ORAN absichern: Halbleiterlösungen für den Netzwerkschutz

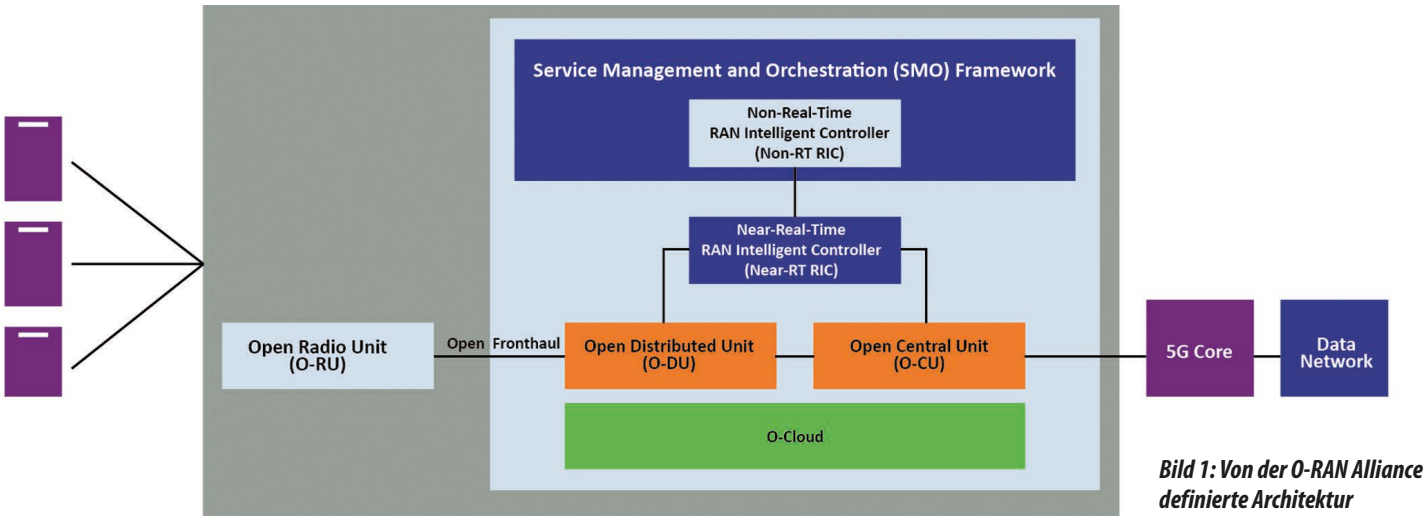

Bild 1: Von der O-RAN Alliance definierte Architektur

Offene Funkzugangsnetze (ORANs, Open Radio Access Networks), unterstützt von Organisationen wie dem Telecom Infra Project (TIP) und der O-RAN Alliance, bieten klare Vorteile gegenüber herkömmlichen, geschlossenen Netzwerken. Um ORAN erfolgreich einzuführen ist jedoch das Entbündeln von Hardware und Software mittels standardisierter, offener Schnittstellen und Protokolle sowie interoperabler Hardware von mehreren Anbietern erforderlich. Kritisch ist auch die Netzwerksicherheit, da Mobilfunknetzbetreiber (MNOs, Mobile Network Operators) bei der Bereitstellung von ORAN-Infrastrukturen Cybersicherheitsrisiken berücksichtigen müssen.

Bild 1 zeigt eine ORAN-Netzwerkarchitektur gemäß der O-RAN Alliance. Die wichtigsten Funktionsblöcke sind die Funkeinheit (RU, Radio Unit), die dezentrale Einheit (DU, Distributed Unit) und der intelligente RAN-Controller (RIC).

Autor:
Thomas Gleiter
Staff Segment Manager der Timing and Communication Group
Microchip Technology
www.microchip.com

Marktdimension

Der weltweite ORAN-Markt, der Hardware, Software und Dienstleistungen umfasst, wird voraussichtlich von 1,1 Mrd. US-$ im Jahr 2022 auf 15,6 Mrd. US-$ im Jahr 2027 wachsen [1]. Dieses Wachstum wird vor allem von MNO vorangetrieben, die von den geringeren Ausrüstungskosten, der verbesserten Netzwerkleistung und der größeren Flexibilität profitieren möchten, die sich aus dem Übergang von geschlossenen, proprietären Systemen hin zu offenen Infrastrukturen ergeben, die auf Multi-Vendor-Ökosystemen basieren. Gleichzeitig besteht ein starker politischer Wille, die Entwicklung von ORAN voranzutreiben – insbesondere durch die Ankündigung, dass im Rahmen des US „CHIPS and Science Act“ von 2022 1,5 Mrd. US-$ für die Entwicklung von ORAN-Systemen bereitgestellt werden.

Sicherheitsherausforderungen für ORAN

Die Schaffung fragmentierter (disaggregierter) Netzwerke mit Produkten verschiedener Anbieter birgt das Risiko, dass ORAN anfälliger für Cyberangriffe sind als ihre „geschlossenen“ Pendants. Auf dieses Potenzial haben insbesondere die US National Security Agency (NSA) und die Cybersecurity and Infrastructure Security Agency (CISA) [1] in ihrem Papier „Open Radio Access Network Security Considerations” hingewiesen. Darin wurden die Sicherheitsaspekte im Zusammenhang mit der Implementierung eines Open RAN gemäß der Architektur und Spezifikationen der O-RAN Alliance bewertet.

Das Papier befasst sich mit der Sicherheit verschiedener technischer Aspekte von ORAN, die von der Verwaltung mehrerer Hersteller über Funk-ICs/-Systeme und Basisstationsausrüstung bis hin zu künstlicher Intelligenz (KI) und allgemeinen Netzwerkaspekten reichen. Darin heißt es: „Die Einführung von Open RAN bringt neue Sicherheitsaspekte für Mobilfunknetzbetreiber (MNO) mit sich. Ein offenes Ökosystem, das eine disaggregierte Umgebung mit mehreren Anbietern umfasst, erfordert naturgemäß eine besondere Konzentration auf Veränderungen der Angriffsfläche an den Schnittstellen zwischen den über die Architektur integrierten Technologien. Neben den Sicherheitsaspekten der Integration von Komponenten verschiedener Hersteller müssen sich Dienstanbieter auch mit anderen Aspekten befassen. Diese hängen mit der Nutzung von Open-Source-Anwendungen und neuen 5G-Netzfunktionen und -Schnittstellen zusammen, deren Standards sich noch in der Entwicklung befinden.

Darüber hinaus müssen MNOs Sicherheitsaspekte berücksichtigen, die zwar nicht ausschließlich mit Open RAN zusammenhängen, aber dennoch relevant sind, z.B. Cloud-Infrastruktur, Virtualisierung, Containerisierung und Distributed-Denial-of-Service-/DDoS-Angriffe.“

Eine der Herausforderungen bei Technologien von mehreren Anbietern ist die Frage, wo die Verantwortung für die Sicherheit liegen sollte. Bei traditionellen und proprietären Netzwerk-Designs lag die Verantwortung für Implementierungsfragen in der Regel bei einem einzigen Anbieter. Im ORAN-Zeitalter müssen MNO jedoch mehr Zeit investieren, zu ermitteln, welche Anbieter für die Sicherheit verantwortlich sind. Zu beachten ist auch, dass viele Betreiber ORAN auf der Grundlage bestehender LTE-Kernnetze aufbauen werden, die selbst anfällig für passive Abhör- und aktive „Man-in-the-Middle“-Angriffe sein können. Darüber hinaus wird die Angriffsfläche mit der steigenden Anzahl vernetzter Geräte weiter zunehmen.

Mit zunehmendem Aufwand für das Sicherheits-Management besteht die Gefahr, dass die Kosten für die Risikominderung die Kosteneinsparungen zunichte machen, die als einer der Hauptvorteile von ORAN angepriesen werden.

Die Möglichkeiten der Virtualisierung führen zu cloudbasierten Implementierungen von RANs. MNO sollten daher in der Lage sein, einige der Sicherheitsbedrohungen durch die robusten Sicherheitsfunktionen etablierter Cloud-Computing-Architekturen abzuwehren. Viele Netzwerke werden jedoch möglicherweise nicht oder nur in begrenztem Umfang virtualisiert, da die Kostenvorteile (die anfänglichen als auch die laufenden Gesamtbetriebskosten) wahrscheinlich der wichtigste Faktor für die Akzeptanz der jeweiligen Implementierungen sein werden.

ORAN-Sicherheit im Fokus

Unabhängig von der Virtualisierung bestehen weiterhin viele Anforderungen an die physische Sicherheit auf Hardware-Ebene. Um diese Sicherheit zu gewährleisten und die Vorteile von ORAN zu erhalten, suchen Systementwickler verstärkt nach Standard-Halbleiterbauelementen und Hardware-Plattformen, die speziell für den Schutz vor Cyberangriffen entwickelt wurden. Dazu gehören Embedded-Prozessoren mit integrierten Sicherheitsfunktionen und zertifizierte TPM (Trusted Platform Modules), die auf branchenweit anerkannten Spezifikationen basieren.

Kernprinzipien

Besonders relevant sind dabei Richtlinien, die OEMs und Bauteilhersteller bei der Implementierung verbesserter Sicherheitsmaßnahmen in kritischen Infrastruktursystemen unterstützen. Dazu zählen die Richtlinien der NIST Special Publication 800-193, die Empfehlungen für mehr Widerstandsfähigkeit von Plattform-Firmware und -Daten gegen potenziell schädigende Angriffe enthalten.

Die NIST-Richtlinien beziehen sich auf die Hardware- und Firmware-Komponenten, die zum Starten und Betreiben eines Systems erforderlich sind – im Hinblick auf Angriffe, die ein System vorübergehend oder dauerhaft außer Betrieb setzen und zu erheblichen Störungen für die Nutzer führen könnten.

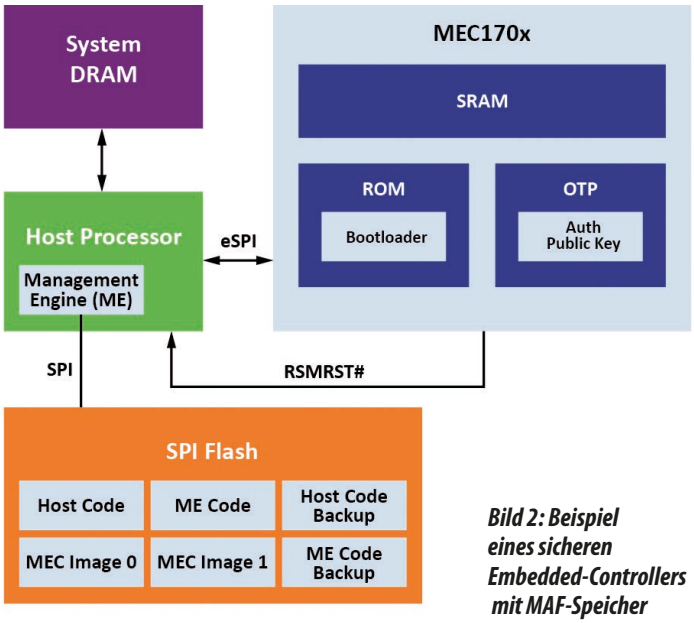

Bild 2: Beispiel eines sicheren Embedded-Controllers mit MAF-Speicher

Die drei Kernprinzipien der Richtlinien lauten:

- **Schützen:** Sicherstellen, dass Code und kritische Daten vor Änderungen geschützt sind, egal ob diese böswillig oder unbeabsichtigt erfolgen
- **Erkennen**, wenn Code und kritische Daten beschädigt wurden
- **Wiederherstellen**: Bereitstellen von Mitteln zum Wiederherstellen von Code und kritischen Daten in einen bekannten guten Zustand.

Kriterien

Diese Anforderungen führen zu einer Reihe von Kriterien für jedes sichere System, das Teil des ORAN-Netzwerks ist:

- **Sicherer Systemstart:** Verwendung einer hardwaregestützten Vertrauensbasis, um die Integrität der Software beim Start sicherzustellen
- **Authentifizierung**: Bereitstellung einer eindeutigen und überprüfbaren Identität
- **Sichere Kommunikation:** Übertragung authentifizierter und verschlüsselter Daten
- **Sichere Programmierung und Fehlerbehebung:** Strenge Kontrolle des Zugriffs auf die physischen Schnittstellen des Systems. Dies umfasst die Entfernung von Schnittstellenports, die während der Produktentwicklung verwendet werden, in der Serienfertigung jedoch nicht benötigt werden.
- **Schutz von Assets**: Strenge Kontrolle über Passwörter, Verschlüsselungsschlüssel und Sicherheitszertifikate
- **Lebenszyklus-Management:** Mit der Weiterentwicklung der Cyberbedrohungen entwickeln sich auch die Cybersicherheitsmaßnahmen weiter.
- **Datensicherheit**: Nachweis, dass alle Geräte im System cybersicher sind und beispielsweise Penetrationstests (Pen-Tests) unterzogen wurden

In den letzten Jahren haben Halbleiterhersteller zahlreiche Technologien mit integrierten Funktionen entwickelt, um die Entwicklung von Systemen, die diese Kriterien erfüllen, einfacher und schneller zu gestalten.

Ein Beispiel sind sichere Embedded-Controller, die ursprünglich für Computer- und Netzwerkspeicheranwendungen entwickelt wurden, sich aber ebenso gut für die Sicherheit in offenen Systemen eignen, auf denen Gerätehersteller und Systemarchitekten ORANs aufbauen. Diese Controller verfügen über eine Secure-Boot-Funktion (Root of Trust), die unveränderlichen Code im Boot-ROM mit Public/Private-Key-Kryptografie kombiniert. Der gesamte Anwendungscode muss vor der Ausführung mit dem öffentlichen Schlüssel authentifiziert werden, während ein ECC-Algorithmus (Elliptic Curve Cryptography) zur digitalen Signatur sowohl zur Authentifizierung des Codes als auch zur Überprüfung seiner Integrität verwendet werden kann.

Im Hinblick auf die NIST-Wiederherstellungsanforderungen ist Redundanz wichtig. Dazu werden mehrere Images des Anwendungscodes des Controllers im externen Speicher abgelegt. Sollte sich beim Booten herausstellen, dass das erste Image beschädigt ist, kann der Boot-Vorgang mit einem anderen Image fortgesetzt werden. Sobald der Anwendungscode geladen wurde, kann die Krypto-Hardware des Controllers genutzt werden, um die Schutz-, Erkennungs- und Wiederherstellungsanforderungen auf das BIOS, die Management Engine (ME) und anderen im Speicher abgelegte Codes und Informationen auszuweiten. Wird beschädigter Systemcode erkannt, kann der Anwendungscode Backup- oder Golden-Images verwenden, um das System wiederherzustellen.

Bild 2 zeigt eine Implementierung eines NIST-konformen Embedded-Controllers, der auf einer Master-Attached-Flash-/MAF-Speicherkonfiguration mit einem einzigen SPI-Flash-Chip basiert. Alternative Konfigurationsoptionen sind MAF mit zwei SPI-Chips, gemeinsam genutzter Flash-Speicher mit einem SPI-Chip und gemeinsam genutzter MAF mit zwei SPI-Chips.

Sicheres Booten ist eine wichtige erste Verteidigungslinie. In manchen Fällen verlangen die Anforderungen jedoch, dass Entwickler von ORAN-Geräten ihre Hardware auf Mikroprozessoren (MPU) basieren, die diese integrierte Funktion nicht bieten und daher den Code nicht vor der Ausführung validieren. In solchen Fällen muss die Secure-Boot-Funktion in das Gerätedesign integriert werden. Eine Möglichkeit dafür ist die Wahl eines gängigen Secure-Boot-Referenz-Designs, das auf neuesten FPGAs (Field Programmable Gate Arrays) basiert.

Wie Bild 3 zeigt, können diese Bausteine, die eine vertrauenswürdige Quelle und einen umfassenden Authentifizierungsprozess nutzen, neben Target-Prozessoren eingesetzt werden und – im Falle der gezeigten Lösung – über DPA-resistente (Differential Power Analysis) Manipulationsschutzmaßnahmen verfügen.

Eigenständige Sicherheits-Kryptoprozessoren

Eine weitere wichtige Entwicklung für ORAN-Gerätehersteller ist das Aufkommen dedizierter und eigenständiger Sicherheits-Kryptoprozessor-ICs, die den vom NIST Computer Security Resource Center (CSRC) entwickelten Federal-Information-Processing-/FIPS-Standards entsprechen und die Spezifikationen der Trusted Computing Group (TCG) unterstützen.

Die FIPS-Standards sind für Behörden konzipiert, die kryptografische Sicherheitssysteme zum Schutz sensibler Informationen in Computer- und Telekommunikationsgeräten einsetzen. Sie bilden somit eine gute Grundlage für die ORAN-Sicherheit auf Hardware-Ebene. FIPS-konforme Chips, die eine Methode zum Speichern von Schlüsseln in geschützter Hardware und zur Verwaltung dieser Schlüssel bieten, um mehrschichtige Sicherheit zu erreichen, fungieren effektiv als Hardware-Krypto-Beschleuniger. Sie übernehmen komplexe Sicherheitsoperationen vom Host-Prozessor und schützen Schlüssel in der Hardware. Da diese Chips bereits in Embedded-Systemen verwendet werden, sind sie bewährt, weitverbreitet und kostengünstig.

Bild 4 zeigt ein Blockdiagramm eines Kryptoprozessor-ICs, der einen Mikrocontroller, geschützten nichtflüchtigen Speicher und eine starke, hardwarebasierte Public-Key-Sicherheitstechnologie (RSA) auf einem einzigen Chip vereint. Der Baustein implementiert die TCG-Spezifikation für Trusted Platform Modules (TPM), verfügt über einen FIPS-zertifizierten Pseudozufallszahlengenerator für die Schlüsselgenerierung, bietet Secure Boot, Schutz des geistigen Eigentums, Authentifizierung und sichere Kommunikation. Hinzu kommen eine aktive Abschirmung sowie eine Reihe von Funktionen zur Manipulationserkennung und -abwehr.

Fazit

ORAN erfordert den Fokus auf Änderungen der Angriffsfläche an den Schnittstellen zwischen den integrierten Technologien. Da viele Betreiber ORAN-Netzwerke auf der Grundlage bestehender LTE-Kernnetze aufbauen, können diese anfällig für passive Abhör- und aktive Man-in-the-Middle-Angriffe sein. Daher müssen Netzwerkarchitekten die Sicherheit jeder einzelnen Verbindung berücksichtigen.

Per Definition basieren ORAN-Architekturen weitgehend auf kostengünstigen, kommerziellen Standardtechnologien, die eine schnellere Implementierung und geringere Kosten ermöglichen. Im Hinblick auf die Sicherheit sind Halbleiter, die Sicherheitsprobleme minimieren und robuste, geschützte ORAN-Infrastrukturen ermöglichen, von entscheidender Bedeutung.

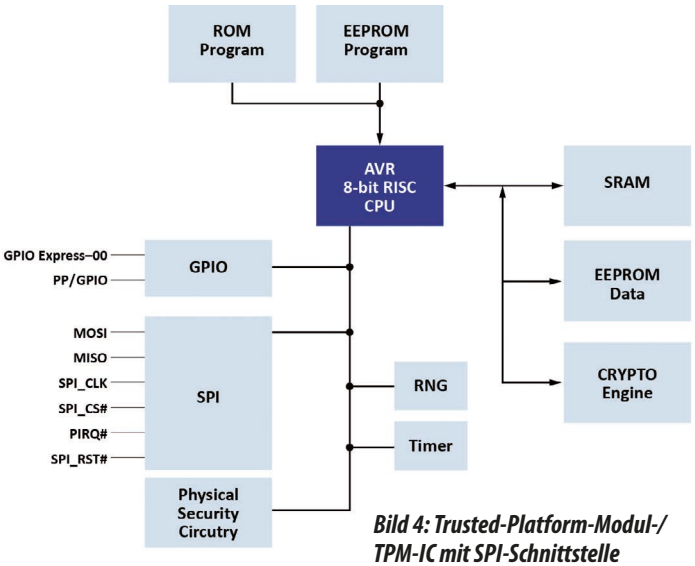

Bild 4: Trusted-Platform-Modul-/ TPM-IC mit SPI-Schnittstelle

Diese Halbleiterbausteine sollten die Anforderungen relevanter Gremien und Normen wie NIST, CISA, FIPs und TCG erfüllen, indem sie Funktionen wie Secure Boot und Hardware Root of Trust bis hin zur Erzeugung und Authentifizierung von Kryptografieschlüsseln, Manipulationserkennung und Lösungen für die Systemwiederherstellung bieten. In immer mehr Fällen sind solche Sicherheitsfunktionen in Controller und TPMs integriert. Wo sie nicht verfügbar sind, lassen sie sich mithilfe bewährter Standardreferenzdesigns hinzufügen. ◄

[1] www.microchip.com/en-us/solutions/data-centers-and-computing/computing-solutions/technologies/platform-root-of-trust-secure-boot

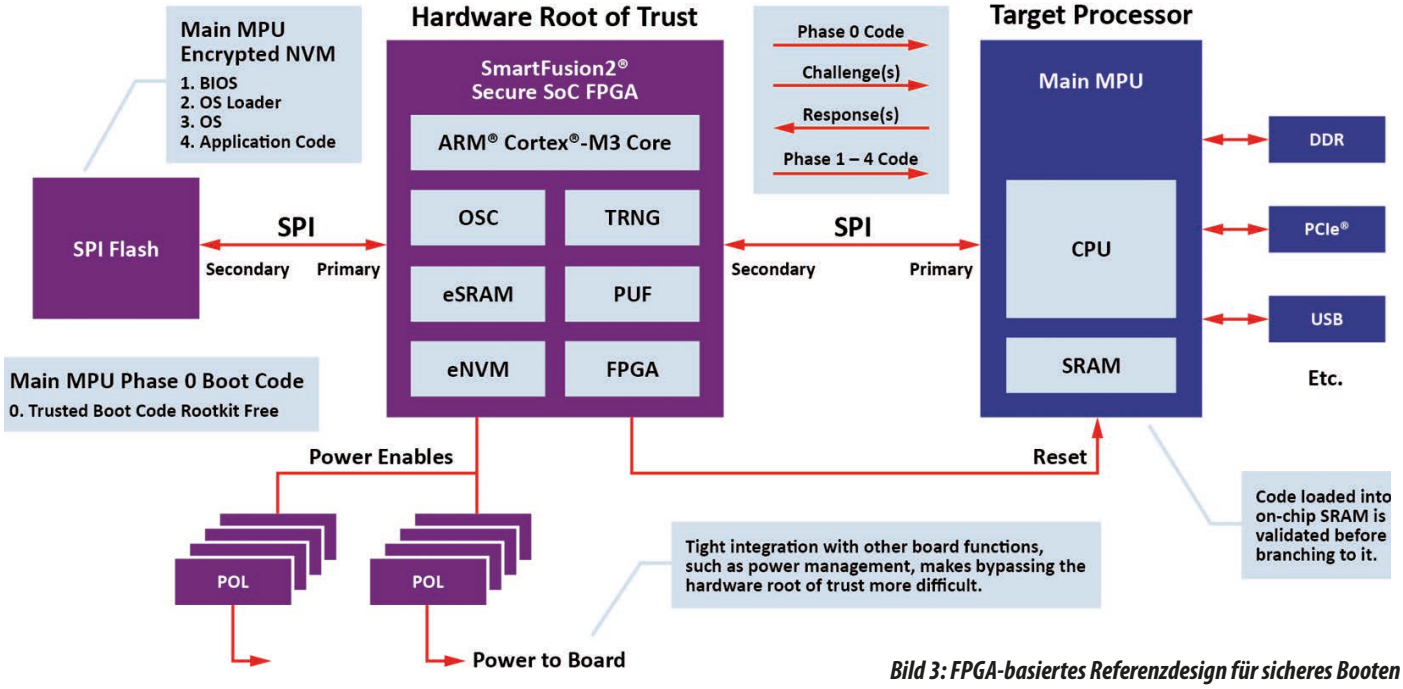

Bild 3: FPGA-basiertes Referenzdesign für sicheres Booten