Sichere Konnektivität für die häusliche Gesundheitsversorgung

Teil 1: Herausforderungen außerhalb der Klinik

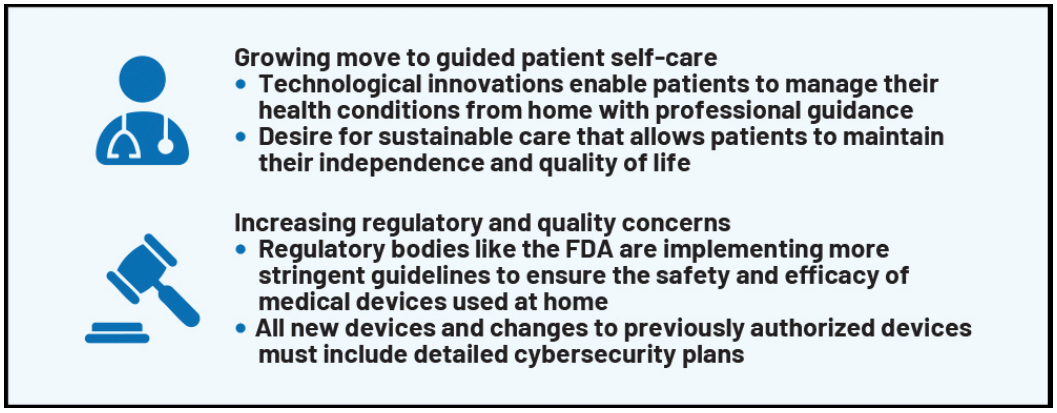

Bild 1: Trends in der häuslichen Gesundheitsversorgung

Dieser Artikel zeigt sichere Konnektivitätslösungen, die den besonderen Anforderungen an Sicherheit und Patientenschutz bei einer Vielzahl medizinischer Geräte in der häuslichen Gesundheitsversorgung gerecht werden.

Einführung

Aufbauend auf den Grundlagen, die im Artikel „Sichere Authentifizierung für medizinische Einwegprodukte“ beschrieben sind, beleuchtet dieser Artikel den wachsenden Trend, medizinische Versorgung vom Krankenhaus in die privaten Haushalte der Patienten zu verlagern (Bild 1). Dabei werden die besonderen Herausforderungen für die Sicherheit bei der Versorgung außerhalb eines medizinischen Umfelds sowie die Anforderungen an die Sicherung von Daten während der Netzwerkübertragung erörtert.

Trends in der häuslichen Gesundheitsversorgung

Zunehmender Trend zur angeleiteten Selbstversorgung von Patienten: Dieser Trend gewinnt an Dynamik, angetrieben durch technologische Innovationen, die es Patienten ermöglichen, ihre Gesundheitszustände bequem von zu Hause aus zu verwalten. Fortschrittliche Tools wie tragbare Geräte, mobile Gesundheits-Apps und Telemedizin-Plattformen liefern Gesundheitsdaten in Echtzeit und professionelle Beratung, sodass Patienten ihren Gesundheitszustand überwachen und fundierte Entscheidungen über ihre Behandlung treffen können. Bei dieser Verlagerung hin zur Selbstversorgung geht es nicht nur um Komfort, sondern auch um die Förderung einer nachhaltigen Gesundheitsversorgung. Durch die Erhaltung der Unabhängigkeit und Lebensqualität der Patienten unterstützt die angeleitete Selbstversorgung das langfristige Gesundheitsmanagement, erweitert den Zugang zur Gesundheitsversorgung und entlastet gleichzeitig die Gesundheitseinrichtungen.

Zunehmende regulatorische und qualitative Bedenken

Da die häusliche Gesundheitsversorgung weiter zunimmt, führen Aufsichtsbehörden wie die FDA (Food and Drug Administration of USA) strengere Richtlinien ein (FDA-2021-D-1158; Abschnitt 524B, HR 2617 Act of Congress; UL2900-2-1 und IEC62443), um die Sicherheit und Wirksamkeit von medizinischen Geräten für den Heimgebrauch zu gewährleisten. Diese Vorschriften sind für den Schutz der Patienten und die Aufrechterhaltung hoher Versorgungsstandards von entscheidender Bedeutung. Neue Geräte sowie Modifikationen an bestehenden Geräten müssen nun detaillierte Cybersicherheitspläne enthalten, um potenzielle Schwachstellen zu beheben und sensible Gesundheitsdaten zu schützen. Diese verstärkte Fokussierung auf die Einhaltung von Vorschriften und die Qualitätssicherung ist unerlässlich, um Vertrauen in Lösungen für die häusliche Gesundheitsversorgung aufzubauen und sicherzustellen, dass Patienten eine sichere, zuverlässige und wirksame Versorgung erhalten.

Typischer Arbeitsablauf in der häuslichen Gesundheitsversorgung

1. Erstuntersuchung und Programmierung des Geräts: Der Prozess der häuslichen Gesundheitsversorgung beginnt oft mit einem ersten Besuch in einem Krankenhaus oder einer Klinik, wo der Patient von einem Arzt umfassend untersucht wird (Bild 2). Während dieses Besuchs beurteilt der Arzt den Zustand des Patienten und legt den geeigneten Behandlungsplan fest. Anschließend programmiert er das medizinische Gerät mit Einstellungen, die auf die spezifischen Bedürfnisse des Patienten zugeschnitten sind. Nach der Konfiguration erhält der Patient detaillierte Anweisungen zur effektiven Verwendung des Geräts zu Hause.

2. Beginn der Behandlung zu Hause: Nach der Rückkehr nach Hause beginnen die Patienten mit der Behandlung, indem sie die Anweisungen des Arztes befolgen und das medizinische Gerät wie verschrieben verwenden. Dieser Zeitraum ist entscheidend, damit sich die Patienten an das Gerät gewöhnen und es in ihren Alltag integrieren können. Funktionen wie Erinnerungen, Warnmeldungen und benutzerfreundliche Oberflächen helfen den Patienten, ihren Behandlungsplan einzuhalten, fördern ihre Unabhängigkeit und verbessern die Gesundheitsergebnisse.

3. Hochladen von Patientendaten: Ein wichtiger Bestandteil der häuslichen Gesundheitsversorgung ist die kontinuierliche Überwachung und Übertragung von Patientendaten. Diese Daten können Vitalparameter, die Einhaltung der Medikamenteneinnahme und andere relevante Gesundheitsdaten umfassen. Beispielsweise könnten die täglichen Aktivitäten automatisch in

Autoren:
Jackson Coole
Systems Applications Engineer,
Michael Haight
Director of Product Line Management
Analog Devices, Inc.
www.analog.com

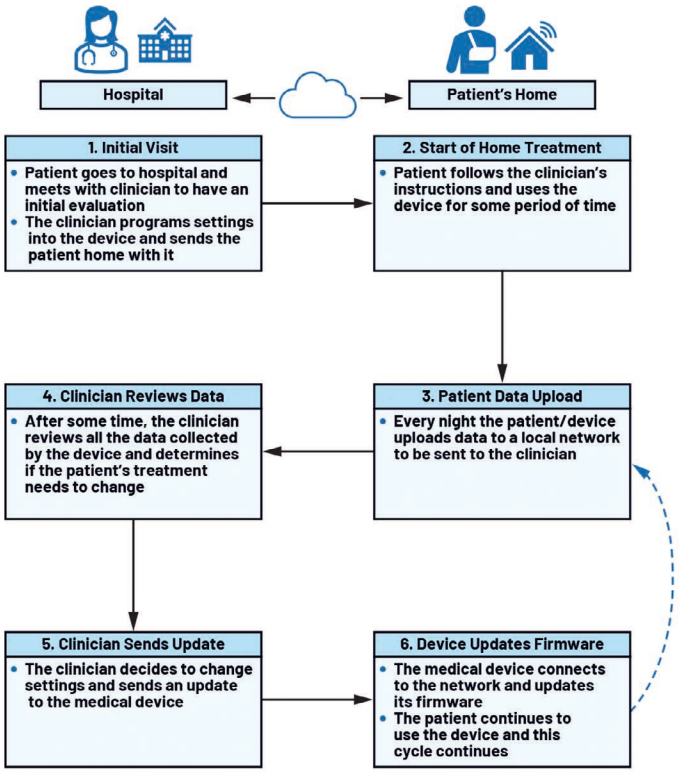

Bild 2: Typischer Arbeitsablauf in der häuslichen Gesundheitsversorgung

ein lokales Netzwerk hochgeladen werden, wenn das Gerät während des Schlafs des Patienten an das Ladegerät angeschlossen ist, das Gerät könnte Daten nur dann senden, wenn ein bestimmtes Ereignis eintritt (z. B. wenn ein Benutzerfehler oder ein unerwünschtes Ereignis erkannt wird), oder die Datenübertragung könnte davon abhängen, dass der Patient Werte manuell in eine mobile Anwendung eingibt. Die nahtlose Übertragung von Informationen stellt sicher, dass der Arzt Zugriff auf aktuelle Daten hat, sodass er bei Bedarf rechtzeitig eingreifen und den Behandlungsplan anpassen kann.

4. Der Arzt überprüft die Daten: Nach einem festgelegten Zeitraum überprüft der Arzt die vom medizinischen Gerät gesammelten Daten. Diese umfassende Analyse ermöglicht es dem Arzt, den Fortschritt des Patienten zu beurteilen und festzustellen, ob Änderungen am Behandlungsplan erforderlich sind. Die Überprüfung durch den Arzt basiert auf den detaillierten Daten des Geräts und liefert ein genaueres Bild des Gesundheitszustands des Patienten als herkömmliche regelmäßige Kontrolluntersuchungen. Dieser proaktive Ansatz hilft, potenzielle Probleme frühzeitig zu erkennen und den Behandlungsplan besser an die Bedürfnisse des Patienten anzupassen.

5. Der Arzt sendet eine Aktualisierung: Wenn der Arzt entscheidet, dass Anpassungen erforderlich sind, können die Einstellungen des medizinischen Geräts aus der Ferne aktualisiert werden. Diese Änderungen der Behandlung können die Anpassung eines wichtigen Messparameters wie die Empfindlichkeit eines Drucksensors oder die Änderung der Häufigkeit der Medikamentengabe oder der Therapie sein. Dies geschieht in der Regel in Form einer neuen Firmware-Version, die sicher auf das medizinische Gerät im Haushalt des Patienten hochgeladen werden muss. Dieses Update wird sicher an das Gerät gesendet, sodass der Patient die aktuellste und wirksamste Behandlung erhält. Die Möglichkeit, Fernanpassungen vorzunehmen, ist ein wesentlicher Vorteil moderner Gesundheitsversorgungssysteme für zu Hause, da sie häufige persönliche Besuche überflüssig machen und eine flexiblere und reaktionsschnellere Versorgung ermöglichen.

6. Gerät aktualisiert Firmware: Sobald der Arzt ein Update sendet, verbindet sich das medizinische Gerät in der Regel mit dem Netzwerk, um das Firmware-Update zu empfangen und zu installieren. Dieser Vorgang ist in der Regel automatisiert, sodass der Patient kaum eingreifen muss und das Gerät mit den neuesten Einstellungen und Sicherheitsprotokollen arbeitet. Nach Abschluss des Updates kann der Patient das Gerät im Rahmen seiner laufenden Behandlung weiter verwenden. Dieser Zyklus aus Datenerfassung, Überprüfung und Anpassung wird fortgesetzt und schafft so eine dynamische und reaktionsschnelle Gesundheitsumgebung, die sich an die sich ändernden Bedürfnisse des Patienten anpasst.

Herausforderungen an die Sicherheit in der häuslichen Gesundheitsversorgung

Die Gewährleistung der Sicherheit von Patientendaten und medizinischen Geräten stellt eine große Herausforderung dar. Die Abhängigkeit von digitalen Plattformen und vernetzten Geräten setzt sensible Gesundheitsdaten potenziellen Cyber-Bedrohungen aus, darunter Datenverstöße und unbefugter Zugriff. Die Bewältigung dieser Sicherheitsherausforderungen ist entscheidend für die Aufrechterhaltung des Vertrauens der Patienten, die Einhaltung von Gesundheitsvorschriften und den Schutz der Integrität der häuslichen Gesundheitsversorgung.

Die Sicherheitsherausforderungen, die für jeden Schritt des typischen Arbeitsablaufs in der häuslichen Gesundheitsversorgung einzigartig sind, werden im nächsten Abschnitt beschrieben (Bild 3).

1. Erstbewertung und Geräteprogrammierung: Bei dem ersten Klinikbesuch und zu Beginn der Behandlung zu Hause müssen mehrere Sicherheitsaspekte berücksichtigt werden. Ein wichtiger Aspekt ist der sichere Start, der sicherstellt, dass das Gerät beim Start nur vertrauenswürdige Software ausführt. Dadurch wird verhindert, dass schädliche Software geladen wird, die die Funktionalität des Geräts und die Sicherheit des Patienten gefährden könnte. Darüber hinaus ist eine sichere Datenspeicherung unerlässlich, um vor unbefugtem Zugriff und Manipulationen zu schützen. Dazu gehören die Verschlüsselung der auf dem Gerät gespeicherten Daten und die Implementierung robuster Zugriffskontrollen, um sicherzustellen, dass nur autorisiertes Personal die Geräteeinstellungen ändern kann. Schließlich muss die Integrität der Firmware-Parameter gewährleistet sein. So ist es beispielsweise für die Patientensicherheit von entscheidender Bedeutung, dass eine Dosierungseinstellung von 10 ml/h nicht versehentlich auf 100 ml/h geändert wird. Dies kann durch kryptografische Prüfsummen und digitale Signaturen erreicht werden, die die Authentizität und Integrität der Firmware überprüfen.

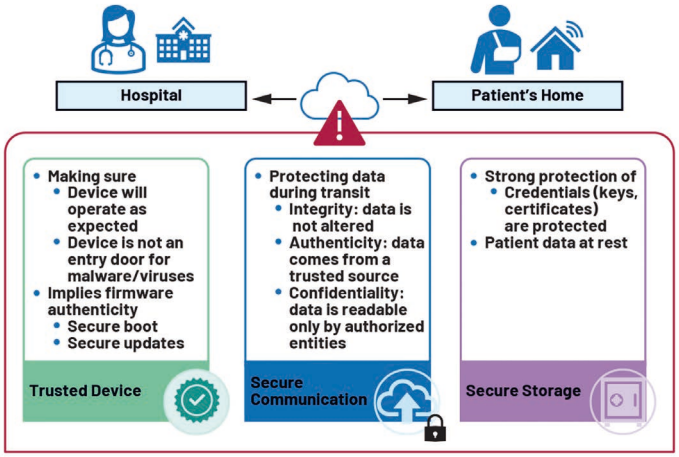

Bild 3: Sicherheitsherausforderungen in der häuslichen Gesundheitsversorgung

2. Hochladen und Übertragen von Patientendaten: Wenn Patientendaten vom medizinischen Gerät an den Arzt übertragen werden, sind mehrere Sicherheitsmaßnahmen erforderlich, um die Daten während der Übertragung zu schützen. Die Authentizität ist dabei von größter Bedeutung, um sicherzustellen, dass die vom Arzt empfangenen Daten tatsächlich vom richtigen Patienten stammen. Dies kann durch eindeutige Patientenidentifikatoren und sichere Authentifizierungsprotokolle erreicht werden. Die Integrität ist ebenfalls von entscheidender Bedeutung, da sie sicherstellt, dass die Daten während der Übertragung nicht verändert wurden. Techniken wie Hashing und digitale Signaturen können verwendet werden, um zu überprüfen, ob die Daten unverändert geblieben sind. Ärzte sind auf genaue und zuverlässige Daten angewiesen, um den Zustand eines Patienten zu beurteilen und die Behandlungspläne entsprechend anzupassen.

Wenn die Daten beschädigt sind, kann dies zu falschen Beurteilungen führen. Beispielsweise könnte ein beschädigter Datenpunkt fälschlicherweise anzeigen, dass der Blutdruck eines Patienten stabil ist, obwohl er gefährlich hoch ist. Schließlich ist die Gewährleistung der Vertraulichkeit von entscheidender Bedeutung, um sensible Patientendaten während der Übertragung zu schützen. Dazu gehört, diese Daten vor unbefugtem Zugriff zu schützen und sicherzustellen, dass sie während der Übertragung vertraulich bleiben. Dies kann durch sichere Kommunikationsprotokolle wie Transport Layer Security (TLS) und virtuelle private Netzwerke (VPNs) erreicht werden, die die übertragenen Daten verschlüsseln. Darüber hinaus stellen strenge Zugriffskontrollen und Authentifizierungsmechanismen sicher, dass nur autorisiertes Personal auf Patientendaten zugreifen kann.

3. Firmware Updates: Wenn der Arzt ein Update an das medizinische Gerät sendet, muss unbedingt sichergestellt werden, dass der Update-Prozess sicher ist. Durch unbefugten Zugriff oder Updates kann ein Eindringling das Verhalten von medizinischen Geräten verändern oder im schlimmsten Fall die vollständige Kontrolle über sie übernehmen. Eine gängige Angriffsmethode ist die Einschleusung von Malware, bei der bösartiger Code in das Firmware-Update eingefügt wird. Wenn ein Angreifer erfolgreich eine gefälschte Firmware installiert, kann dies schwerwiegende Folgen haben. Beispielsweise könnte das kompromittierte Gerät ohne Genehmigung vertrauliche und sensible Daten, wie private medizinische Informationen von einem tragbaren Gesundheitsmonitor, übertragen. In einem größeren Zusammenhang könnte bösartige Firmware Verschlüsselungscodes öffentlich zugänglich machen und damit die Sicherheit des gesamten Systems gefährden.

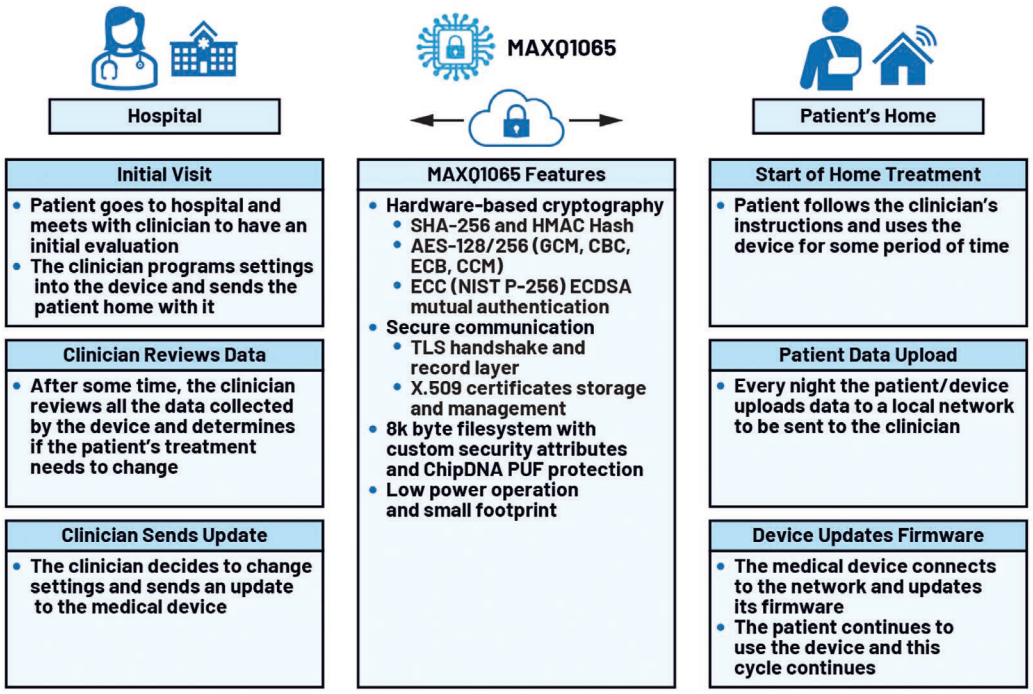

Bild 4: Der MAXQ1065 adressiert Sicherheitsbedenken in der häuslichen Gesundheitsversorgung.

Darüber hinaus könnte das Gerät zu Fehlfunktionen gezwungen werden, was erhebliche Risiken für die Patientensicherheit und die Datenintegrität mit sich bringt. Daher muss die Authentizität der neuen Firmware überprüft werden, um sicherzustellen, dass sie aus einer vertrauenswürdigen Quelle stammt. Dies kann durch digitale Signaturen und Zertifikate erreicht werden, die die Quelle der Firmware authentifizieren. Genau wie bei der ersten Einrichtung des medizinischen Geräts in der Klinik ist die Integrität des Firmware-Updates von entscheidender Bedeutung, um sicherzustellen, dass alle Parameter korrekt sind und nicht manipuliert wurden. Zur Überprüfung der Integrität der Firmware können kryptografische Prüfsummen und Integritätsprüfungen verwendet werden. Schließlich muss während der Übertragung des Firmware-Updates die Vertraulichkeit gewahrt werden, um sensible Daten zu schützen. Durch die Verschlüsselung des Firmware-Updates wird sichergestellt, dass es nicht von Unbefugten abgefangen und abgerufen werden kann.

Sicherheit gewährleisten

Die Lösung ist ein Sicherheits-Coprozessor, der schlüsselfertige kryptografische Funktionen für Root-of-Trust, gegenseitige Authentifizierung, Datenvertraulichkeit und -integrität, sicheres Booten, sichere Firmware-Updates und sichere Kommunikation bietet (Bild 4). Die wichtigsten Merkmale sind in Tabelle 1 aufgeführt.

Sicherer Start und Firmware-Updates

Das Grundprinzip eines sicheren Firmware-Downloads auf Basis asymmetrischer Kryptografie besteht in der Verwendung eines privaten Schlüssels zur Signatur durch den Firmware-Entwickler und eines entsprechenden öffentlichen Schlüssels zur Verifizierung, der auf dem medizinischen Gerät gespeichert ist. Diese Methode gewährleistet insbesondere bei Verwendung des elliptischen Kurven-Digital-Signatur-Algorithmus (ECDSA), dass ein Angreifer den für die Signatur der Firmware und der Daten verwendeten privaten Schlüssel selbst mit ausgeklügelten invasiven Angriffen nicht abrufen kann. Die einzigen Informationen, die ein Angreifer vom medizinischen Gerät erhalten kann, sind der öffentliche Schlüssel und mit ECDSA ist es mathematisch unmöglich, den privaten Schlüssel aus dem öffentlichen Schlüssel abzuleiten.

Wenn die Firmware vom Mikrocontroller des medizinischen Geräts ausgeführt werden muss, ruft der Host-MCU-Boot-Manager sie zunächst ab und übergibt sie zur SHA-256-Hash-Berechnung an den Controller (Bild 5). Nach Abschluss der SHA-256-Hash-Berechnung liefert der Prozessor die ECDSA-Signatur der Firmware oder der Daten, die während der Entwicklungsphase berechnet und an die Datei angehängt wurde. Der Hauptprozessor sendet dann die Firmware- oder Datendatei und die erwartete digitale Signatur. Der Sicherheits-Coprozessor überprüft die Signatur und gibt das Ergebnis zurück, wobei er angibt, ob die

Funktion	Beschreibung
Hardwarebasierte Kryptografie	SHA-256 und HMAC-Hash; AES-128/256 (GCM, CBC, ECB, CCM); ECC (NIST P-256); ECDSA zur gegenseitigen Authentifizierung.
ChipDNA PUF Technologie	Bietet höchsten Schutz für kryptografische Schlüssel und sensible Daten. Schützt den sicheren Schlüssel, indem sichergestellt wird, dass er nie statisch in Registern oder im Speicher abgelegt wird und nie die elektrische Grenze des IC verlässt.
Sichere Kommunikation	Unterstützt sichere Datenübertragung über TLS/DTLS 1.2-Protokolle. TLS-Handshake und Record Layer. Speicherung und Verwaltung von X.509-Zertifikaten.
Sicherer Speicher	8 kB sicherer Speicher für Benutzerdaten, Schlüssel, Zertifikate und Zähler.
Manipulationserkennung	Erkennt physische Manipulationsversuche und reagiert darauf.
Kommunikationsschnittstelle	SPI/I2C.
Niedriger Stromverbrauch	Geräte für die Gesundheitsversorgung zu Hause sind häufig batteriebetrieben, wodurch Energieeffizienz entscheidend ist. Der extrem niedrige Stromverbrauch des MAXQ1065 ermöglicht einen langfristigen Betrieb ohne häufige Batteriewechsel – besonders vorteilhaft für tragbare Gesundheitsmonitore und andere mobile medizinische Geräte.

Tabelle 1: Merkmale des MAXQ1065 Features

Überprüfung erfolgreich war oder ob ein Fehler aufgetreten ist. Wenn die Signaturüberprüfung erfolgreich ist, kann die Firmware ausgeführt werden.

Eine ausführlichere Erläuterung dieses Prozesses finden Sie im Artikel: "The Fundamentals of Secure Boot and Secure Download: How to Protect Firmware and Data Within Embedded Devices."

Sichere Speicherung und Manipulationserkennung

Der MAXQ1065 verfügt über Manipulationserkennungsfunktionen, um physische Manipulationsversuche zu erkennen und darauf zu reagieren. Dies sorgt für eine zusätzliche Sicherheitsebene und gewährleistet, dass das Gerät auch bei potenziellen Eindringversuchen vertrauenswürdig bleibt.

Die ChipDNA Embedded Security-Technologie von ADI mit physikalisch nicht klonbarer Funktion (PUF) bietet einen exponentiell höheren Schutz vor invasiven Angriffen und Reverse Engineering durch Hacker. Versuche, den Betrieb von ChipDNA zu untersuchen oder zu beobachten, verändern die zugrunde liegenden Schaltungseigenschaften und verhindern so die Entdeckung des eindeutigen Werts, der von den Kryptografiefunktionen des Chips verwendet wird. Ebenso werden umfassendere Reverse-Engineering-Versuche aufgrund der werkseitigen Konditionierung, die erforderlich ist, um die ChipDNA-PUF-Schaltung funktionsfähig zu machen, vereitelt. Der für jedes Gerät einzigartige Schlüssel wird von der ChipDNA-PUF-Schaltung nur bei Bedarf für kryptografische Vorgänge generiert und anschließend sofort gelöscht.

Transport Layer Security (TLS)-Schutz

Der MAXQ1065 unterstützt die Protokolle TLS/DTLS 1.2 für eine sichere Datenübertragung und gewährleistet so die Vertraulichkeit und Integrität der Daten. Dies ist von entscheidender Bedeutung für medizinische Geräte für den Heimgebrauch, die Patientendaten an Gesundheitsdienstleister oder cloudbasierte Systeme übertragen müssen.

In diesem Szenario verwendet ein medizinisches Gerät im Haushalt des Patienten TLS für die sichere Kommunikation mit einem Cloud-Server. TLS umfasst zwei Phasen: den Handshake und die sichere Kommunikation. Sichere ICs verbessern TLS, indem sie die Stammzertifikate der Zertifizierungsstelle in einem nichtflüchtigen Speicher ablegen, sodass nur authentifizierte Administratoren sie ersetzen können. In der Handshake-Phase werden die Sicherheitseinstellungen ausgehandelt und gemeinsame Schlüssel festgelegt, während in der Phase der sicheren Kommunikation diese Schlüssel für die Verschlüsselung und Authentifizierung verwendet werden. Die Implementierung von TLS auf eingebetteten Geräten kann komplex sein und Risiken wie das Überspringen der Zertifikatsüberprüfung oder die Verwendung schwacher Verschlüsselungssuiten mit sich bringen. Der MAXQ1065 bietet hardwarebasierte Schutzmaßnahmen, die unbefugten Zugriff verhindern und die Integrität der TLS-Prozesse gewährleisten. Er schützt vor Angriffen wie Man-in-the-Middle und der Offenlegung von Sitzungsschlüsseln und gewährleistet so die Vertraulichkeit und Integrität von Gesundheitsdaten, ohne die Geräteleistung zu beeinträchtigen.

Darüber hinaus ermöglicht dieser kryptografische Controller Geräteherstellern die Einrichtung einer eigenen CA für verbundene Geräte, die sichere Speicherung von öffentlichen Root-Schlüsseln und die Verhinderung unbefugter Änderungen. Die ChipDNA-Technologie schützt den privaten Schlüssel zusätzlich, indem sie ihn zu einem Nebenprodukt der normalen physischen Fertigung des IC macht und ihn so vor Hacking und Reverse Engineering schützt.

Eine ausführliche Übersicht über die Verwendung sicherer Begleit-ICs zum Schutz von TLS-Implementierungen zeigt Artikel "Using Secure Companion ICs to Protect a TLS Implementation."

Fazit

Da die Nachfrage nach Lösungen für die Gesundheitsversorgung zu Hause weiter steigt, wird der Bedarf an sicheren und zuverlässigen medizinischen Geräten immer wichtiger. Ein Kryptografie-Controller erfüllt diese Anforderungen mit seinen fortschrittlichen Sicherheitsfunktionen, seinem geringen Stromverbrauch und seiner einfachen Integration. Durch die Integration dieses Coprozessors in Geräte für die Gesundheitsversorgung zu Hause können Hersteller sicherstellen, dass Patientendaten sicher bleiben und die Geräte langfristig zuverlässig funktionieren.

Wer schreibt:

Jackson Coole ist systems applications engineer bei Analog Devices und arbeitet im Team für medizinische Instrumente.

Michael Haight ist Director of Product Line Management bei Analog Devices, wo er für eingebettete HW-basierte Sicherheitsprodukte verantwortlich ist. ◄

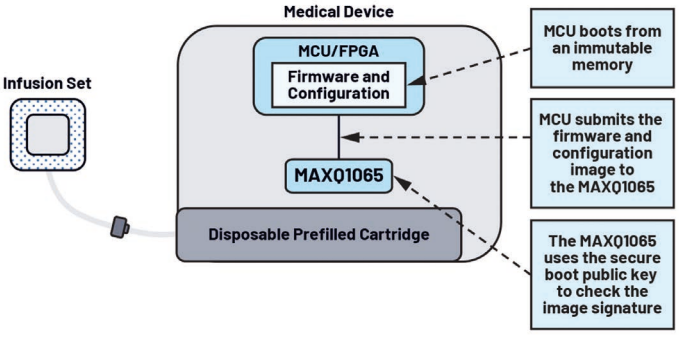

Bild 5: Sicherer Startvorgang