw. zeitlich gesteuerte Zugriffe auf gemeinsam verwendete Speicherbereiche oder Peripheriemodule, beispielsweise ein USB-Interface.

Die CPUs dürfen sich also bei der Verwendung gemeinsamer Speicher und anderer Ressourcen für unterschiedliche Aufgaben in einem Mikrocontroller nicht in die Quere kommen. Ein erfolgreiches Software-Projekt erfordert eine klare Aufteilung und Trennung der verfügbaren Ressourcen auf die zu lösenden Softwareaufgaben.

Die Speicher-Partitionierung ist die Basis für

- konsistente Daten bei einer parallelen Datenverarbeitung
- sichere Daten für die Gewährleistung der Funktionalen Sicherheit
- verschlüsselte und damit geschützte Daten im Speicher und bei der Datenübertragung

Parallele Datenverarbeitung in Multicore-Mikrocontrollern

Multicore-Systeme machen es möglich, dass auf Smartphones oder Tablets gleichzeitig unterschiedliche Apps ausgeführt werden können. Damit dabei auch die „Privatsphäre“ der User-Daten sichergestellt wird, ist es zwingend notwendig, eine Speicherzugriffsteuerung in der Krypto-Hardware bereitzustellen. Im Mensch-Maschine-Umfeld (zum Beispiel im Automobil) mit seinen sehr harten Realzeit-Anforderungen gilt das ebenso. Hier sind hohe Sicherheitsanforderungen zu erfüllen; bei einer parallelen Abarbeitung der Software-Steuerungsmodule erfordert dies die strikte Synchronisation von Speicherzugriffen. Dazu stellt man sich folgende wichtige Fragen:

- Wann darf auf gemeinsam verwendete Speicherpartitionen zugegriffen werden?
- Wie kann der Zugriff auf diese Partitionen überwacht werden?

Für diese Echtzeit-Leistungsfähigkeit sind Mikrocontroller-Architekturen mit den folgenden wichtigen Merkmalen vonnöten:

- Multicore-Implementierung (mehrere CPUs in einem Mikrocontroller)
- Crossbar: Multi-Master/Multi-Slave Bus-Matrix
- Globale und CPU-lokale Speicherimplementierung
- MPU(s) – Memory Protection Unit(s)
- Krypto-Hardware zur Datenverschlüsselung

Sichere Daten für sichere Software: Funktionale Sicherheit

Für die Datensicherheit sind folgende Aspekte essentiell:

- **Speicheraufteilung**: Welche Applikation bekommt welche Speicherpartitionen zugewiesen?
- **Speicherzugriffssteuerung**: Wer darf wann auf eine gemeinsame Speicherpartition lesend oder schreibend zugreifen?

Jeder Lese- und Schreibzugriff muss während der Programmverarbeitung überwacht werden, damit nur zulässige Zugriffe durchgeführt werden. Werden verbotene Zugriffe erkannt, muss eine Fehlerbehandlungsroutine gestartet werden.

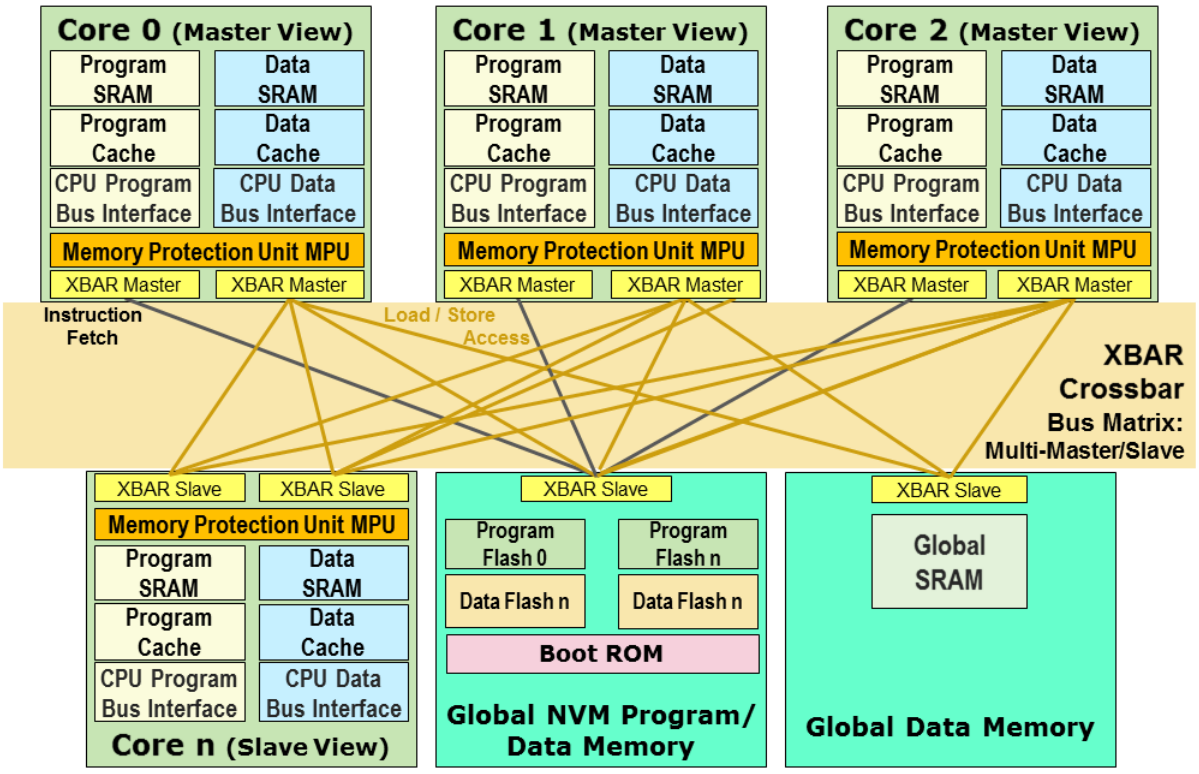

Bild 1: Multicore-Architektur – Zugriff auf gemeinsame Ressourcen mit XBAR-Bus

Die Memory Protection Unit (MPU) verhindert via Speicherzugriffssteuerung unerlaubte Speicherzugriffe. Dazu bestimmt der Entwickler für jeden Teil der Applikation (z.B. für jede Software-Task), welche Programmspeicher gelesen und welche Applikationsdaten in den Datenspeichern und Peripherie-Modulen nur gelesen, nur geschrieben oder gelesen und geschrieben werden dürfen (*Read*, *Write* und *Read-Write*-Protection). Will ein Programmteil bzw. eine Task auf einen nicht freigegebenen Speicherbereich zugreifen, verhindert die MPU den Zugriff und ruft eine MPU-Fehlerroutine (Error Task) auf.

Daten so sicher wie in einem Tresor

Sollen Daten im Speicher und bei einem Datenaustausch zwischen verschiedenen Geräten geschützt werden, kommt die Datenverschlüsselung ins Spiel. Eine Applikation, die sensible Daten verarbeiten soll, muss Speicherinhalte vor unerlaubten Zugriffen (im Speicher und bei der Datenübertragung) durch Verschlüsselungstechniken schützen. Dazu werden eigene Security-System-on-Chip (SoC) Strukturen eingesetzt und abgegrenzte Security-Bereiche auf einem Mikrocontroller definiert. Diese Bereiche sind mit einer Firewall geschützt, die unberechtigte Zugriffe auf den geschützten Bereich verhindern sollen.

Die neuesten Multicore-Architekturen bieten ein Hardware-Security-Modul (HSM), um erweiterte Sicherheitsanforderungen zu erfüllen, z.B. seitens der KfZ-Hersteller nach erweitertem Schutz ihrer Systeme gegen Manipulation und/oder gegen potenzielle Hacker-Angriffe. So wird die Sicherheit der Personen im Fahrzeug und die der Verkehrsteilnehmer außerhalb gewährleistet.

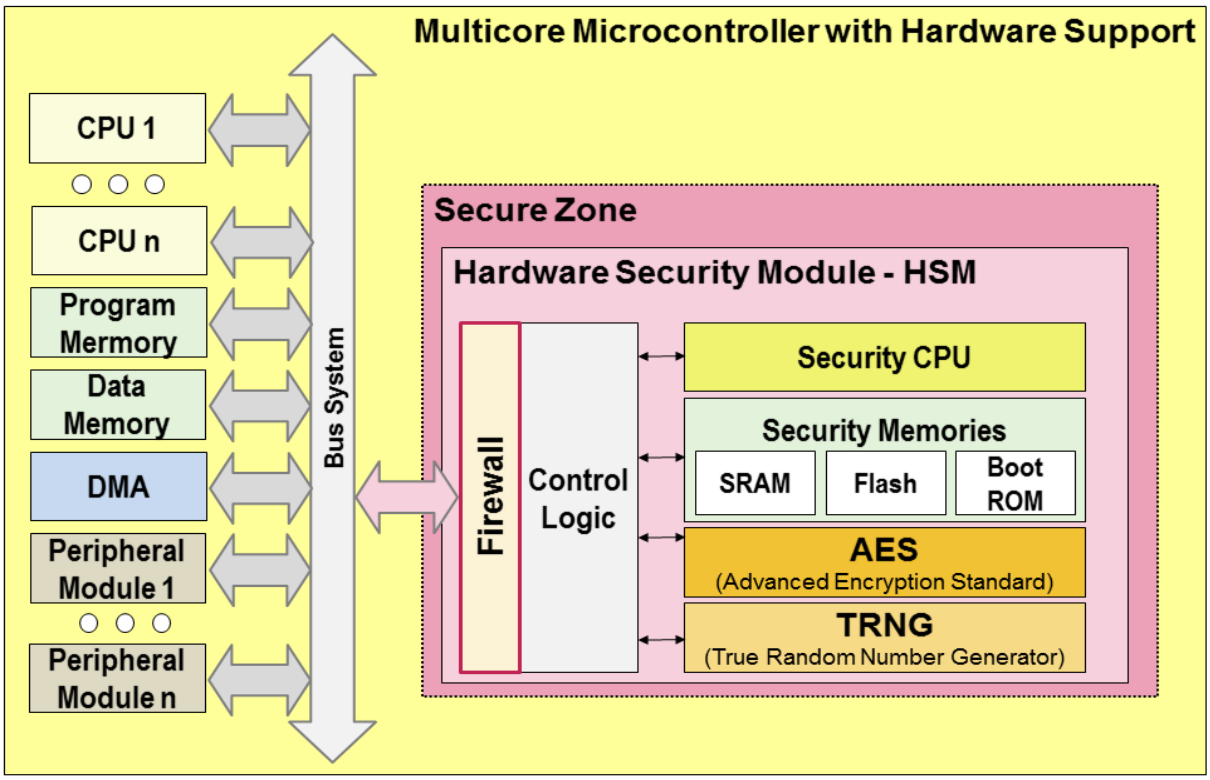

Bild 2: Multicore Microcontroller mit Hardware Security Modul – HSM

In der “sicheren Zone” eines Mikrocontrollers verarbeitet eine eigene CPU Security-Applikationen. Diese geschützte CPU verfügt über verriegelte Speicher (ROM und RAM), auf die die anderen CPUs und Bus-Master (wie das DMA-Modul) des Multicore-Mikrocontrollers nicht zugreifen können.

Richtig sicher wird das **H**igh **S**ecurity **M**odule (HSM) durch einerseits das **Krypto-Hardwaremodul** (z.B. Advanced Encryption Standard Modul AES) sowie durch den **True Random Number Generator** (TRNG), der gleich mehrere Funktionen hat:

- Erzeugen von sicheren kryptographischen Schlüsseln (Secure Cryptographic Key Generation)
- Sichere Speicherung kryptographischer Schlüssel (z.B. Master Keys) in einem nichtflüchtigen Key-Speicher (Non-volatile Memory NVM, z.B. in einem Daten-Flashmodul)
- Verwaltung der kryptographischen Schlüssel (Key Management)
- Verarbeitung und Management kryptographischer Daten in Secure-Funktionen (Verschlüsselungs- und Signaturfunktionen)

Holen Sie sich das richtige Wissen, um Daten in dieser Umgebung effizient zu schützen – von den Anforderungen bis hin zur Implementierung.

MicroConsult bietet Ihnen professionelle Trainings und Coachings rund um die Themen Multicore-Mikrocontroller, Safety, Security, Requirements Engineering, Softwarearchitektur uvm. an.

Weiterführende Informationen

MicroConsult Training & Coaching zum Thema Multicore

MicroConsult Training & Coaching zum Thema Safety & Security

Alle MicroConsult Trainings & Coachings

MicroConsult Fachwissen zum Thema Multicore

MicroConsult Fachwissen zum Thema Safety & Security

Autor:

Ingo Pohle ist Mitgründer und Geschäftsführer der MicroConsult GmbH und international anerkannter Spezialist für Embedded-Lösungen, mit einem reichen Erfahrungsschatz rund um den Einsatz von Embedded-Mikrocontrollern, Bussystemen und RTOS.