Sicherheitsaktivierung auf Jacinto™ 7-Prozessoren

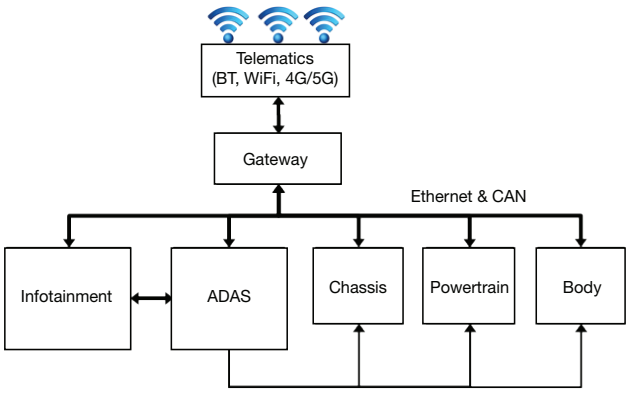
Steve Reis
Systemanwendungen und Architektur
Jacinto-Prozessoren

Integrierte Prozessor- und System-On-Chip (SoC)-Lösungen mit immer mehr Funktionen ermöglichen es Entwicklern, immer bessere und leistungsfähigere Systeme zu entwickeln. Sowohl kabelgebundene als auch drahtlose Kommunikationsoptionen gehören inzwischen zur Standardausrüstung der meisten integrierten Systeme. Sie ermöglichen die Verbindung zu Fernsteuerungs- und Verwaltungsfunktionen und die Integration in noch komplexere und leistungsfähigere Systeme in Fabriken, Fahrzeugen oder Gebäuden.

Außerdem gehören Funktionen die der Unterstützung von Remote-Updates, zur Fehlerkorrektur (Bugfixing) oder zum Einspielen neuer Funktionen genutzt werden inzwischen auch zur Standardausrüstung vieler Systeme. Leider bieten diese Funktionen möglichen Angreifern größere Angriffsflächen. Um zu verhindern, dass ein System kooptiert, falsch gebraucht oder sogar unsicher wird, müssen deshalb besondere Sicherheitsmaßnahmen implementiert werden.

Abbildung 1 zeigt ein Fahrzeugsystem mit Chassis, Antriebsstrang und Karosseriesystemen, zusammen mit einem Infotainment-System und einem erweiterten Fahrerassistenz-(ADAS-)System. Alle Systeme sind über eine Netzwerk-Gateway miteinander verbunden, die den Datenaustausch unter den verschiedenen elektronischen Steuereinheiten ermöglicht. In einem typischen integrierten Fahrzeugsystem kann das ADAS-System Funktionen wie das automatische Einparken, den Spurhalte-Assistent und andere automatisierte Fahrfunktionen steuern. Eine Telematik-Gateway ermöglicht den Zugriff auf die Cloud, um von dort Software-Updates und andere Daten herunterzuladen.

Die externen Schnittstellen dieser Gateways, insbesondere die Drahtlos-Schnittstellen, sind Schwachstellen, die Angreifer nutzen können, um sich per Fernzugriff Zugang zum System zu verschaffen. Erschwerend kommt hinzu, dass Systeme immer vernetzter werden. Dies kann dazu führen, dass Sicherheitsverletzungen sich schnell in weiten Teilen des Systems ausbreiten können. Auch aus diesem Grund ist es besonders wichtig, leistungsstarke Sicherheitsfunktionen zu implementieren.



Example interconnect vehicle architecture with wireless connectivity

***Abbildung 1**. Vernetzte Fahrzeugarchitektur.*

In diesem Whitepaper werden wir uns die Jacinto 7 Prozessorfamilie genauer ansehen, darunter die TDA4x- und DRA8x-Prozessoren. Außerdem möchten wir

einen Überblick über die in der Jacinto 7 SoC-Familie verfügbaren Sicherheitsfunktionen geben und zeigen, wie Entwickler mithilfe dieser Sicherheitsfunktionen die Sicherheitsanforderungen ihrer Systeme erfüllen können. Wir bezeichnen diese als **Sicherheitsaktivierer**. Erfahren Sie mehr über unsere Sicherheitsaktivierer auf TI.com/security.

Sicherheits-Framework

Bereits auf der Anwendungsebene können durch die Implementierung von Sicherheitsfunktionen Assets vor Angriffen geschützt werden. Auf der Halbleiter-Ebene sind die wichtigsten Assets, die es zu schützen gilt, Daten, Code, Geräteidentitäten und Schlüssel. Schwachstellen in einem System (auch oft als Angriffsoberfläche bezeichnet) sind der Hauptgrund dafür, dass Angriffe zu jedem Zeitpunkt im Anwendungs- und Systemlebenszyklus, und während des Betriebs auftreten können.

Wenn Sie Bausteine für Ihr Design auswählen, sollten Sie sich deshalb Gedanken darüber machen, welche Assets es zu schützen gilt und welche Angriffsoberflächen das System hat. Dann können Sie entsprechend Ihren Anforderungen die passenden Sicherheitsaktiverungs-Bausteine und Sicherheitsfunktionen wählen, mit denen Sie Ihr System angemessen schützen können. **Abbildung 2** zeigt ein Beispiel für ein Sicherheits-Framework

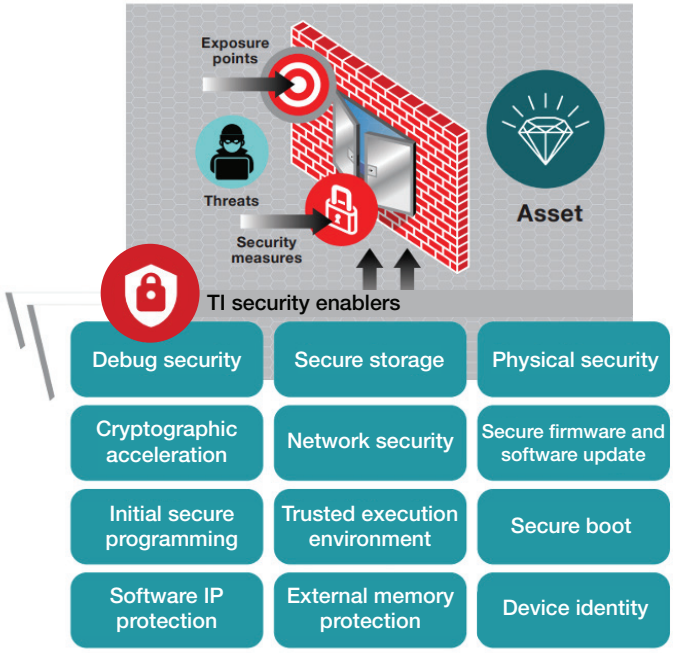


***Abbildung 2**. Sicherheits-Framework*

Die Jacinto 7 SoC-Familie unterstützt viele Sicherheitsaktivierungsfunktionen, die unseren Kunden dabei helfen strenge, an ihr System individuell angepasste Sicherheitsfunktionen zu implementieren und das System vor potenziellen Angriffen zu schützen, indem sie den Zugriff auf das System über die Angriffsoberflächen des Systems beschränken oder ganz verhindern. Dazu gehören:

- Geräteidentität (Unique ID)
- Secure Boot (Vertrauensanker-Public Key)
- Sichere Erst-Programmierung
- Kryptografische Beschleunigung
- Schutz externer Speicher (Firewalls)
- Debugging-Sicherheit (Joint Test Action Group [JTAG] Sperre mit Passwort)
- Software-seitiger Schutz geistigen Eigentums (IP) (Debugging-Sperre)

Standard-Sicherheitsprozessor und Firmware von TI

Das Herzstück der Sicherheitsaktivierungsfunktionen der Jacinto 7-SoCs bilden ein dedizierter Arm® Cortex®-M Prozessor und ein sicherer Arbeitsspeicher, der die Firmware für die Standard-Sicherheitsfunktionen enthält. Diese Funktionen umfassen Secure-Boot- und Sicherheitsfunktionen, sichere eFuse-Schlüsselverwaltung, Geräte-Firewallverwaltung, Authorisierungsfunktionen für den Zugriff auf JTAG

und Funktionen zum Schutz vor Firmware-Rollback. Je nach Baustein, können außerdemzusätzliche Funktionen gewählt werden.

Geräteidentität, Verschlüsselung und Secure Boot-Funktion

Ein wichtiges Vorteil der Sicherheitsaktivierungsfunktionen der Jacinto 7-Plattform ist, dass sie Unterstützung für die Secure-Boot-Funktion und Vertrauensanker bieten. Gemeinsam sichern diese den Boot-Prozess und verhindern damit das Laden und die Ausführung von nicht vertrauenswürdiger Software.

Dieser Sicherheitsanker ist auf einem im Jacinto-7-SoC integriertem Vertrauensanker oder Schlüsselset aufgebaut.

Diese Schlüssel bestehen aus einem Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel für asymmetrische Verschlüsselung, einem gemeinsamen geheimen Schlüssel und einem gerätespezifischen Schlüssel. Der öffentliche Schlüssel (Public Key) wird während der Fertigung der Hardware auf einen einmalig programmierbaren eFuse-Speicher gelötet. Dieser öffentliche Schlüssel wird dann dazu verwendet das Basis-Software-Image, das beim Erststart des Systems aufgespielt wird, zusammen mit den Basis-Gerätesicherheitskonfiguratio nskomponenten zu authentifizieren. Dies geschieht über die in der Software integrierten digitalen Zertifikate und Authentifikatoren. Dieser Prozess kann erweitert werden, indem Vertrauensrichtlinien zu weiteren Schlüsseln hinzugefügt werden und die Vertrauenskette durch die Authentifizierung zusätzlicher Softwarekomponenten erweitert wird. Zu diesen Softwarekomponenten gehören zusätzliche Bootloader und Betriebssystem-Kernel für die Mehr-Kern- Architektur des Jacinto 7-SoC.

Der Hersteller des Systems verwahrt die Root Keys in einer sicheren Rechnerumgebung, um die Integrität des Systems zu wahren und den Zugriff für autorisierte Benutzer zu beschränken. Die Benutzer besitzen nur indirekt Zugriff auf die Schlüssel, um die Software für die Jacinto 7-Prozessorkerne auf ihren Systemen zu authentifizieren oder zu verschlüsseln. Die Software wird über das Standard-Zertifizierungsformat X.509 authentifiziert. Dieses Format benötigt kein eigenes Zertifikat oder bestimmte Authentifizierungstools und kann deshalb mit gängigen Tools erstellt werden. Dies macht die Implementierung in einer sicheren Rechnerumgebung beim Benutzer sehr einfach und sorgt dafür, dass die Sicherheit ihrer privaten Schlüssel bewahrt bleibt.

Die Secure-Boot-Funktion des Jacinto 7-SoC sorgt dafür, dass die Software, die auf dem Gerät ausgeführt wird vor dem Laden immer authentifiziert wird und verhindert somit das Laden nicht autorisierter Software während der Boot-Phase beim entscheidenden Erststart des Systems. Der Secure-Boot-Prozess beim Erststart wird mithilfe eines Festwertspeichers implementiert, dessen Aufgabe darin besteht, die Authentifizierung der Software-Komponenten gegenüber dem Vertrauensanker-Gerät zu erzwingen. Boot-Authentifizierungsoptionen können dabei entweder Rivest-Shamir-Adleman-Authentifizierung (RSA) (bis zu 4.096 Bit-Schlüssel), Elliptic Curve Digital Signature-Authentifizierung (ECDSA) oder elliptic curve cryptography (ECC) bis zu 521 Bit-Keys, in Kombination mit dem SHA2-512-Secure Hash Algorithm für Software- und Zertifikatauthentifizierung unterstützen. Außerdem wird zusätzlich als Option AES-256-Verschlüsselung für den Bootloader unterstützt

Sichere Erst-Programmierung

Bei der Bereitstellung von Geräten mit symmetrischen Schlüsseln müssen geheime Schlüssel sicher programmiert werden. Die Bereitstellung von Geräteschlüsseln wird vom Hersteller in der eigenen Fabrik mit den von TI bereitgestellten sicheren Bereitstellungstools durchgeführt. Der Hersteller besitzt die vollständige Kontrolle über den gesamten Bereitstellungsprozess. So können Sicherheit, geringe Komplexität und vollständige Flexibilität bei der Schlüsselprogrammierung gewährleistet werden. Verschlüsselungsschutz verhindert zusätzlich, dass der symmetrische Schlüssel während des Bereitstellungsprozesses an andere weitergegeben wird. Damit kann die Bereitstellung und Herstellung von Geräten mit symmetrischen Schlüsseln auch in einer nicht vertrauenswürdigen Fabrikumgebung durchgeführt werden.

Kryptografische Beschleunigung

Kryptografische Funktionen können, je nachdem welche Flexibilitäts- und Durchsatzanforderungen erfüllt werden müssen, auf Universal-Computerkernen oder speziellen Hardwarebeschleunigern programmiert werden. Jacinto 7-SoCs enthalten mehrere Kerne, die als Beschleuniger für gängige kryptografische Funktionen dienen und Unterstützung für die folgenden kryptografischen Instrumente bieten:

- Asymmetrische Kryptografie: RSA und ECC-Funktionen
- Hash-Funktionen: Message Digest Algorithm (MD5), SHA1 und SHA2-224/256/384/512
- Symmetrische Kryptografie-Funktionen: AES-128/192/256
- Hardware-TRNG-Modul mit Nachbearbeitung für einen deterministischen Zufallsbitgenerator (DRBG)

Zusätzlich dazu unterstützen Arm Cortex-CPUs ARMv8-Kryptografieerweiterungen. Diese Erweiterungen stellen neue Befehle zur Beschleunigung der Ausführung von AES-, SHA1- und SHA2-Algorithmen bereit.

Schutz der Software-IP (Firewalls)

Bausteine der Jacinto 7-SoC-Familie besitzen einen Satz heterogener, für verschiedene Aufgaben perfektionierter Prozessorkerne, darunter 64-Bit-Arm-Kerne und 32-Bit-Arm-Mikrocontroller-Kerne, außerdem Digitalsignalprozessoren (DSPs) von TI; einige Bausteine der Reihe besitzen zudem spezielle DSP-Beschleuniger. Da einige dieser Komponenten möglicherweise dafür genutzt werden, Aufgaben durchzuführen, die mit sicheren Assets arbeiten, müssen sie extra geschützt und von anderen Systemfunktionen getrennt werden. Auch hierfür besitzt Jacinto 7 eine Lösung: Er enthält einen umfassenden Satz von System-Firewalls, die dem Schutz von Runtime-Ereignissen dienen und Isolierung für extra Sicherheit bieten. Mithilfe von Firewalls können Benutzer bestimmen, auf welche Hardware-Elemente und Speicherbereiche jeder einzelne Prozessorkern oder jedes Startersystem Zugriff haben soll. Diese Firewall-Infrastruktur ist eine der wichtigsten Schutzaktivierungsfunktionen für das System, da die Firewalls das Weitergeben von geheimen Informationen verhindern, die Auswirkungen potenzieller Sicherheitsverletzungen minimieren und das System frei von Störungen halten.

Debuggersicherheit

Der allgegenwärtige JTAG-Debug-Port, der auf den meisten programmierbaren Geräten zu finden ist, bietet viele nützliche Funktionen, wie zum Beispiel einfachen Zugriff auf die Register und den Speicher des Geräts, Methoden zum einfachen erstmaligen Laden und zur Programmablaufverfolgung. Der JTAG-Port wird aufgrund seiner einfachen Zugänglichkeit als die verwundbarste Komponente in einem System angesehen. Deswegen ist der JTAG-Debugging-Port der Jacinto 7-SoCs an sicheren Geräten standardmäßig deaktiviert, sodass er nicht von Angreifern genutzt werden kann, die sich Zugang zum SoC verschaffen und dessen Betrieb stören möchten. Der JTAG-Port an einem Jacinto 7-Baustein kann aber auch – sicher – aktiviert werden und zum Testen oder für Analysefunktionen genutzt werden. Um den JTAG-Port zu aktivieren muss der Benutzer die entsprechenden Berechtigungen besitzen oder sich über ein Zertifikat, das mit dem Vertrauensanker verbunden ist, authentifizieren. Außerdem ist jedes Debugging-Zertifikat an ein einzelnes Gerät gebunden und kann nur den Zugriff zum Debugging für die entsprechende Geräte-ID freischalten. Darüber hinaus besteht die Möglichkeit, den Zugriff auf den JTAG-Port über ein einmalig-programmierbares eFuse-Programm vollständig zu deaktivieren, sollte dies im Sicherheitsprotokoll für das System so bestimmt sein. Diese Funktionen bieten verschiedene Sicherheits- und Zugriffsebenen. Sie bieten den Benutzern Flexibilität in der Entwicklungsphase und sorgen für die Systemsicherheit während der Fertigung.

Trusted Execution Environment (TEE)

Die Arm Cortex-A72 TrustZone®-Funktion der Jacinto 7-SoCs bietet Isolierungsfunktionen bei der Ausführung sicherer Softwarekomponenten und dient dem Schutz wichtiger Assets, wie Schlüssel, Daten und spezieller Algorithmen. Um die Nutzung dieser sicheren Umgebung zu vereinfachen, wird ein Trusted Execution Environment (TEE) verwendet, das einen Teil des Systems abschottet und eine sichere Laufzeitumgebung für isolierte Anwendungen zur Verfügung stellt. Das Linux® Software Entwicklungskit des Jacinto 7-Bausteins ermöglicht die Integration des Linaro OP-TEE-Secure-Stack. Mit dem Linaro OP-TEE-Secure-Stack können sichere Anwendungen über die Standard-GlobalPlatform-Anwendungsprogrammierung sschnittstellen für die Arm-Plattform entwickelt werden. Ein weiterer Vorteil des TEE besteht darin, dass sichere Anwendungen voneinander, sowie vom Rest des Linux-Stacks abgeschottet sind. Dies bedeutet, dass mehrere Clients gleichzeitig das TEE nutzen können, ohne ihre Assets preiszugeben.

Sichere Firmware- und Software-Updates

Sichere Firmware-Updates, vor allem OTA-Updates, in Embedded Systeme zu integrieren gewinnt mehr und mehr an Bedeutung, denn sie dienen der schnellen Vor-Ort-Bereitstellung neuer und erweiterter Funktionen und der Implementierung von Bugfixes und Sicherheitspatches,

ohne die hohen Kosten und den Zeitaufwand, der mit dem Einsatz von Außendienstmitarbeitern oder dem Werksservice verbunden sind. Der Update-Prozess selbst kann jedoch auch ein Sicherheitsrisiko darstellen; nämlich dann, wenn es Angreifern gelingen sollte das System durch das Maskieren Ihrer Identität zu täuschen, auf eine frühere Version zu bringen oder den Update-Mechanismus zu nutzen, um kompromittierte Software-Images zu installieren.

Update-Images sollten immer eine Hashfunktion und eine Sicherheitssignatur zur Prüfung ihrer Integrität und Echtheit besitzen. Mithilfe von Echtheits-Prüfungen lässt sich verifizieren, ob das Update von einer bekannten und vertrauenswürdigen Quelle kommt. Integritätskontrollen überprüfen, ob die Images während der Datenübertragung oder des Ladeprozesses verändert oder manipuliert wurden. Die gleichen Jacinto 7-SoC-Funktionen, die zur Secure-Boot-Authentifizierung verwendet werden, können zur Authentifizierung von Software- und Daten-Updates genutzt werden

Fazit

Die Sicherheitsaktivierungsfunktionen der Jacinto 7-Bausteinfamilie bieten umfassende integrierte Sicherheitsfunktionen, die Entwicklern und Systemarchitekten die Möglichkeit gibt, die Sicherheitsanforderungen ihrer Systeme zu erfüllen. Diese Anforderungen werden üblicherweise im Rahmen einer Sicherheitsimplementierungsphase festgelegt: dies beinhaltet die Bestimmung spezieller Sicherheitsziele und Maßnahmen für jedes einzelne Projekt und die Sicherheitsaktivierer, die zum Zweck der Erfüllung dieser Ziele eingesetzt werden sollen. Weitere Informationen finden Sie unter ti.com/security.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (https:www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265