SentriX
Embedding Security for a Connected World

SICHERHEIT FÜR DIE ELEKTRONISCHE LIEFERKETTE MIT DER SENTRIX® IoT SECURITY DEPLOYMENT PLATFORM

VEREINFACHUNG DER IOT-SICHERHEIT

Data I/O

Inhaltsübersicht

I. EINLEITUNG 3

II. DIE IOT-SECURITY LANDSCHAFTEN 4

GEFÄLTSCHTE PRODUKTE 5

IP- (INTELLECTUAL PROPERTY) UND MARKENSCHUTZ 5

SAFETY 5

DEN FOKUS SETZEN 5

III. SICHERE PRODUKTION VERTRAUSENSWÜRDIGER PRODUKTE 7

DER ANSPRUCH AN SICHERE UND VERTRAUENSWÜRDIGE PRODUKTE 7

DIE LIEFERKETTE DER ELEKTRONIKFERTIGUNG - HEUTE 7

OEM-FIRMWARE- UND DATENPROGRAMMIERUNG - HEUTE 8

INTEGRITÄT DER ELEKTRONISCHEN LIEFERKETTE 10

INTEGRATION VON SICHERHEITSELEMENTEN WÄHREND DER FERTIGUNG 10

PROVISIONIERUNG VOR ODER WÄHREND DER FERTIGUNG? 10

SICHERHEITSFAKTOREN 12

KOSTEN 13

IV. DIE SENTRIX SECURITY DEPLOYMENT PLATFORM 14

DIE SENTRIX SECURITY DEPLOYMENT PLATFORM: FUNKTIONSWEISE 15

PHASE I: SICHERHEITSKONZEPT UND SICHERER TRANSPORT VON OEM-DATEN 15

PHASE II: SICHERER IMPORT VON OEM-SICHERHEITSDATEN 16

PHASE III: SICHERHEITSPROVISIONIERUNG DER ICs 16

PHASE IV: REPORTING DER PROVISIONIERUNG 16

V. WIE SENTRIX DIE LIEFERKETTE ABSICHERT 17

AUSSCHLUSS VON GEFÄLSCHTEN ICS 17

SCHUTZ VON OEM-FIRMWARE UND -SOFTWARE WÄHREND DER FERTIGUNG 18

SCHUTZ VON OEM-GEHEIMNISSEN 18

VERMEIDUNG VON ÜBERPRODUKTIONEN 18

VERBESSERTE RÜCKVERFOLGBARKEIT IN DER LIEFERKETTE 18

NACHGELAGERTE SERVICES 19

VI. ZUSAMMENFASSUNG 21

I. Einleitung

DATA I/Os SENTRIX® SECURITY DEPLOYMENT PLATFORM ERFÜLLT DEN BEDARF DER ELEKTRONIKINDUSTRIE NACH EINER VEREINFACHUNG DES DEPLOYMENT-PROZESSES FÜR DIE IOT-SICHERHEIT

EINLEITUNG

Der Einsatz von IoT-Anwendungen und vernetzten Systemen steigt an. Das konfrontiert OEM und Anbieter datenzentrierter Dienste mit der Frage: **Wie lassen sich Security-Elemente einfach, sicher und kostengünstig in IoT-Bausteine implementieren?**

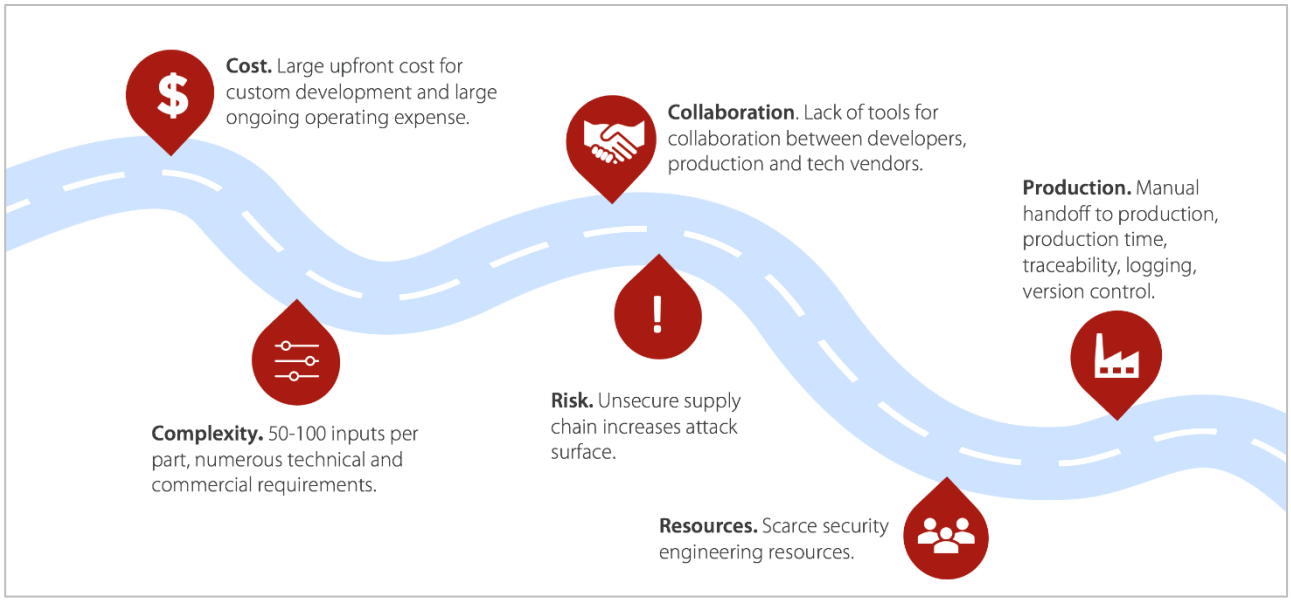
Die sichere Programmierung von IoT-Bausteinen ist der Prozess von der Definition bis zur sicheren Massenproduktion von Sicherheitsprofilen, Kontrollmaßnahmen und Konfigurationen, die erforderlich sind, um die Sicherheitsrisiken eines Bausteins während seines Lebenszyklus zu eliminieren.

Im Folgenden werden die Herausforderungen der heutigen Sicherheitsbereitstellungsprozesse und -systeme untersucht. Anschließend wird gezeigt, wie die SentriX Security Deployment Platform von Data I/O den Bedarf der Elektronikindustrie nach einer Vereinfachung des IoT-Sicherheitsimplementierungsprozesses sowie den Bedarf von OEMs nach einer kosteneffizienten und sicheren Lösung für die Programmierung sicherer Bausteine erfüllt.

Die moderne Elektronik-Lieferkette ist global, dezentralisiert und umfasst mehrere geografische Regionen, Organisationen und funktionale Abteilungen von verschiedensten Teilnehmern der Wertschöpfungskette, wie z. B. Halbleiteranbieter, Komponentenhändler, OEMs, Auftragshersteller (CMs) und andere. Die Komplexität der IoT-Bausteinsicherheit sowie die Komplexität und der Kostendruck der globalen Elektronik-Lieferkette schaffen mehrere Hindernisse für den Erfolg beim Einsatz von IoT-Sicherheit in der Massenproduktion:

- Kosten für benutzerdefinierte Software und Prozesse für die Implementierung von Sicherheit
- Mangel an Tools für die Zusammenarbeit der unterschiedlichen Organisationen an den verschiedenen Standorten
- Die manuelle Übergabe von Sicherheitsanforderungen von der Entwicklung an die Produktion ist fehleranfällig und nicht durchgehend nachvollziehbar.
- Es bestehen Sicherheitsrisiken, je nachdem, welche Unternehmen in die Lieferkette eingebunden sind.
- Mangel an spezialisierten Ressourcen für Sicherheits- und Software-Teams
- Komplexität der integrierten ICs und sicheren Mikrocontroller

II. Die IoT-Security Landschaften



Die IoT-Security Landschaften

Die Ursprünge von vertrauenswürdigem Handel anstelle des Austausches von Sachwerten reicht über 5.000 Jahre zurück.[1] Die alten Mesopotamier verwendeten Tontafeln und Siegel, um Banktransaktionen zu tätigen. Heute sind unsere Anmeldedaten (in der Regel unsere digitale Identität ergänzt durch einen zusätzlichen einzigartigen, geheimen Faktor) in modernen Kreditkartenchips eingebettet, die täglich Milliarden von Transaktionen in alle Länder der Welt ermöglichen.

Businessmodelle verändern sich heutzutage in Bezug auf Umsatzmodelle, Kundenerfahrungen und Unternehmensstrukturen, in ähnlicher Weise, wie der Handel durch sichere Kredite verändert wurde. Industrie- und Konsumgüterunternehmen setzen vernetzte Tools und Systeme ein, um Daten von Nutzern zu sammeln und um Kaufentscheidungen zu fördern. Unzählige Mensch-zu-Maschine- und Maschine-zu- Maschine-Transaktionen im Handel, bei Datendiensten und sogar bei sicherheitsrelevanten Abläufen basieren auf Daten vernetzter IoT-Systeme.

Ähnlich wie der Bankensektor mit seinen Kreditkarten hat auch die Industrie- und Konsumgüterbranche die Notwendigkeit und den Nutzen der Sicherung ihrer datengesteuerten Transaktionen und Kundenerfahrungen erkannt. Vertrauen ist ein wesentlicher Bestandteil für jede Anwendung, die zwischen vernetzten Geräten vorgenommen wird.

Ein ideales System zur Implementierung von Sicherheit, das Risiken beseitigt, weist die folgenden Eigenschaften auf:

- Niedrige Anfangskosten innerhalb eines Dienstleistungsmodells
- Intuitive Tools für die Zusammenarbeit von Fachleuten bei OEMs, Halbleiterherstellern und Produktionsstätten
- Automatisierte Handhabung von Sicherheitsmerkmalen und Programmierbausteinen, um Fehler zu reduzieren und Rückverfolgbarkeit zu ermöglichen
- Sichere Programmierung in einer vertrauenswürdigen Produktionsstätte
- Keine Notwendigkeit, umfangreiche spezialisierte Software- und Sicherheitsteams zu beschäftigen
- Abstrahierung der Komplexität von Sicherheits-ICs und sicheren Mikrocontrollern für eine einfache Nutzung

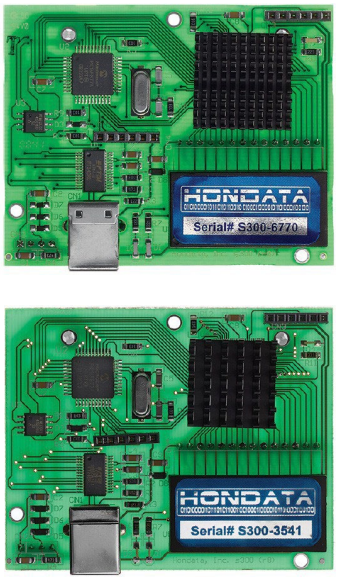
II. Die IoT-Security Landschaften

GEFÄLSCHTE PRODUKTE

Die Internationale Handelskammer schätzt, dass gefälschte Produkte und Produktpiraterie weltweit jährlich Kosten in Höhe von 1,7 Billionen Dollar verursachen.[2] Elektronik- und Halbleiterprodukte machen weltweit einen großen Teil der Fälschungen aus, wobei geschätzte 169 Milliarden Dollar an gefälschten Elektronikkomponenten im Umlauf sind.[3]

IP- (INTELLECTUAL PROPERTY) UND MARKENSCHUTZ

Im Jahr 2014 wurde ein Mann aus Florida wegen Handels mit gefälschten Hondata K-Pro- und S300-Motorsteuergeräten verurteilt. [4] Der Mann gab zu, dass er die Geräte in China nachbauen ließ - inklusive der Herstellung von Platinen und der Verwendung urheberrechtlich geschützter Software. Abgesehen von den offensichtlichen wirtschaftlichen Folgen für Hondata entstanden Sicherheitsprobleme, die sich auf den OEM und die Honda- und Acura-Fahrzeuge auswirkten, in die die gefälschten Einheiten eingebaut wurden.



Originale und gefälschte Hondata S300 Motorsteuergeräte. Können Sie die Fälschung erkennen? (Es ist das untere.)

SAFTEY

Nach Angaben des World Semiconductor Council gibt es Distributoren und Broker, die gefälschte Mikrocontroller (MCUs) zur Verwendung in zahlreichen sicherheitsrelevanten Anwendungen liefern oder dies versucht haben. So entdeckten die amerikanischen Strafverfolgungs-behörden beispielsweise gefälschte Mikrocontroller, die für Bremssysteme für Hochgeschwindigkeitszüge vorgesehen waren. Ein anderer OEM setzte gefälschte ICs für Ladestationen für Elektrofahrzeuge ein und erlitt einen Ausfall von 50 % aller Ladesäulen. Im einem dritten Beispiel kaufte ein OEM der auf automatisierte externe Defibrillatoren spezialisiert war gefälschte ICs von einem Zwischenhändler und erlitt eine Ausfallquote von 80 %.[5] Nach Angaben des US-Ministeriums für Heimatschutz aus dem Jahr 2019 stellten 16 % der von der US-Zollbehörde und der Einwanderungsbehörde beschlagnahmten Schmuggelware eine direkte und offensichtliche Bedrohung für die Gesundheit und Sicherheit dar.[6]

DEN FOKUS SETZEN

In der IoT-Sicherheitslandschaft gibt es die verschiedensten Möglichkeiten für Sicherheits-Anwendungsfälle, für Marken- und IP-Schutz (Firmware und/oder Sicherheitsnachweise) sowie zum Datenschutz und zur Regulierung.

II. Die IoT-Security Landschaften

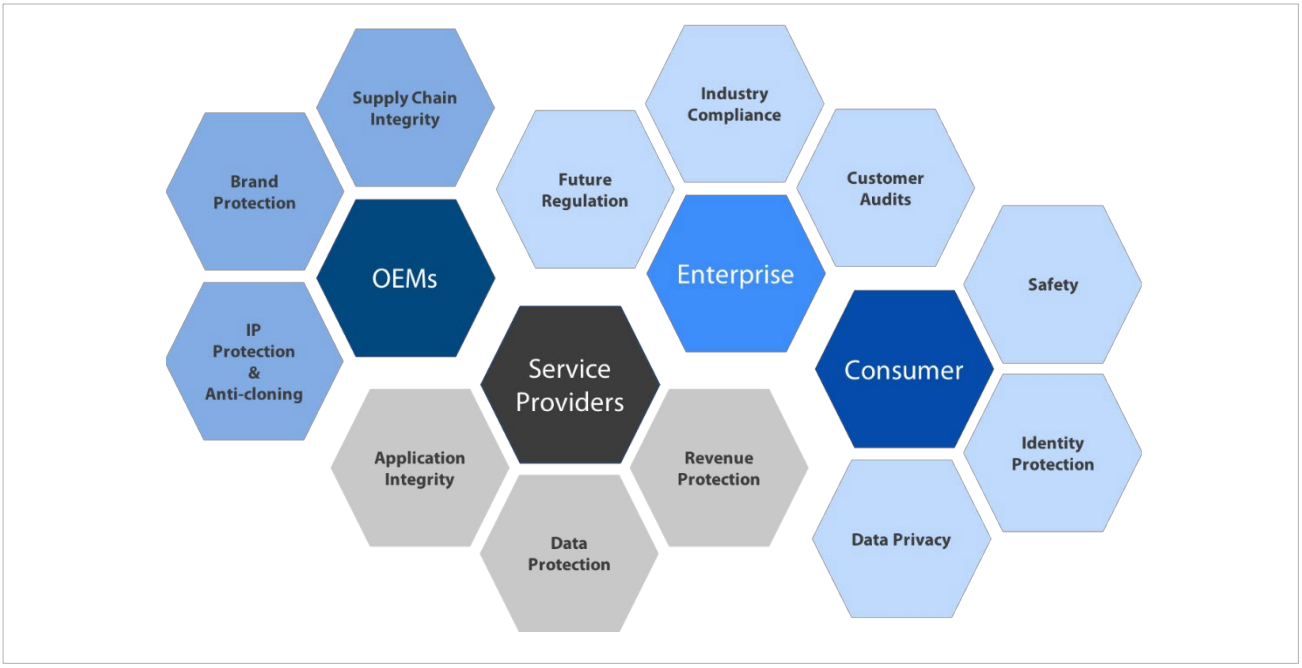


ABBILDUNG 2. IoT-Sicherheitslandschaft

Die überwiegende Mehrheit der Anwendungsfälle kann in unterschiedliche Gruppen von technischen Anforderungen heruntergebrochen werden, die durch Softwareanwendungen verwaltet werden können. Wir werden aufzeigen, warum diese Anwendungsfälle in der Elektronik-Lieferkette (einschließlich der Fertigung) wichtig sind und wie sie auf vereinfachte und kapitalschonende Weise realisiert werden können.
Die Markteinführungszeit vernetzter digitaler Produkte ist maßgeblich von den Ressourcen der Software- und Sicherheitsteams abhängig. Daher liegt es im unternehmerischen Interesse, bestehende Sicherheitsimplementierungsdienste zu nutzen, wenn sich dadurch die folgenden Hindernisse umgehen lassen:

- Hoher und nicht ausreichend genutzter Investitionsaufwand
- Hohe Betriebskosten für besonders gesicherte Betriebsstätten und spezialisierte Ressourcen
- Schreiben von spezialisiertem Code
- Unsichere Prozessen und Richtlinien

Die Vorabkosten für die Erstellung und Bereitstellung von Hunderttausenden Identitätsnachweisen für ein vernetztes Produkt können im ersten Jahr leicht 500.000 US-Dollar übersteigen. Auch die laufenden Betriebskosten können leicht 200.000 Dollar pro Jahr übersteigen. Diese hohen Kosten sind auf die herkömmliche Praxis zurückzuführen, bei der ein maßgeschneiderter Prozess mit kundenspezifischer Software und spezieller Hardware, in einer Fertigungslinie, bei einem Auftragsfertiger oder im Werk des OEMs, eingesetzt wird. Darüber hinaus führt die Implementierung von Sicherheitsmaßnahmen am oder kurz vor dem Ende des Elektronikmontageprozesses zu zusätzlichen Sicherheitsrisiken, da kein Schutz vor Eingriffen in den Lebenszyklus der Produkte vor der Implementierung der Sicherheitsmaßnahmen besteht.

III. Sichere Produktion vertrauenswürdiger Produkte

Der Anspruch an sichere und vertrauenswürdige Produkte

Die meisten elektronischen Produkte, mit denen wir heute interagieren (z. B. ein intelligentes Thermostat, Smartwatches, vernetzte Autos), sind Teil einer Vielzahl von Technologien (Sensorknoten, Gateways und Cloud-Server), die entweder mit der Cloud, miteinander oder mit beidem verbunden sind. Der smarte Charakter dieser Produkte ist auf die jeweils eingesetzte Anwendungs-firmware zurückzuführen, die auf jedem elektronischen Produkt läuft. In einer typischen IoT-Anwendung erfassen die Sensoren die physische Umgebung und erstellen Datensätze für die Analyse. Datensätze von verschiedenen Edge-Knoten werden gesammelt und in Datenaggregationssystemen wie Gateways verarbeitet (gefiltert, formatiert). Die Gateways senden die Daten dann zur Verarbeitung an die Cloud-Server weiter. Sobald die Daten auf den Gateways oder Servern verarbeitet sind, werden in der Logikeinheit Entscheidungen getroffen und/oder Befehle an Ausgabesysteme und Steuergeräte gesendet, um eine Aktion durchzuführen.

Eine vernetzte und dezentrale IoT-Anwendung, wie oben beschrieben, ist, wenn sie nicht ausreichend gesichert ist, sehr anfällig für Angriffe, wie:

- Hacken von Systemen, um Daten oder Firmware zu stehlen
- Einschleusen von Malware, um den Betrieb zu verändern
- Ändern der bestehenden Firmware, um Funktionsabläufe zu ändern
- Einschleusen gefälschter Bausteine durch vorherigen Diebstahl von Identitäten
- Austausch fehlerhafter Daten zwischen Bausteinen und Anwendungsprogrammen

Jede dieser Aktionen kann einem OEM einen enormen finanziellen und ideellen Schaden zufügen. Daher ist der Schutz von programmierbaren Bausteinen und Anwendungen vor Man-in-the-Middle-Angriffen für OEMs unerlässlich. Um eine IoT-Anwendung entsprechend zu schützen, müssen alle Bausteine, die in die Anwendung einbezogen sind, einen vertrauenswürdigen Status haben und abgesichert sein.

Ein abgesicherter Programmierbaustein weist die folgenden Sicherheitsmerkmale auf:

- Eine unveränderliche und eindeutige Identität innerhalb der IoT-Anwendung
- Eine Sicherung von Firmware und Daten vor unbefugten Änderungen oder Verlust
- Die Fähigkeit zur Ausführung von Firmware und zur Verarbeitung von Daten in einer sicheren Prozessumgebung
- Schutz der Daten vor Veränderung oder Verlust beim Austausch mit anderen Geräten

Die Lieferkette der Elektronikfertigung - Heute

Um den Einsatz von IoT-Sicherheit in der Massenproduktion besser zu verstehen, ist es wichtig, den Lebenszyklus elektronischer Geräte und die jeweiligen Teilnehmer der Lieferkette zu kennen. Die folgende Abbildung 3 zeigt den Lebenszyklus eines Programmierbausteins.

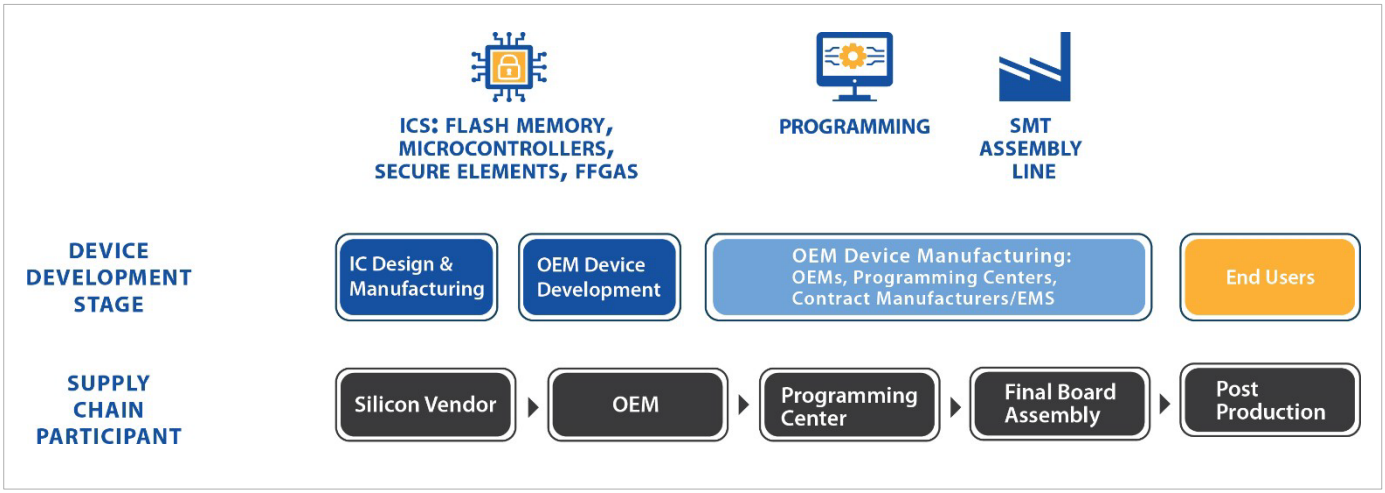


ABBILDUNG 3. Lebenszyklus der Herstellung eines elektronischen Produktes

III. Sichere Produktion vertrauenswürdiger Produkte

Ein Halbleiterhersteller ist ein Unternehmen, das integrierte Schaltungen (ICs) wie Mikroprozessoren, Mikrocontroller und Speicherchips entwickelt und herstellt. Beispiele für Halbleiterhersteller sind Intel, NXP, Infineon, Broadcom, Mikrochip, usw. Die ICs sind das Gehirn des elektronischen Geräts.

Der OEM ist das Unternehmen, das das elektronische Produkt (z. B. ein Auto, einen intelligenten Stromzähler, ein intelligentes Schloss, etc.) entwickelt und gestaltet. Während der Entwicklung definiert der OEM die Anforderungen und Merkmale des elektronischen Produktes, entwirft die Hardware (einschließlich der IC-Auswahl), entwickelt die Leiterplatte (PCB) und die Firmware, die auf dem Prozessor-IC laufen wird. Während dieser Entwicklungsphase stellt der OEM auch einige Muster des elektronischen Produktes her, um Merkmale und Funktionalitäten zu validieren und zu testen. Das Produkt geht dann von der Entwicklungsphase in die Fertigungsphase.

In der Fertigungsphase arbeiten die meisten OEMs mit Zulieferern wie IC-Distributoren, IC-Programmierzentren und Auftragsherstellern (CMs) zusammen, um Teile zu beschaffen und technische Geräte in ihrem Namen herzustellen. Wenn ICs von Distributoren bezogen werden, werden diese direkt an die Auftragshersteller geschickt, die die IC-Komponenten auf einer Leiterplatte montieren, in der Regel mit SMT-Technologie (Surface Mount Technologie). Sobald die Leiterplatten mit den richtigen IC-Komponenten bestückt sind und die richtige OEM-Firmware mit den entsprechenden Daten in die ICs programmiert wurden, durchlaufen die neuen elektronischen Produkte Hardware- und Softwaretests sowie Validierungen, um sicherzustellen, dass alles wie erwartet funktioniert. Die Produkte gehen dann von der Herstellungsphase in die Nachproduktionsphase (auch "Betriebsphase" genannt) über, wo sie für die Endbenutzer konfiguriert werden.

OEM-Firmware und Datenprogrammierung - Heute

Abbildung 4 zeigt die verschiedenen Methoden der OEM-Firmware- und Datenprogrammierung während des Lebenszyklus.

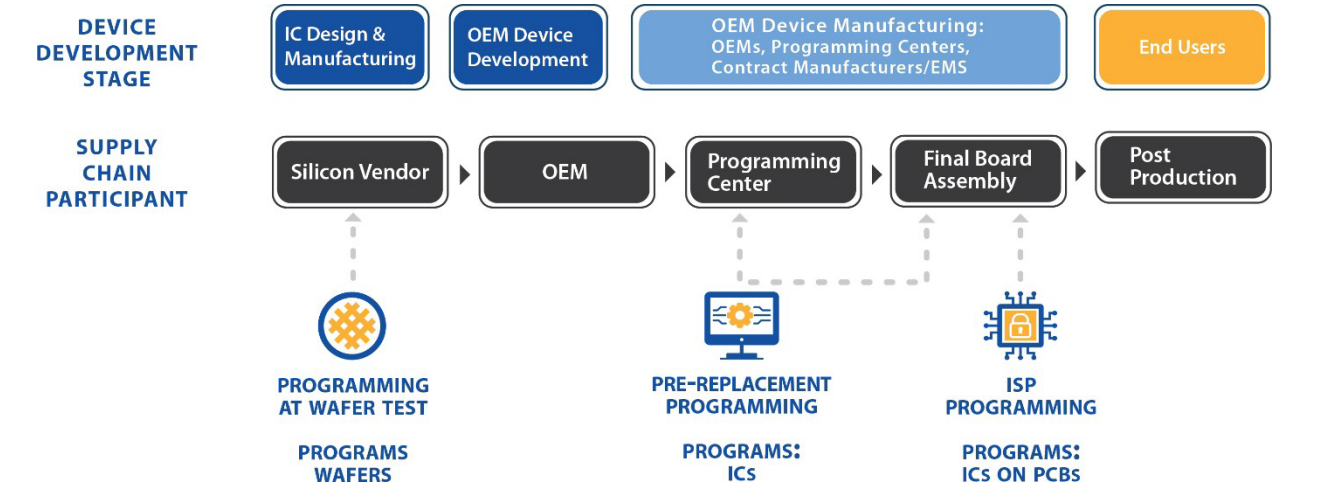


ABBILDUNG 4. Programmiermethoden, die während des Lebenszyklus eines elektronischen Produktes verwendet werden.

III. Sichere Produktion vertrauenswürdiger Produkte

Für die OEM-Firmware- und Datenprogrammierung in ICs während der Fertigung, stehen den OEMs im Allgemeinen zwei Möglichkeiten zur Verfügung:

Pre-Programming

- Die Programmierung erfolgt in einem Programmierzentrum (ein Zulieferer, der Firmware- und Datenprogrammierungs-dienste anbietet) oder bei einem Auftragsfertiger
- Die Programmierung erfolgt, bevor die ICs auf einer Leiterplatte bestückt werden.
- Jeder einzelne IC wird in einem bauteilspezifischen Sockel in einem Programmiersystem programmiert
- Die Programmierung erfolgt durch die Aktivierung der IC-Pins über ein vom IC unterstütztes Kommunikationsprotokoll (z. B. JTAG, UART, I2C, SPI usw.)

In-System-Programming (ISP)

- Die Programmierung erfolgt bei einem Auftragsfertiger
- Die Programmierung erfolgt, nachdem die ICs auf einer Leiterplatte bestückt wurden.
- Der Programmierprozess ist in die Phase der Funktionsprüfung und des Tests des Produktes nach der Leiterplatten-bestückung integriert.
- Die Programmierung erfolgt über Pads auf der Leiterplatte, die die IC-Pins über ein vom IC unterstütztes Kommunikationsprotokoll aktivieren (z. B. JTAG, UART, I2C, SPI usw.)

Um kleine Datenmengen in Bausteine zu programmieren, gibt es noch eine dritte Möglichkeit der Programmierung. Diese kann auch während der Wafer-Testphase der IC-Herstellung erfolgen. Bei der Programmierung auf Wafer-Ebene werden Wafersonden verwendet, die zum Testen der ICs eingesetzt werden. Es handelt sich definitionsgemäß nicht um einen bauteilspezifischen Prozess, da der gesamte Wafer programmiert wird. Die Program-mierung auf Waferebene findet am Standort der IC-Fertigung statt, so dass der Halbleiterhersteller die endgültige Kontrolle über die Programmierung hat.

Zur Erinnerung: Die Lieferkette der Elektronikfertigung ist global und geografisch weltweit verteilt. Sie besteht aus mehreren Beteiligten, die an den unterschiedlichen Herstellungsphasen im Lebenszyklus von technischen Produkten beteiligt sind. Im Herstellungsprozess ist es gängige Praxis, dass ein OEM ein Produkt in einem OEM-Entwicklungslabor entwickeln lässt, dass geografisch unterschiedliche Standorte hat. Die IC-Beschaffung und Programmierung von Firmware und Daten kann wiederum in der Fabrik eines Dritten, in einem anderen Teil der Welt, stattfinden. Auch die abschließende Prüfung und Montage der ICs kann bei einem Drittanbieter an einem weiteren geografischen Standort stattfinden. Die Betriebsphase, in der die Konfiguration für den End-User erfolgt wird in der Regel in einem weiteren Betrieb und an einem anderen Standort vorgenommen, der sich von allen Standorten und Betriebseinheiten der Vorfertigung und Fertigung unterscheidet. Ein wichtiger Grund für eine solche global verteilte Lieferkette ist die Kostenoptimierung. Mit anderen Worten: Die Lieferkette für die Herstellung ist in erster Linie darauf ausgerichtet, die Gesamtkosten für die Herstellung zu optimieren.

III. Sichere Produktion vertrauenswürdiger Produkte

Integrität der elektronischen Lieferkette

Im Folgenden geht es um die Sicherheit in der Fertigung und die zentrale Frage: Ist die Lieferkette für elektronische Produkte heutzutage sicher? Sicherheitsexperten behaupten, sie sei es nicht. [7] Das liegt daran, dass die derzeitigen Fertigungsverfahren, die in der Lieferkette eingesetzt werden, meist unsicher sind. So können OEMs beispielsweise nicht sicherstellen, dass die in den Betriebsstätten eines Drittanbieters hergestellten Produkte echte ICs und keine Fälschungen beinhalten. Es gibt keine Garantie dafür, dass die Produkte ohne Änderungen mit der vom OEM spezifizierten Firmware und den Daten programmiert werden. Es gibt auch keine Garantie dafür, dass das geistige Eigentum der OEMs (IP) wie das Leiterplattendesign, Firmware oder Daten während des Herstellungsprozesses nicht gestohlen werden. Ein weiteres Problem für OEMs ist die Verwaltung des Herstellungsprozesses, so dass nur eine vom OEM vorgegebene Anzahl eines Produktes produziert wird. Die Verwendung gefälschter ICs, das Klonen von elektronischen Produkten, die Manipulation und die Überproduktion sind akute Probleme in der Elektronikfertigung, die OEMs Milliarden von Dollar an entgangenem Umsatz und Markenwert kosten. Berichten zufolge verlieren Verbrauchsgüter- und Industrieunternehmen jedes Jahr 250 Milliarden Dollar durch gefälschte elektronische Komponenten.[8] In ihrem derzeitigen Zustand ist die Lieferkette der Elektronikfertigung unsicher und man kann sich nicht darauf verlassen, dass sie Software, Firmware und das geistige Eigentum der OEMs schützt.

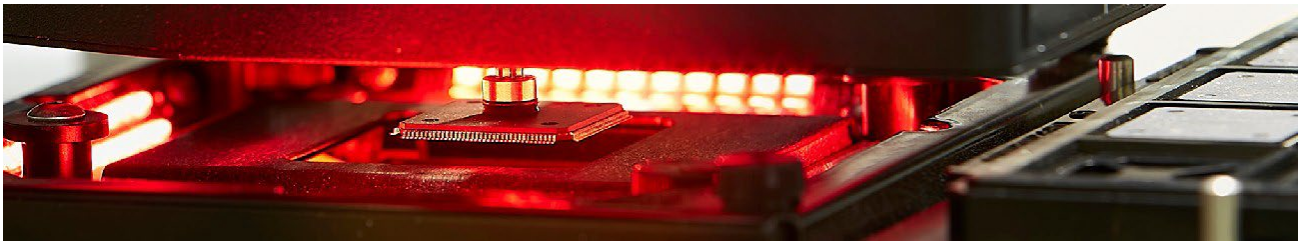
Eine sichere Fertigung erfordert von den OEMs die Einführung neuer und verbesserter Verfahren und Tools, die eine bessere Kontrolle und Verwaltung der Fertigungsprozesse in den Fabriken von Zulieferern ermöglichen.

Ziel ist es, sicherzustellen, dass OEM-Produkte gemäß den OEM-Spezifikationen für Hardware, Firmware und Daten und ohne Verlust von OEM-IP hergestellt werden. Eine wichtige Anforderung der OEMs ist, dass neue Prozesse oder Tools, die zur Sicherung der Lieferkette eingeführt werden, keine wesentlichen zusätzlichen Herstellungskosten verursachen, die Markteinführung nicht verzögern und den bestehenden Herstellungsprozess nicht stören dürfen. In welcher Phase des Produktlebenszyklus sollte das Produkt gesichert werden? Heutzutage ist es üblich, dass elektronische Produkte ein Firmware-Update (für neue Funktionen, zur Behebung von Softwarefehlern, zur Beseitigung von Sicherheitslücken) herunterladen, wenn es zum ersten Mal in Betrieb genommen wird. Um einen solchen Vorgang sicher zu unterstützen, muss das Produkt mit einem OEM-Update-Server kommunizieren. Dies bedeutet, dass es über eine sichere Identität sowie die Fähigkeit zur sicheren Datenkommunikation verfügen muss, die während der Herstellung integriert wurde. Daher ist es für OEMs unerlässlich, ihre Produkte abzusichern, bevor sie im Feld in Betrieb genommen werden.

Werden beispielsweise während der IC-Fertigung unveränderliche IC-Identitäten eingeführt, können gefälschte ICs während der Programmierung vor der Fertigung entdeckt und aus der Produktionskette entfernt werden, bevor in einem späteren Stadium zusätzliche Programmierungen vorgenommen werden, die die Firmware potenziell in einem gefälschten Chip speichert.

Integration von Sicherheitselementen während der Fertigung

In erster Linie müssen OEMs ihre Produkte nach dem Prinzip "Security by Design" entwickeln. Sicherheit durch Design erfordert, dass OEMs ihre Produkte mit ICs entwickeln, die Folgendes bieten:



III. Sichere Produktion vertrauenswürdiger Produkte

- Schutz des Speichers durch einen hardwarebasierten Roots-of-Trust
- Eine zuverlässige Anwendungsumgebung
- Ein unveränderlicher Boot-Pfad
- Ein Mechanismus zur Erzeugung echter Zufallszahlen (TRNG)

Ein verschlüsselter Speicher dient zur sicheren Datenspeicherung von Firmware im Ruhezustand und zur sicheren Speicherung von Daten während der Codeausführung. Ein unveränderlicher Boot-Pfad und ein Mechanismus zur Erzeugung echter Zufallszahlen ermöglichen die Erzeugung und Verwendung einer eindeutigen Bausteinidentität. Secure Elements und Secure Mikrocontroller sind zwei Typen von Sicherheits-ICs mit integriertem hardwarebasiertem Roots-of-Trust. Secure Elements sind Standalone-ICs, die in Kombination mit einem unsicheren Mikrocontroller (mit bestimmten Prozessen und Verfahren) ein OEM-Produkt absichern können. Secure Mikrocontroller verfolgen einen anderen Ansatz als Secure Elements, da sie die hardwarebasierten Sicherheitsgrundlagen direkt in sich integrieren. Die Verwendung sicherer ICs ist zwar notwendig, um das Endprodukt zu sichern, aber sie allein reicht nicht aus. Es müssen zusätzliche Vorgänge durchgeführt werden, um die Sicherheit, die durch den hardwarebasierten Roots-of-Trust gegeben ist, weiter auszubauen und zu verbessern. Dies wird in der Fertigung durch den Prozess der Sicherheitsprovisionierung erreicht.

Konkret wird bei der Sicherheitsprovisionierung die Programmierung des Hardware-Roots-of-Trust in einen IC vorgenommen. Damit werden die Bausteinidentität und die spezifischen Sicherheitsnachweise erstellt und als Sicherheitselemente an den IC gebunden. Dieser Prozess der Sicherheitsprovisionierung ermöglicht die folgenden Sicherheitsmerkmale auf dem Endprodukt:

- Bausteinidentität und Authentifizierung
- Vertrauenswürdiger Speicher für Firmware und Daten
- Vertrauenswürdige Ausführung von Firmware
- Secure Boot
- Ausführung von authentifizierter und/ oder verschlüsselter Firmware
- Verschlüsselung/ Entschlüsselung von Daten
- Firmware-Updates

Die Sicherheitsmerkmale, die in einem programmierten Baustein aktiviert werden müssen, sind von Baustein zu Baustein unterschiedlich und hängen von der Anwendung, der Art des Einsatzes und der physischen Umgebung ab, in welcher der IC eingesetzt wird. Dennoch sind alle oben genannten Sicherheitsmerkmale auf einen sicheren Provisionierungsprozess angewiesen. Sicherheitsnachweise wie Schlüssel, Zertifikate, Firmware und Daten, die in einem IC hinterlegt werden, sind sehr wichtige Geheimnisse für einen OEM. Sollte ein krimineller Akteur während des Herstellungsprozesses Zugang zu diesen Sicherheitsdaten erhalten, kann die Sicherheit der Endprodukte gefährdet sein. Um die Sicherheitsdaten zu schützen, die während der Herstellung der Produkte implementiert werden, ist es von grundlegender Bedeutung, dass der Provisionierungs-prozess selbst sicher ist.

III. Sichere Produktion vertrauenswürdiger Produkte

Provisionierung vor oder während der Fertigung?

Sicherheitsfaktoren

Ein gängiges Szenario bei der Herstellung von OEM-Produkten kombiniert die Montage und Prüfung dieser Produkte mit zunächst nicht verschlüsselten MCUs durch einen externen Auftragsfertiger. Der OEM stellt dem Auftragsfertiger IC-Komponenten und Anwendungsfirmware zur Verfügung, die nach der Leiterplatten- bzw. Bausteinbestückung mittels In-System-Programmierung (ISP) provisioniert werden. Da der OEM in diesem Szenario den Prozess der Montage nicht kontrolliert, gibt es für ihn keine Möglichkeit die Authentifizierung der MCUs, bevor die Bausteine auf der Platine platziert sind. Ein krimineller Akteur könnte hier die ursprünglichen Mikrocontroller leicht durch eine gefälschte Variante ersetzen. Die gefälschten Mikrocontroller werden dann zur Herstellung eines Produktes verwendet und durchlaufen Funktionsprüfungen und Tests, ohne dass der OEM bemerken konnte, dass seine spezifizierten und bereitgestellten ICs vertauscht wurden. Eine ähnliche Situation kann in Bezug auf programmierte Firmware entstehen: Hier könnte in der Einrichtung eines Drittanbieters Malware oder Backdoor-Software zusammen mit der Original-Firmware provisioniert werden, wodurch das Produkt während seines Betriebs anfällig für Angriffe wird.

Ein anderer Ansatz besteht darin, ein Produkt zu verschlüsseln, in dem Secure Mikrocontroller verwendet werden, die durch Pre-Placement-Programmierung im Werk des OEM oder in einem Programmierzentrum provisioniert werden. Bei der Implementierung von Sicherheitsmerkmalen in ein elektronisches Produkt wird ein Identitätszertifikat erzeugt, das dem Schlüssel für die Produktidentität entspricht, und zusammen mit der Firmware in den Mikrocontroller eingespielt wird. Zusätzlich werden eine Signatur der Firmware sowie ein entsprechender Schlüssel im sicheren Speicher des MCU provisioniert. Die provisionierten MCUs werden dann verriegelt und zur Montage und Prüfung an den Auftragsfertiger versandt. Nach dem Zusammenbau und während der Funktionsprüfung beim Auftragsfertiger kann der OEM einen Test durchführen, um die Authentizität der Mikrocontroller nachzuweisen. Dieser wird nur bestanden, wenn die vom OEM sicher programmierten, also provisionierten MCUs verbaut wurden. Sollte bei der Montage ein Austausch vorgenommen worden sein, schlägt der Echtheitstest fehl. Kriminelle Handlungen sind unmöglich, da sich die richtigen Sicherheitsnachweise (ein Identitätszertifikat mit entsprechendem Identitätsschlüssel) auf dem gefälschten MCU nicht erstellen lassen.

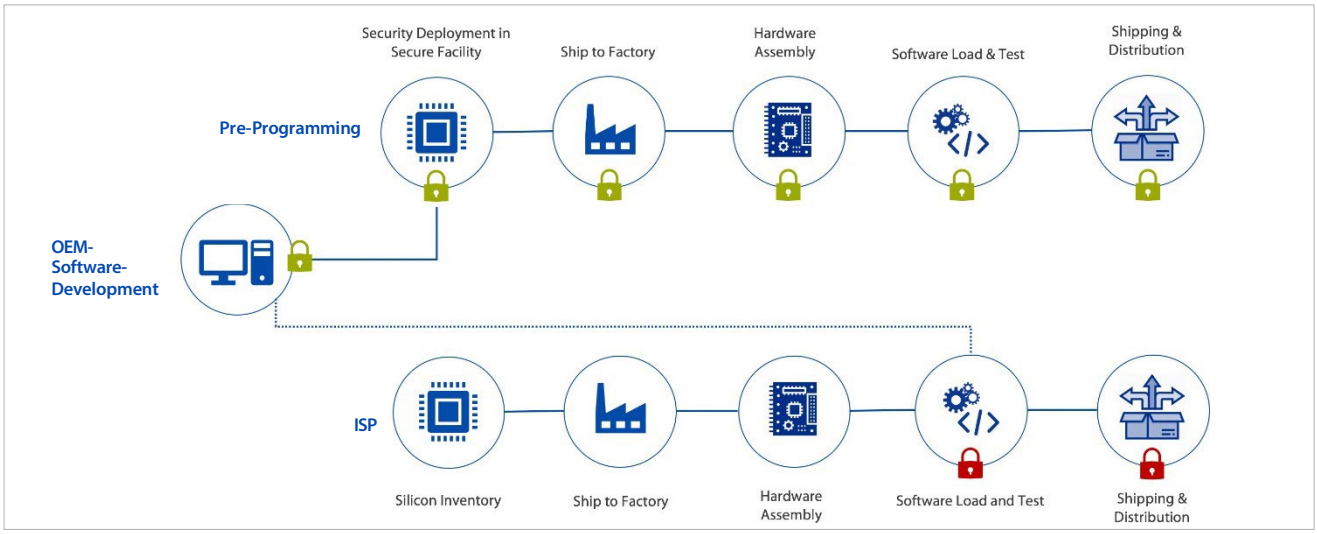


ABBILDUNG 5: Integrität der Lieferkette bei der Einführung von Sicherheit durch Vorprogrammierung im Vergleich zur systeminternen Programmierung.

III. Sichere Produktion vertrauenswürdiger Produkte

Zusätzlich zum MCU-Authentizitätstest wird die programmierte Firmware auf Veränderungen geprüft. Die Firmware-Signatur wird anhand der gespeicherten Sicherheitsmerkmale neu generiert und mit der Signatur, die während der Firmware-Programmierung erstellten wurde, verglichen. Wenn die Signatur nicht übereinstimmt, schlägt der Test fehl. Wenn entweder der MCU-Authentifizierungstest oder der Firmware-Signaturtest fehlschlägt, wird das Produkt entfernt.

Um eine verschlüsselte Programmierung von ICs zu gewährleisten, müssen OEMs ihre Sicherheitsdaten (Schlüssel, Bootloader, Firmware) Dritten zur Verfügung stellen. In solchen Fällen ist die Provisionierungsmethode für ICs durch Vorprogrammierung (bevor die ICs auf die Leiterplatte verbaut werden) wesentlich sicherer als die Provisionierung durch systeminterne Programmierung (nachdem die ICs auf die Leiterplatte montiert wurden). Dies liegt daran, dass bei der Vorprogrammierungsmethode die Angriffsfläche auf die Pins des IC-Gehäuses beschränkt ist, während sich bei der systeminternen Programmiermethode die Bedrohungsfläche auf die gesamte Leiterplatte bzw. auf das gesamte Bauelement und die zahlreichen Verbindungen sowie die Software, die mit den Pins des ICs verbunden ist, ausdehnt. Die letztgenannte Bedrohungsfläche ist sicherlich viel größer als die Erstgenannte.

Kosten

Um die systeminterne Programmierung durchzuführen, muss der OEM die Programmierung während der Designphase des Bauteils/der Leiterplatte einplanen (z. B. müssen Programmierkontakte auf der Leiterplatte platziert werden). Dieser Schritt erhöht die Komplexität, den Zeitaufwand und die Kosten des PCB-Designprozesses. Jeder Fehler im Designprozess kann sich stark auf die Massenproduktion des Endproduktes auswirken und Korrekturen sind mit sehr hohen Kosten und Verzögerungen verbunden (Neudesign oder Neulayout der Baugruppe). Im Gegensatz dazu erfolgt die Vorprogrammierung über die Pins des IC-Gehäuses, wobei das Gehäuse und die Pinbelegung während der IC-Herstellung festgelegt werden.

Daher hat die Vorprogrammierung keine Auswirkungen auf den Designprozess des OEMs und verursacht keine zusätzlichen Entwicklungskosten. Die Vorprogrammierung erfolgt asynchron zur Leiterplattenbestückung, so dass keine Abhängigkeiten oder Einschränkungen bei der Bestückung entstehen. Die Methode der Vorprogrammierung ist im Allgemeinen flexibler und kostengünstiger als die systeminterne Programmierung. Der Grund dafür ist, dass die Entwicklung der Programmierung eines ICs einmalige Hardware- und Firmware-Kosten verursacht, die über mehrere Designs und mehrere OEMs, die denselben IC für ihr Produkt wählen, amortisiert werden können. Im Gegensatz dazu ist die Hardware- und Firmware-Freischaltung für die In-System-Programmierung sehr spezifisch für ein PCB-Design-Layout. Daher können die Aktivierungskosten nicht über unterschiedliche Produkte desselben OEM oder über ähnliche ICs, die von verschiedenen OEMs verwendet werden, amortisiert werden.
Zusammenfassend lässt sich sagen, dass die Kosten für eine ISP-Lösung für den Einsatz von OEM-Sicherheit wesentlich höher sind und je nach Produktionsvolumen das Zwei- bis Fünffache betragen können.

Für die Sicherheitsprovisionierung mittels ISP müssen OEMs zusätzliche Sicherheitsvorrichtungen (Schlüsselserver, ein Hardware-Sicherheitsmodul (HSM) usw.) bei ihrem Auftragsfertiger implementieren, um eine sichere Verbindung an das Programmiersystem zu schaffen. Während Auftragsfertiger diese Infrastruktur betreiben, liegt das Wissen über den Sicherheitsprozess im Allgemeinen ausschließlich beim OEM. Daher werden die betriebliche Wartung und der laufende Support für die Provisionierung in der Regel vom OEM durchgeführt, was spezielles Fachpersonal erfordert und die Betriebskosten für die OEMs in die Höhe treibt. Da die Provisionierungs-Lösung in den Räumlichkeiten eines Drittanbieters betrieben wird, der sich möglicherweise an einem anderen Ort als der OEM befindet, kann die Behebung von Problemen im Zusammenhang mit der sicheren Programmierung kostspielig sein. Bei der Sicherheitsprovisionierung durch Vorprogrammierung fallen derartige Betriebskosten nicht an.

IV. Die SentriX Security Deployment Platform

ABBILDUNG 6. SentriX Security Deployment Platform

Die SentriX Security Deployment Platform

Data I/O hat die SentriX Security Deployment-Platform entwickelt, um eine sichere Fertigung zu gewährleisten. Mit SentriX haben OEMs nun die Möglichkeit, ihre Lieferkette zu sichern und mithilfe eines vertrauenswürdigen Sicherheitsimplementierungsdienstes verschlüsselte Programmierbausteine in großem Umfang herzustellen. Die Implementierung von Sicherheitsmechanismen in die Halbleiter übernimmt eine Sicherheitsmanagement-Software. Die Betriebskosten sind weder von einem bestimmten PCB-Design abhängig noch erfordern sie Vorabinvestitionen in Software oder Hardware. Abbildung 6 zeigt das SentriX-Sicherheitssystem, das aus mehreren Hardware- und Softwarekomponenten besteht, darunter:

- Software für das Sicherheitsmanagement
- Entwicklungstools
- Rückverfolgbarkeitssoftware (Track & Trace)
- Mehrere Bausteinprogrammer
- Hardware-Sicherheitsmodul (HSM)
- IC-Bestückung (pick-and-place)
- Computer-Vision-System IC-Lasermarkierung

Alle oben aufgeführten Komponenten sind in ein System integriert, in dem mehrere Bausteinprogrammer gleichzeitig auf bis zu 112 Sicherheitsmikrocontroller eine verschlüsselte Programmierung durchführen. SentriX integriert ein FIPS 140-2 Level 2 konformes HSM, das die sichere Programmierung von Authentifizierungsdaten in Sicherheits-ICs ermöglicht. Die SentriX-Sicherheitsplattform umfasst ein Entwicklungstool namens SentriX Product Creator, mit dem OEMs die in ihrem Baustein zu implementierenden Sicherheitsfunktionen definieren können. SentriX Product Creator schützt auch die Geheimnisse und die Firmware während des Transports zwischen den Betriebsstätten des OEM zu jenen, in denen SentriX betrieben wird. Die Sicherheitsverwaltungssoftware ermöglicht die Erstellung und Ausführung von Provisionierungsaufträgen auf der SentriX-Plattform. Teil des Systems ist eine Rückverfolgbarkeits- und Berichterstattungssoftware, die Programmieraufträge und weitere Informationen auf IC-Ebene verwaltet, um für die Rückverfolgbarkeit, die Auditierbarkeit und die Übermittlung von OEM-Sicherheitsnachweisen zu sorgen.

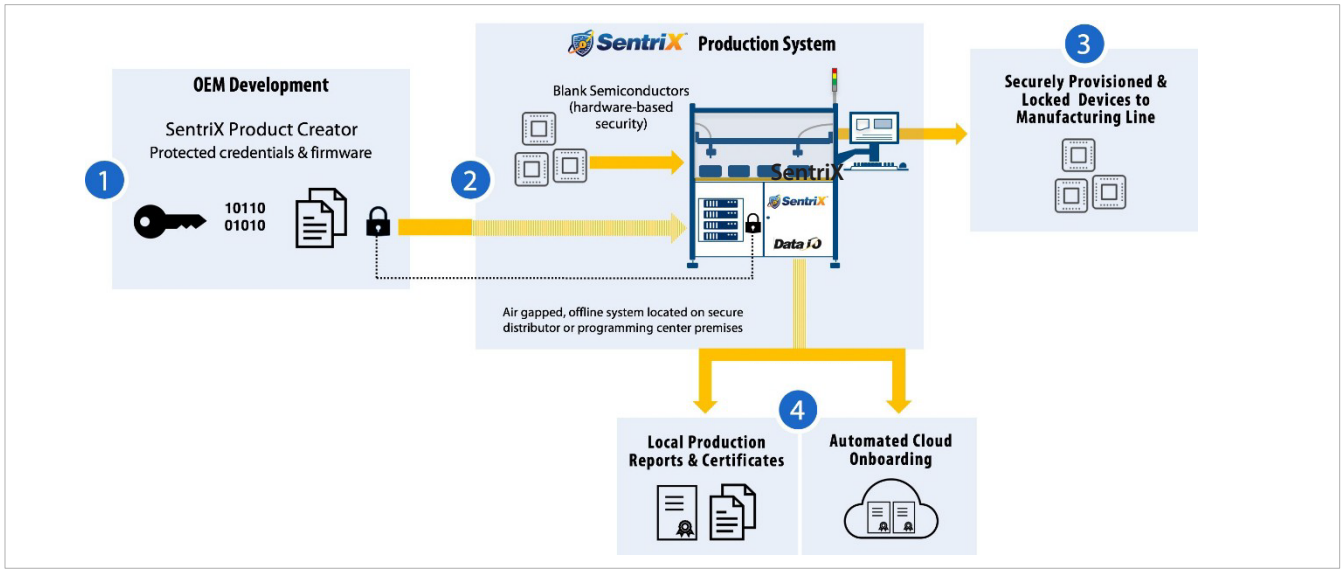


ABBILDUNG 6. SentriX Security Deployment Prozess und Platform.

IV. Die SentriX Security Deployment Platform

Die SentriX Security Deployment Platform: Funktionsweise

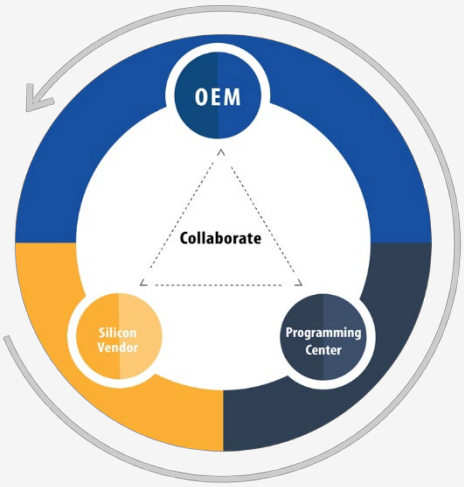
Phase I: Sicherheitskonzept und sicherer Transport von OEM-Daten
Um den Prozess der Sicherheitsimplementierung einzuleiten, wird das SentriX Product Creator-Tool am OEM-Entwicklungsstandort verwendet. OEMs verwenden das SentriX Product Creator-Tool, um auszuwählen, welche Sicherheitsmerkmale in die ICs eingesetzt werden sollen und wie. Das Tool unterstützt zwei Modelle: Vorkonfigurierte und benutzerdefinierte Anwendungsfälle.

Das benutzerdefinierte Deployment-Modell ermöglicht die Programmierung aller Sicherheitsfunktionen und -einstellungen, die für einen bestimmten IC verfügbar sind. Das Modell für vorkonfigurierte Anwendungsfälle stellt dem OEM die gängigsten IoT-Anwendungsfälle zur Verfügung und nimmt im Namen des OEMs allgemeine Entscheidungen, Richtlinien und Einstellungen vor, um die Nutzung zu erleichtern. Die vorkonfigurierten Anwendungsfälle hängen von dem jeweiligen IC ab, umfassen aber typischerweise:

- Chip-ID
- Authentizität der Chips
- Onboarding in der Cloud
- Secure Boot
- Zugangskontrolle
- Verschlüsselte Firmware
- Sichere Kommunikation
- Statische Daten

Vorkonfigurierte Anwendungsfälle
- Unterstützt die gängigsten Anwendungsfälle
- Geeignet für große und kleine Stückzahlen
- Einfach zu verwendende vorkonfigurierte Anwendungsfälle

Benutzerdefinierte Anwendungsfälle
- Unterstützt jeden Anwendungsfall
- Hohe Flexibilität
- Geeignet für hohe Stückzahlen
- Optimiertes Sicherheitsmanagement



Ein Tool für OEMs, Halbleiterhersteller und Programmierhäuser

ABBILDUNG 8. Modell der Zusammenarbeit mit dem SentriX Product Creator

Der SentriX Product Creator schützt Firmware und Sicherheitsnachweise (zusammen das "Sicherheits-definitionspaket") vor einem Man-in-the-Middle-Angriff, bei dem versucht werden könnte, das Sicherheits-definitionspaket während der Übertragung zu stehlen oder zu verändern. Das geistige Eigentum wird durch Verschlüsselung und elektronische Signaturen geschützt. Um das geistige Eigentum auch während des Transports zu schützen, bindet das SentriX Product Creator-Tool das Sicherheitsdefinitionspaket an ein bestimmtes SentriX-Produktionssystem oder eine Gruppe von SentriX-Produktionssystemen, die vom selben Unternehmen betrieben werden. Wenn ein krimineller Akteur versucht, dieses OEM- Sicherheitsdefinitionspaket zu verwenden, um Bausteine auf einem anderen System zu provisionieren, schlägt der Prozess fehl.

Der SentriX Product Creator ermöglicht mehreren Projekt-teilnehmern die sichere Erfassung von Sicherheitsobjekten wie Schlüsseln oder Zertifikaten für ein und denselben OEM-Baustein. Darüber hinaus verwaltet das SentriX-Produktions-system potenzielle Konflikte zwischen diesen Eingabe-quellen, so dass die endgültige Implementierung der Sicherheitsmerkmale eine verwaltete und kontrollierte Kombination der erforderlichen Eingaben darstellt. Das Ergebnis ist eine verbesserte Zusammenarbeit zwischen der Entwicklung, dem Chiphersteller und der Produktionsstätte.

IV. Die SentriX Security Deployment Platform

Phase II: Sicherer Import von OEM-Sicherheitsdaten
Sobald das Sicherheitsdefinitionspaket vom OEM bei der für die Provisionierung der OEM-ICs verantwortlichen Drittpartei eingegangen ist, wird es in das spezifische SentriX-System (oder die System-Gruppe) geladen, an das (bzw. die) das IP-Paket in Phase I gebunden ist. SentriX ist aus Sicherheitsgründen während der Fertigung in der Regel nicht direkt mit dem Internet verbunden und wird in einer getrennten oder nur zeitweise verbundenen Umgebung betrieben. Daher wird das OEM-Sicherheitsdefinitionspaket mit Hilfe physischer Speichermedien in den Host-Computer des SentriX-Systems geladen. Sobald dies geschehen ist, verwendet ein Administrator des SentriX-Systems die Sicherheitsverwaltungssoftware auf dem Host-Computer, um einen "Job" zur Sicherheitsprovisionierung zu erstellen. Ein Job besteht aus einer Reihe von Anweisungen für die Programmierung von Halbleitern, der unter anderem die Anzahl der zu programmierenden Bausteine, Sicherheitsinformationen, verschiedene Kennungen sowie die Firmware und andere zu programmierende Daten enthalten kann. Im Rahmen dieses Joberstellungsprozesses wird das gesicherte OEM-IP-Paket vom physischen Speichermedium auf das HSM kopiert, das fest in das SentriX-System integriert ist.

Bei der Erstellung von Provisionierungsaufträgen wird überprüft, ob das Sicherheitsdefinitionspaket auf dem jeweiligen SentriX-System verwendet werden darf. Schlägt diese Sicherheitsprüfung fehl, schlägt auch der Joberstellungsprozess fehl. Außerdem wird das Sicherheitsdefinitionspaket während der Joberstellung im SentriX HSM verarbeitet, um sicherzustellen, dass es authentisch ist und während des Transports vom OEM zum SentriX-System nicht verändert wurde. Das Paket wird dann innerhalb des HSM entschlüsselt, um bei der Provisionierung verwendet zu werden. Bei der Joberstellung werden dieses OEM-Paket und ein IC-spezifischer Provisionierungsalgorithmus (eine IC-spezifische Firmware, die auf den SentriX-Programmiersystemen ausgeführt wird) mit dem Provisionierungsjob verknüpft.

Phase III: Sicherheitsprovisionierung der ICs
In dieser Phase findet die eigentliche Provisionierung der Programmierbausteine statt. Dieser Prozess wird eingeleitet, indem der Bediener eines SentriX-Systems einen (in Phase II erstellten) Provisionierungsjobs auswählt und einen Programmierzyklus startet. Damit beginnt das Einlegen der ICs in die Sockel der SentriX Programmer sowie das Laden und Programmieren des Algorithmus auf die Bausteine. Während des Provisionierungsprozesses können neue Sicherheitsnachweise im SentriX HSM, im IC oder in beiden erstellt und verarbeitet werden. Die Sicherheitsprovisionierung kann auch als Übertragung von Sicherheitsnachweisen vom SentriX HSM zum Baustein und umgekehrt erfolgen. Der Prozess der Erzeugung, Verarbeitung und Verschiebung von sicherheitsrelevanten Berechtigungsnachweisen im Provisionierungsprozess wird durch den Algorithmus auf dem SentriX-Host-Computer koordiniert.

Am Ende dieser Phase sind alle ICs mit Sicherheitsvorkehrungen versehen und werden von den Programmern für die anschließende Verwendung im nachgelagerten Fertigungsprozess auf ein Ausgabemedium übergeben.

Phase IV: Reporting der Provisionierung
Während sich die ICs im SentriX-System auf dem Programmiersockel zur Provisionierung befinden, wird ein Rückverfolgbarkeitsdatensatz für jeden durchgeführten Job und für jeden bereitgestellten IC erstellt. Die Art der Informationen, die für jeden Auftrag und jeden IC erfasst werden, zeigt Tabelle 1:

RÜCKVERFOLGBARKEIT JOB PROVISIONIERUNG	RÜCKVERFOLGBARKEIT DER EINZELNEN ICs
Job ID	Halbleiter-Hersteller-ID
Job Name	Produkt-ID
Dauer der Provisionierung	Baustein-UUID
Anzahl der Bausteine	Identitätszertifikat des Halbleiterherstellers
Anzahl der Bausteine, die nicht provisioniert werden konnten	Identitätszertifikat der Programmierbausteine
IC-Algorithmus-ID und Versionsnummer	ID des Programmiersystems
ID des Programmiersystems	ID des Programmers
ID des Programmers	ID des Programmiersockels
Datum, Uhrzeit und Ort der Programmierung	Provisionierungsstatus des IC: Erfolgreich / Fehlgeschlagen
	Dauer der Provisionierung
	Lese- und Schreibdauer
	Zeitstempel der Programmierung

TABELLE 1: Übersicht der Rückverfolgbarkeitsinformationen nach Typ

Am Ende des Sicherheitsprovisionierungsjobs werden die Datensätze zur Rückverfolgbarkeit für jeden Job und jeden IC an den OEM geschickt.

Wie SentriX die Lieferkette absichert

Folgende sechs Sicherheitsrisiken werden durch das SentriX-System gelöst:

1) Der Ausschluss von gefälschten ICs
2) Die Veränderung oder der Verlust von OEM-Firmware/ Software
3) Gefährdung von OEM-Zugangsdaten (Geheimnissen)
4) Überproduktion von Bausteinen
5) Rückverfolgbarkeit
6) Erleichterung nachgelagerter Services

Ausschluss von gefälschten ICs
Die Programmierprozesse von SentriX sind so konzipiert, dass die ICs zunächst auf den Herkunftsnachweis des Halbleiterherstellers überprüft werden, bevor die Bausteine mit zusätzlichen Sicherheitsnachweisen versehen werden. Wenn sich ein bestimmter IC nicht als ein original hergestellter Baustein authentifizieren lässt, wird er als Abfall aus dem Herstellungsprozess entfernt.

Während des IC-Authentifizierungs-prozesses werden eine Halbleiter-hersteller-ID, eine Produkt-ID und eine Seriennummer aus dem IC ausgelesen und mit einer vom Halbleiterhersteller bereitgestellten Liste verglichen. Wenn die vom IC gelesenen Daten nicht in der bereitgestellten Liste enthalten sind, wird der Baustein als Fälschung gekennzeichnet.

Secure-Element-ICs bieten ein sicheres, kryptografisch gestütztes Authentifizierungsverfahren, das auf einem IC-Identitätszertifikat des Halbleiterherstellers basiert, das während des IC-Herstellungsprozesses vorpro-grammiert wurde. Für solche Program-mierbausteine, umfasst der Authenti-fizierungsprozess die kryptografische Authentifizierung des Zertifikats des Secure-Element-ICs (durch Authentifizierung eines öffentlichen Schlüssels über ein Challenge/Response-Verfahren) sowie die Validierung einer PKI (Public Key Infrastructure) Identität. Wenn die Authentifizierung fehlschlägt, wird der Baustein als Fälschung markiert und ebenfalls aus dem Herstellungs-prozess ausgeschlossen.

V. Wie SentriX die Lieferkette absichert

Es ist anzumerken, dass die Praxis des Hinzufügens von kryptografischen Identitäten und IC-Identitäts-zertifikaten bei den Halbleiterherstellern nicht einheitlich ist. Dies kann an folgenden Gründen liegen:

- Kosten und Zeitaufwand für den IC-Herstellungs-prozess
- Zusätzliche Kosten im Zusammenhang mit der Verwaltung und Unterstützung von IC-Schlüsseln und Sicherheitszertifikaten der Hersteller (erforderlich für die Authentifizierung der ICs während ihres Lebenszyklus)
- Erhöhtes Haftungsrisiko für einen Hersteller, wenn IC-Identitäten von OEMs stellvertretend für die OEM-Bausteinidentität verwendet werden (z. B. wenn Fehlfunktionen implizit mit der IC-Identität in Verbindung gebracht werden)

Schutz von OEM-Firmware und -Software während der Fertigung

Das Tool SentriX Product Creator ermöglicht es OEMs, ihre Firmware/Software während des Transports von der OEM-Entwicklungsabteilung zum Ort der Provisionierung zu schützen. Das Tool ermöglicht dies, indem es das OEM-IP-Paket verschlüsselt und elektronisch signiert. Außerdem bindet das Tool das OEM-IP-Paket an ein bestimmtes HSM des SentriX Produktionssystems, so dass es nur von diesem SentriX-System entschlüsselt und anschließend für die sichere Programmierung verwendet werden kann. Durch diesen Prozess wird sichergestellt, dass die OEM-IP auf dem gesamten Weg vom OEM zur SentriX-Programmierstätte gesichert ist. Ein Man-in-the-Middle-Angriff eines Dritten (während des Transports oder zum Zeitpunkt der Programmierung) ist unwirksam.

Schutz von OEM-Geheimnissen

Das SentriX Product Creator Tool und das SentriX HSM schützen zudem Sicherheitsnachweise, krypto-grafische Schlüssel und Zertifikate. Alle diese Geheimnisse werden kryptografisch so verschlüsselt, dass sie nur vom ausgewähltem SentriX HSM gelesen werden können.

Vermeidung von Überproduktionen

Die SentriX-Sicherheitsplattform gibt OEMs die vollständige Kontrolle darüber, wie viele ICs in der Programmierstätte eines Dritten provisioniert werden sollen. Die OEMs legen die zulässige Produktionszahl für ICs als Teil des OEM-IP-Pakets fest. Das OEM-IP-Paket wird verschlüsselt und an die Programmierstätte weitergegeben, wo es während der Joberstellung an einen Provisionierungsauftrag gebunden, anschließend sicher entschlüsselt und im HSM des SentriX-Systems gespeichert wird. Während des Provisionierungs-prozesses wird die Anzahl der zu programmierenden Bausteine mitgezählt. Wird die autorisierte Menge erreicht, können keine weiteren ICs provisioniert werden.

Die Mengen-Verarbeitung erfolgt im SentriX HSM, wo kein Dritter Änderungen vornehmen kann, so dass die Sicherheit in Bezug auf die autorisierte Menge gewährleistet ist. Zusammenfassend lässt sich sagen, dass hier keine Man-in-the-Middle-Angriffe möglich sind und dass die Anzahl der zu programmierenden ICs in der Kontrolle des OEM bleibt.

Verbesserte Rückverfolgbarkeit in der Lieferkette

Die SentriX Security Deployment Platform erstellt für jeden Job Rückverfolgbarkeitsdatensätze. Für OEMs ist die Rückverfolgbarkeit in der Elektronikfertigung der Prozess der Aufzeichnung von Aktionen, die an einem OEM-Baustein von verschiedenen Beteiligten im Herstellungs-prozess durchgeführt werden.

Rückverfolgbarkeitsinformationen sind für OEMs nützlich, da sie alle, am Baustein vorgenommenen Änderungen verfolgen und die Effizienz eines bestimmten Herstellungsprozesses analysieren können (z. B. Betriebseffizienz). Rückverfolgbarkeitsinformationen können auch zur Analyse von Bausteinausfällen verwendet werden, insbesondere wenn die Fehlerursache während der Herstellung aufgetreten ist. Die Ermittlung der Grundursache eines Fehlers hilft auch bei der Identifizierung anderer Bausteine, bei denen derselbe Fehler auftreten könnte.

V. Wie SentriX die Lieferkette absichert

Durch Rückverfolgbarkeitsaufzeichnungen können OEMs feststellen und überprüfen, wie viele ICs tatsächlich von einem Dritten provisioniert wurden. Dies geschieht durch die Überprüfung der Anzahl der vom System provisionierten Bausteine. Die Rückverfolgbarkeits-datensätze können auch bestimmte OEM-Zertifikate enthalten, die während der sicheren Programmierung erstellt wurden und an den OEM zurückgemeldet werden müssen. Um die Authentizität und Vertraulichkeit der Rückverfolgbarkeitsdatensätze während des Transports vom Programmiersstandort zurück zum OEM-Standort zu gewährleisten, werden die Datensätze verschlüsselt und durch elektronische Signaturen geschützt.

Nachgelagerte Services

Einer der wichtigsten Mechanismen für OEMs, um nachgelagerte Dienste zu ermöglichen, besteht darin, eine eindeutige Identität für den Baustein zu schaffen. Eine wichtige und strategische Anforderung ist, dass die Bausteinidentität vollständig vom OEM verwaltet und kontrolliert wird (und unabhängig von den IC-Identitäten, die vom Halbleiterhersteller selbst eingebracht wurden). Hierfür gibt es zwei strategische Gründe:

1) Der OEM behält sich die Möglichkeit vor, den Baustein während des gesamten Lebenszyklus zu authentifizieren, und 2) der OEM behält die Kontrolle über künftige Einnahmequellen (und ist nicht von einem Halbleiterhersteller abhängig, der den Zugang zu einem Baustein gewährt oder authentifiziert).

Die am häufigsten verwendete Methode zur Festlegung einer zugeordneten OEM-Bausteinidentität besteht darin, während der Herstellung eindeutige Seriennummern in die ICs zu programmieren. Eine andere gängige Praxis ist die Programmierung einer eindeutigen Seriennummer und einer eindeutigen MAC-Adresse (Media Access Control). Nach der SMT-Bestückung und während der Funktionsprüfung wird die MAC-Adresse dann in die Netzwerkkarte (NIC) provisioniert. Diese Kombination wird dann von der Firmware und den auf dem Baustein laufenden Diensten (während des Betriebszustands) als Identität des Bausteins verwendet.

Das beschriebene Verfahren ist höchst unsicher, da Seriennummern und MAC-Adressen, wenn sie nicht auf dem Baustein schreibgeschützt sind, während der Herstellung oder im Betrieb verändert werden können. Darüber hinaus können ungeschützte Nummern von einem IC oder dem fertigen Endprodukt ausgelesen und auf andere Bausteine dupliziert werden.

Der Ansatz ein OEM-Produkt mit einem Sicherheits-IC (z. B. einem Sicherheitscontroller oder Sicherheits-Mikrocontroller) auszustatten und die Identität des Bausteins zusätzlich durch eine hardwarebasierte Root of Trust und Kryptographie-Prozesse abzusichern, gewährt mehr Schutz. Der Prozess der sicheren Programmierung in SentriX beginnt mit der Generierung eines eindeutigen asymmetrischen Schlüsselpaars für die Bausteinidentität auf dem Sicherheits-IC des Bausteins. Der durch diesen Prozess erzeugte private Baustein-Schlüssel wird in einem lesegeschützten Speicher auf dem Sicherheits-IC versteckt.

Der öffentliche Schlüssel der Baustein-Identität und die Chip-ID werden dann aus dem Sicherheits-IC ausgelesen und zur Erstellung eines OEM-Baustein-Identitäts-zertifikats verwendet. Das Baustein-Identitätszertifikat wird mit dem Schlüssel aus dem Zertifikat einer Zwischenzertifizierungsstelle (ICA) des OEM signiert (das ICA-Zertifikat wurde über das SentriX Product Creator Tool bereitgestellt). Der beschriebene Prozess der Erstellung von Baustein-Identitätszertifikaten findet im HSM des SentriX-Systems statt. Im letzten Schritt der Provisionierung des Bausteins wird das Baustein-Identitätszertifikat vom SentriX-System in den Sicherheits-IC übertragen, wo es sicher in einem schreibgeschützten Speicher abgelegt wird.

Wenn der provisionierte Sicherheits-IC in ein OEM-Produkt eingebaut wird, stellt das OEM-Bausteinidentitätszertifikat auf dem Sicherheits-IC die Identität des OEM-Produkts dar. Dieser Provisionierungs-prozess führt zu einer OEM- Produktidentität, die auf dem Baustein geschützt ist. Von hier kann sie nicht geändert oder auf einen anderen Baustein geklont werden.

V. Wie SentriX die Lieferkette absichert

Die Implementierung von OEM-Baustein-Identitäten in ICs verbessert die Sicherheit der nachgelagerten Lieferkette. Unter der Annahme, dass die Bausteinidentität vor der Montage des Bausteins in den Sicherheits-IC provisioniert wird, kann der Schritt der Funktionsprüfung und Verifizierung nach der Montage den Baustein anhand der OEM-Identität authentifizieren. Fehlerhafte Bausteine werden direkt aus der Lieferkette entfernt.

Cloud Onboarding

Viele der derzeit wichtigsten Anwendungen und Dienste sind Cloud-basiert und nutzen IoT-Bausteine als Teil ihrer Cloud-Anwendungen. Um in einer Cloud-Anwendung funktionieren zu können, müssen die Bausteine zunächst in die entsprechende IoT-Cloud eingebunden werden. Beim Cloud-Onboarding wird eine Bausteinidentität, die den Bausteinen während der Herstellung zugewiesen wird, bei der entsprechenden Cloud-Plattform registriert. Der erste Schritt in diesem Prozess besteht darin, die Cloud-Identität eines OEM in der Cloud-Plattform zu erstellen (z. B. im Identitätszugriffsmanagementsystem einer bestimmten Cloud). Der nächste Schritt besteht darin, die "Chain-of-Trust" des OEM, die zur sicheren Programmierung von Bausteinidentitätszertifikaten während der Herstellung verwendet wird, mit der Cloud-Identität des OEM zu verbinden. Der letzte Schritt besteht darin, die Bausteinzertifikate (die während der Herstellung in den Bausteinen provisioniert wurden) mit der entsprechenden "Identity-Chain-of-Trust" im Cloud-Konto des OEMs zu verbinden. Nun werden die Bausteine mit denselben Sicherheitsanmeldeinformationen in der Cloud angemeldet. Dadurch können alle OEM-Produkte (Cloud-Server, Gateways, Endgeräte), die zu einer Anwendung gehören, sicher miteinander kommunizieren.

SentriX bietet eine leistungsstarke One-Touch-Lösung für die Provisionierung und das Onboarding von Bausteinen in der Cloud, indem ein Cloud-Onboarding-Service als optionale Erweiterung des Provisionierungsprozesses während der Fertigung integriert wird. Der Provisionierungsprozess in der Cloud extrahiert die "Chain- of-Trust" und die Bausteinzertifikate, die als Ergebnis des Provisionierungsprozesses für die Bausteinidentität erstellt werden, und bindet die Bausteine dann, durch die Verwendung einer Cloud-Onboarding-API, in ein entsprechendes OEM-Konto in der Cloud ein.

Bausteinmanagement und Firmware-Updates

Das Bausteinmanagement umfasst Dienste, die auf einem Baustein ausgeführt werden, während sich dieser im Betriebszustand befindet. In diesem Zustand müssen Bausteine möglicherweise ständig verwaltet werden, um ihre Firmware zu aktualisieren, Sicherheitsnachweise oder -dienste hinzufügen oder zu löschen, den Zustand des Bausteins zu überwachen oder die Lebensdauer eines Bausteins zu beenden. Service-Provider bündeln diese Baustein-Dienste unter dem Oberbegriff "Device Management".

Die sichere Aktivierung und der Betrieb von Baustein-managementdiensten erfordert die Provisionierung von kryptografischen Schlüsseln und Sicherheitsnachweisen in die Bausteine. In der Regel wollen OEMs jeden Baustein eines bestimmten Typs mit einem Standardsatz von Diensten ausstatten und diese Dienste dann während des Betriebs aktivieren. SentriX bietet OEMs die Möglichkeit, die mit diesen Diensten verbundenen Sicherheitsberechtigungen während der Herstellung sicher zu provisionieren.

Es ist heute gängige Praxis für OEMs, die Firmware ihrer Bausteine zu verwalten und zu aktualisieren, sobald ein Baustein im Betrieb eingeschaltet wird. Der Grund dafür ist, dass die Herstellung eines Bausteins ein viel längerer Prozess ist, als das Zeitfenster eines OEMs, um Fehler zu beheben und neue Funktionen hinzuzufügen. Die OEMs sind nun auf die Flexibilität des Firmware-Update-Prozesses angewiesen, um Fehler zu beheben, neue Funktionen freizugeben und sicherzustellen, dass die Bausteine im Feld auf die neueste Softwareversion aktualisiert werden können.

Die Gefahr liegt darin, dass der Prozess der Firmware-Aktualisierung missbraucht werden könnte, um eine veränderte Kopie auf den Baustein aufzuspielen oder die vorhandene Firmware zu verändern, um Zugriff auf Daten und Sicherheitsinformationen zu erhalten. Für OEMs ist es äußerst wichtig, den Prozess der Firmware-Aktualisierung zu sichern. Die Sicherung des Firmware-Update-Prozesses erfordert die Provisionierung von Firmware, die den Austausch eines alten Firmware-Images durch eine neue Firmware verwaltet, sowie die Provisionierung von Sicherheitsschlüsseln, die zur Überprüfung der Authentizität des neuen Firmware-Images verwendet werden. SentriX verwaltet und führt einen solchen Provisionierungsprozess durch. Der auf der Pre-Programmierung basierende Ansatz ist nicht nur wesentlich sicherer als die Verwendung von ISP, sondern senkt durch die Kombination mehrerer Provisionierungsfunktionen in einer einzigen Provisionierungsmethodik die Gesamtkosten für die Sichherheitsprogrammierung.

VI. Zusammenfassung

SentriX wurde mit dem vorrangigen Ziel entwickelt, den IC-Provisionierungsprozess abzusichern und zu vereinfachen. SentriX verwendet softwaredefinierte Sicherheitsalgorithmen, bei denen der Einsatz von Sicherheitsmerkmalen nicht von OEM-spezifischen PCB-Designs abhängt; SentriX erfordert auch keine Installation von teurer Sicherheits-Hardware und -Software. Folglich wird SentriX als Dienstleistung ohne Vorabinvestitionen angeboten. Die SentriX Product Creator-Tools vereinfachen die Sicherheitsimplementierung mit intuitiven Kollaborationstools, die vorkonfigurierte Anwendungsfälle und kundenspezifische Sicherheitsimplementierungen unterstützen. Darüber hinaus nutzt SentriX Security Deployment die Sicherheitsprovisionierung über Pre-Programmierung, was die Kosten senkt und im Vergleich zur ISP-Programmierung mehr Sicherheit bietet. Die SentriX Security Deployment Plattform ist mit einer Reihe von technischen und betriebswirtschaftlichen Attributen ausgestattet, die OEMs dabei helfen, die wichtigsten Herausforderungen der IoT-Sicherheitsdefinition, der sicheren Fertigung und der Provisionierung von Zertifikaten in Programmierbausteine während der Fertigung zu meistern.

Quellenübersicht

1. https://www.creditcards.com/statistics/history-of-credit-cards/
2. https://iccwbo.org/news-publications/policies-reports/economic-impacts-counterfeiting-piracy-report-prepared-bascap-inta/
3. 2019: Industry Week sized the worldwide counterfeit semiconductor market at $75B.
4. 2019: Havocscope reported more than $169B of counterfeit electronics in circulation.
5. https://www.justice.gov/usao-cdca/pr/florida-man-charged-federal-counterfeit-case-trafficking-bogus-automotive-devices
6. https://hackaday.com/2017/05/31/counterfeit-hardware-may-lead-to-malware-and-failure/
7. https://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market
8. Data Integrity & Safety Risks examples provided by members of World Semiconductor Council (of which the Semiconductor Industry Association in the U.S. is a member)

Über
Data I/O

Seit 1972 entwickelt Data I/O innovative Lösungen für das Design und die Herstellung von elektronischen Produkten für die Bereiche Automotive, Internet of Things, Medizintechnik, Wireless, Unterhaltungselektronik, industrielle Steuerungen und anderer elektronischer Produkte. Heute nutzen unsere Kunden die Security- und Programmierlösungen von Data I/O, um zuverlässig, sicher und kosteneffizient neue innovative Produkte zum Leben zu erwecken. Diese Lösungen werden von einem globalen Netzwerk von Data I/O Support- und Servicefachleuten unterstützt, um den Erfolg unserer Kunden zu gewährleisten.

Data I/O GmbH

Am Haag 10
82166 Gräfelfing
+49 (0) 89 8585850
info@data-io.de