ANALOG DEVICES

Die Entschlüsselung industrieller Cybersecurity

BESUCHEN SIE: ANALOG.COM/CYBERSECURITY

DAS VERTRAUENSWÜRDIGE SYSTEM DER MODERNEN DIGITALEN FABRIK

Die digitale Transformation hat den Wandel in der Industrie vorangetrieben. Die Digitalisierung produziert dabei immer mehr Daten, die eine Entscheidungsfindung in Echtzeit ermöglichen – dies erhöht die Automatisierung und verbessert die Prozesseffizienz. Um diese Daten optimal nutzen zu können, sind digitale Unternehmen zunehmend vernetzt, was die Konvergenz der Netzwerke von OT (Operational Technology) und Office IT (Information Technology) erfordert. Dieser rasante technologische Fortschritt hat die Leistungsfähigkeit des intelligenten Edge freigesetzt und ermöglicht nahtlose Verbindungen zwischen Edge und Cloud. Mit der fortschreitenden Einführung der digitalen Verbindungstechnologie, die eine höhere Bandbreite und einen besseren Zugang zu Erkenntnissen allen Bereichen der Prozessanlage und der Fabrikhalle ermöglicht, muss ein zunehmendes Maß an Schwachstellen in Bezug auf Cybersecurity berücksichtigt werden. Da neuere industrielle Ethernet-Technologieinfrastrukturen zu einer IP-Adressierbarkeit an allen Knotenpunkten und der Entfernung von Gateway-Geräten führt, ist der Schutz von Geräten und Systemen vor Cyberangriffen von entscheidender Bedeutung. Die potenziellen Kosten dieser Angriffe sind nicht nur extrem hoch, sie können bei sicherheitsrelevanten Steuerungssystemen sogar Menschenleben gefährden.

Unternehmen müssen heute überlegen, wie sie in einer Welt operieren können, in der industrielle automatisierte Kontrollsysteme (IACS) gegen Cyberangriffe resistent sein müssen. Steuerungs-Systeme verwalten Befehle, regulieren das Verhalten anderer Geräte und stellen bei einem Angriff eine Gefahr für die gesamte Fertigungsinfrastruktur dar. Cyberangriffe können invasiv oder nichtinvasiv sein. Bei einem invasiven Angriff öffnet eine cyberkriminelle Partei das Gehäuse des Geräts, um dessen Speicherinhalt zu manipulieren, die Firmware zu ersetzen oder die Leiterbahnen zu untersuchen. Nichtinvasive Angriffe werden in der Regel aus der Ferne über Kommunikations-Ports durchgeführt und zielen auf Sicherheitslücken in der Firmware des Geräts ab.

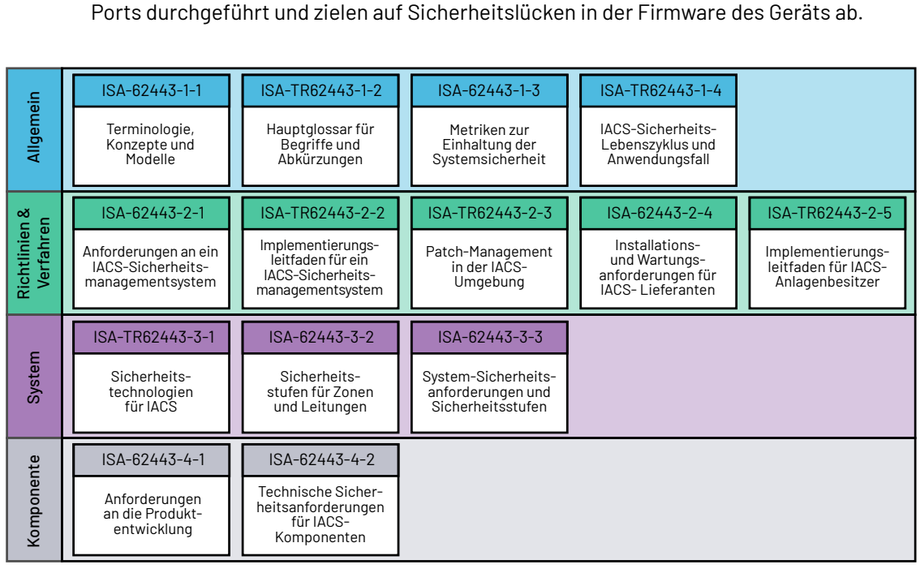
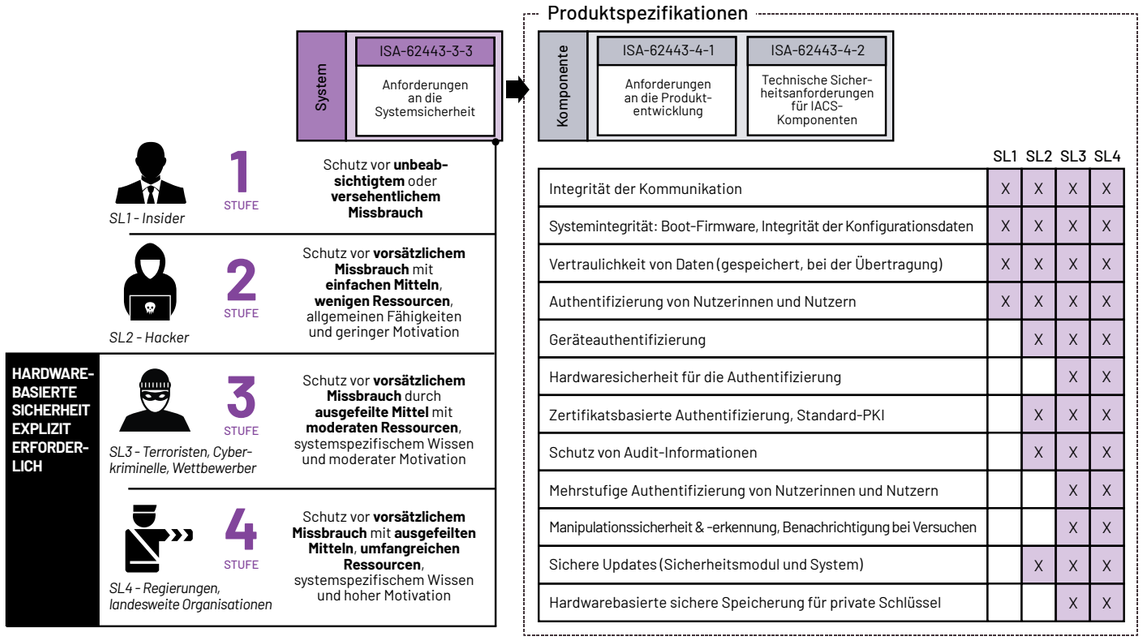


Abbildung 1: *IEC 62443 Reihe von Sicherheits-standards*

Der EU-Rechtsakt zur Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen (Cyber Resilience Act, CRA) ist ein neues EU-Gesetz, das die Cybersicherheit von in der EU verkauften digitalen Produkten regelt und globale Auswirkungen auf Hersteller, Entwickler und Anbieter von „Produkten mit digitalen Elementen" (PDEs) hat, die für den EU-Markt bestimmt sind, einschließlich der Einführung einer obligatorischen CE-Kennzeichnung für Produkte bis 2027. Dies hat zu einer Priorisierung von Sicherheitsaspekten geführt, die bereits in der Anfangsphase in neue Produktentwicklungszyklen integriert werden – andernfalls besteht die Gefahr, dass neue Produkte, die heute entwickelt werden, nach 2027 nicht mehr den erforderlichen Standards für den Verkauf auf dem EU-Markt entsprechen.

SIE MÖCHTEN MEHR ERFAHREN? Lesen Sie *"The IEC 62443 Series of Standards: How to Defend Against Infrastructure Cyberattacks"*, Fachartikel von Analog Devices

Um die Übernahme der CRA-Bestimmungen zu erleichtern, hat die Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity, ENISA) die EU-CRA-Anforderungen dem Standard IEC 62443-4 zugeordnet. Die Normenreihe IEC 62443 befasst sich mit der Cybersecurity für Betriebstechnologie in Automatisierungs- und Steuerungsprozessen. Dieser führende Standard bietet eine umfassende Sicherheitsebene, um Angriffe zu verhindern und ihre Auswirkungen zu mindern. Er ist in vier Ebenen und Kategorien unterteilt: „Allgemein" beinhaltet Themen, die für die gesamte Serie gelten; „Richtlinien und Verfahren" konzentriert sich auf Methoden und Prozesse im Zusammenhang mit der IACS-Sicherheit; „System" beschreibt die Anforderungen auf Systemebene und „Komponente" enthält detaillierte Anforderungen für IACS-Produkte.



	SL1	SL2	SL3	SL4
Integrität der Kommunikation	X	X	X	X
Systemintegrität: Boot-Firmware, Integrität der Konfigurationsdaten	X	X	X	X
Vertraulichkeit von Daten (gespeichert, bei der Übertragung)	X	X	X	X
Authentifizierung von Nutzerinnen und Nutzern	X	X	X	X
Geräteauthentifizierung		X	X	X
Hardwaresicherheit für die Authentifizierung			X	X
Zertifikatsbasierte Authentifizierung, Standard-PKI		X	X	X
Schutz von Audit-Informationen		X	X	X
Mehrstufige Authentifizierung von Nutzerinnen und Nutzern			X	X
Manipulationssicherheit & -erkennung, Benachrichtigung bei Versuchen			X	X
Sichere Updates (Sicherheitsmodul und System)		X	X	X
Hardwarebasierte sichere Speicherung für private Schlüssel			X	X

Abbildung 2: *IEC 62443 Anforderungen an Komponenten, die den gewünschten System-Sicherheits-stufen zugeordnet sind*

Um eine sichere Komponente zu entwerfen, ist es wichtig, zunächst durch eine Risikobewertung zu entscheiden, welche Sicherheitsstufe ein Gerät benötigt. Das Ergebnis der Bewertung wird klären, welcher Angriffsstufe ein Gerät standhalten muss: Stufe 1: „Insiderangriffe" sind in der Regel unbeabsichtigte oder versehentliche Sicherheitsverletzungen durch Missbrauch; Stufe 2: „Hacker" sind vorsätzliche Versuche, begrenzte Ressourcen zu schädigen; Stufe 3: „Cyberkriminelle" und Stufe 4 „Regierungen" beabsichtigen, Schaden anzurichten und verfügen über ausgefeilte Ressourcen, um Systeme anzugreifen.

Die Kombination aus ISA-62443-3-3 „System Security Requirements and Security Levels" und den Spezifikationen auf Komponentenebene (ISA-62443-4-1, ISA-62443-4-2) gibt vor, wie sichere Komponenten gestaltet werden müssen, die Cyberangriffen standhalten können. Auf der Grundlage der gewünschten Sicherheitsstufen müssen spezifische Anforderungen im Rahmen des Designs berücksichtigt werden. Alle Stufen erfordern Vertraulichkeit für Daten, die als sensibel eingestuft werden. Für die Sicherheitsstufen SL2-SL4 ist eine Geräteauthentifizierung erforderlich, während für jedes Gerät, das für den Betrieb auf SL3-SL4 ausgelegt ist, ein sicherer Hardwarespeicher für private Schlüssel vorgeschrieben ist. Der Lebenszyklus der sicheren Produktentwicklung von ADI ist nach IEC-62441-4-1:2018 zertifiziert.

SICHERHEITSLÜCKEN IN DER INDUSTRIE VERSTEHEN

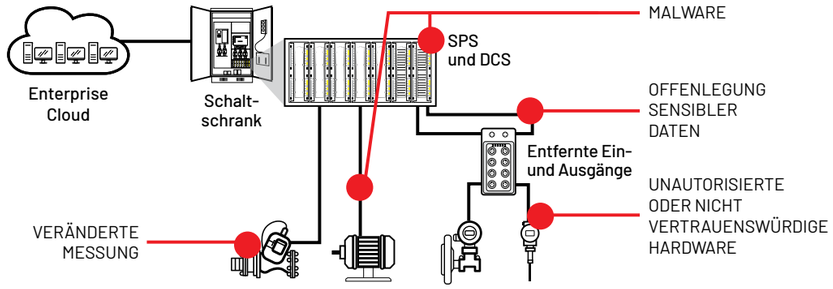


Abbildung 3: *Häufige Sicherheitslücken in industriellen Anwendungen*

In einer industriellen Umgebung gibt es eine Reihe von Lücken, die gesichert werden müssen, um die Integrität der Betriebsinfrastruktur zu gewährleisten. Betrachten wir vier häufige Schwachstellen, die alle mit schlüsselfertigen sicheren ICs geschützt werden können. Durch wesentliche Mechanismen wie die sichere Schlüsselspeicherung werden die Entwicklerinnen und Entwickler von IACS-Komponenten entlastet und es müssen keine Ressourcen in die Erarbeitung komplexer Sicherheitsprimitive investiert werden. Das Hinzufügen eines sicheren IC zu einem unsicheren System erhöht die Systemsicherheit, ohne dass eine architektonische Neugestaltung erforderlich ist. Ein solches Gerät muss spezialisiert sein und starke Kryptografiefunktionen enthalten, aber dennoch eine hohe Flexibilität aufweisen, um eine Vielzahl von Sicherheitsfunktionen auf Systemebene zu unterstützen. Spezifische Produktempfehlungen finden Sie in den Auswahltabellen.

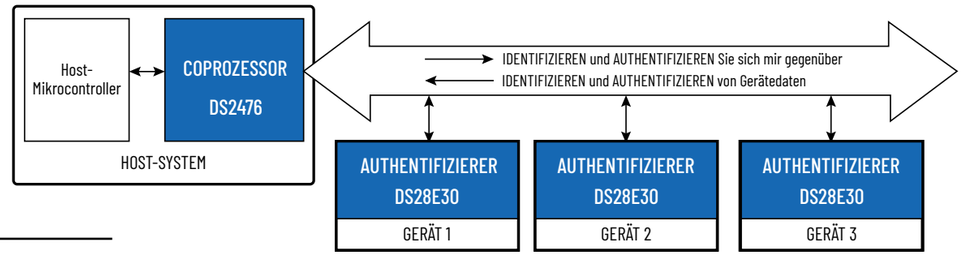


Abbildung 4: *Wie sichere Authentifikatoren und Coprozessoren die Kryptografie vereinfachen können*

UNERLAUBTE ODER NICHT VERTRAUENSWÜRDIGE HARDWARE

Vertrauen zwischen Geräten kann durch eine Challenge-Response-Authentifizierung hergestellt werden, die im Falle einer symmetrischen Authentifizierung auf einem gemeinsamen geheimen Schlüssel oder bei einer asymmetrischen Authentifizierung auf einem privaten/öffentlichen Schlüsselpaar beruht. Während der öffentliche Schlüssel so konzipiert ist, dass er öffentlich bekannt ist, stellen sowohl der geheime als auch der private Schlüssel ein Sicherheitsrisiko dar – wenn sie gestohlen werden, ist die Sicherheit des gesamten Netzwerks gefährdet.

Obwohl der öffentliche Schlüssel nicht geheim gehalten werden muss, muss man sicher sein können, dass der öffentliche Schlüssel echt ist. Der öffentliche Schlüssel und die Geräte-ID eines Geräts können von einer externen Zertifizierungsstelle (Certificate Authority, CA) zertifiziert werden, die ein digitales Zertifikat ausstellt. Während des Schlüsselauthentifizierungsprozesses kann der öffentliche Schlüssel der CA verwendet werden, um die Echtheit des bereitgestellten öffentlichen Geräteschlüssels zu überprüfen.

Die Challenge-Response-Authentifizierung ist auf die Fähigkeit angewiesen, einen echten zufälligen Bitstrom zu erzeugen, der als Nonce bezeichnet wird. Die Verwendung einer starken, zufällig generierten Nonce bei jedem Austausch schützt vor der Möglichkeit eines „Replay-Angriffs“. Sichere Authentifikatoren können als schlüsselfertige Authentifizierungslösungen verwendet werden, um eine Challenge-Response-Authentifizierung durchzuführen.

OFFENLEGUNG SENSIBLER DATEN

Der Schutz von Daten, die sich auf einem Gerät befinden oder bei der Kommunikation mit anderen Systemen im Netzwerk übertragen werden, beruht auf Verschlüsselung. Durch den Einsatz bewährter Verschlüsselungsmethoden wie dem Advanced Encryption Standard (AES) kann die Offenlegung sensibler Daten vermieden werden.

In Situationen, in denen Angriffe auf Geräteebene stattfinden, bei denen die Daten als „gespeichert“ betrachtet werden, gewährleistet eine sichere Speicherlösung, dass selbst bei einem Zugriff auf den Speicher alle Daten mit Methoden verschlüsselt werden, die die zufälligen Eigenschaften des einzelnen Geräts bei der Herstellung nutzen, um eine physisch nicht klonbare Funktion (Physically Unclonable Function, PUF) zu schaffen. In PUF-basierten sicheren ChipDNA®-Authentifikatoren von Analog Devices wird jeder Schlüssel als präzises analoges Merkmal des IC generiert und niemals im Speicher abgelegt, wodurch er immun gegen alle bekannten invasiven Angriffswerkzeuge und -methoden ist.

Bei der Datenübertragung stellt die Verschlüsselung der Nachrichtendaten sicher, dass keine sensiblen Informationen an Personen weitergegeben werden, die das Netzwerk abhören. Das Transport Layer Security (TLS) Protocol ist das am häufigsten verwendete Protokoll zum Schutz von Daten während der Übertragung und gewährleistet die Authentizität, Integrität und Vertraulichkeit der Kommunikation.

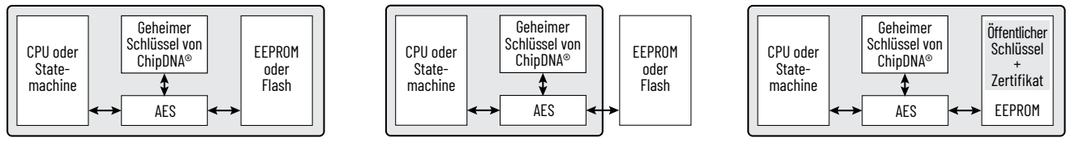


Abbildung 5: *Sicherheits-konfigurationen von ChipDNA® PUF*

MALWARE

Jedes Gerät, das mit einem unsicheren Netzwerk wie dem Internet verbunden ist, kann anfällig für Malware-Angriffe sein. Geräte, die Updates von Herstellern benötigen, müssen überprüfen können, ob das Update autorisiert und unverändert ist. Digitale Signaturen gewährleisten, dass nur verifizierte Firmware akzeptiert wird. Geräte mit Secure-Boot-Funktionalität stellen die Authentifizierung der Firmware eines Geräts beim Einschalten sicher. Wenn eine modifizierte Firmware auf dem Gerät installiert wurde, verweigert das System den Start, da die Firmware nicht mehr kryptografisch mit dem übereinstimmt, was der Hersteller ursprünglich auf dem Gerät implementiert hat, und die digitale Signatur ungültig ist.

VERÄNDERTE MESSUNGEN

Datenmanipulation oder veränderte Messungen von Edge-Geräten können zu einer verzerrten Wahrnehmung des Zustands eines Systems führen. Da immer mehr Systeme automatisiert werden, ist es von entscheidender Bedeutung, dass datengestützte Entscheidungen auf der Grundlage vertrauenswürdiger Messungen getroffen werden. Wenn ein böswilliger Akteur versucht, den Betrieb von Edge-Geräten zu beeinflussen oder Statusmeldungen zu manipulieren, verhindert die Überprüfung von Befehlen durch Signaturen, dass veränderte Messungen den Betrieb beeinträchtigen.

WICHTIGE ERKENNTNISSE

Damit ein System sicher ist, müssen Geräte in der Lage sein, mithilfe von Authentifizierung vertrauenswürdige Verbindungen herzustellen. Geräte müssen die Vertraulichkeit von Informationen durch Ver- und Entschlüsselung gewährleisten und dazu fähig sein, die Integrität von Befehlen zu überprüfen. So können sie potenzielle Angriffspunkte minimieren, die Hacker ausnutzen könnten, um die Kontrolle über industrielle Prozesse zu erlangen. Schlüsselfertige sichere ICs von Analog Devices bieten diese Funktionen und erhöhen die Systemsicherheit, ohne dass eine Neukonstruktion der IACS-Architektur erforderlich ist.

DIGITALE ZERTIFIKATE UND BEREITSTELLUNG

Eine von der absendenden Person mit einer digitalen Signatur versehene Nachricht kann als Nachweis dafür verwendet werden, dass die Nachricht von dieser Person gesendet wurde und unverändert ist. Eine digitale Signatur allein kann jedoch nicht die Identität des Absenders oder der Absenderin nachweisen. Der Identitätsnachweis wird durch ein digitales Zertifikat erbracht. Dieses digitale Dokument enthält Informationen über den öffentlichen Schlüssel und die ID, die zur Überprüfung der Eigentümerschaft des Schlüssels verwendet werden können. ADI kann die Zertifikate und Schlüssel im Auftrag von Kundinnen und Kunden als Service programmieren. Durch die Nutzung digitaler Zertifikate und sicherer Bereitstellungsverfahren können Industrieunternehmen ihre Cybersicherheits-Infrastruktur erheblich verbessern und die Integrität, Vertraulichkeit und Authentizität ihrer kritischen Systeme und Daten sicherstellen.

Digitale Zertifizierung

Digitales Dokument zur Überprüfung des Schlüsselbesitzes

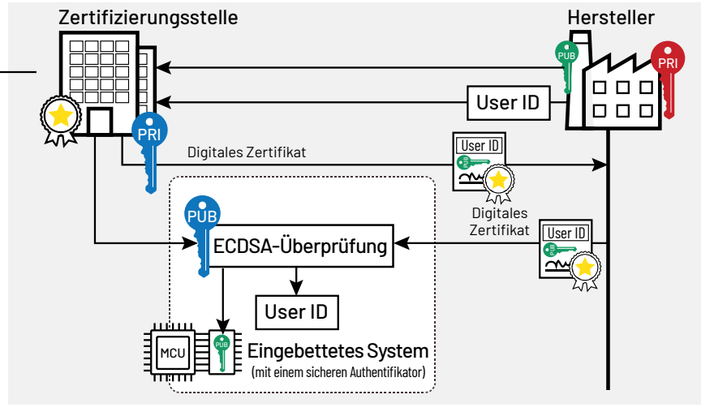


Abbildung 6:
Verwendung einer Zertifizierungsstelle zur Generierung eines digitalen Zertifikats

FIRMWARE UPDATE

Kritische Firmware Updates können mithilfe signierter Nachrichten auf Geräten im Feld bereitgestellt werden, wodurch sichergestellt wird, dass die Firmware sowohl authentisch als auch unverändert ist.

Signierte Nachrichten

Gewährleistung der Authentizität und Integrität von Informationen

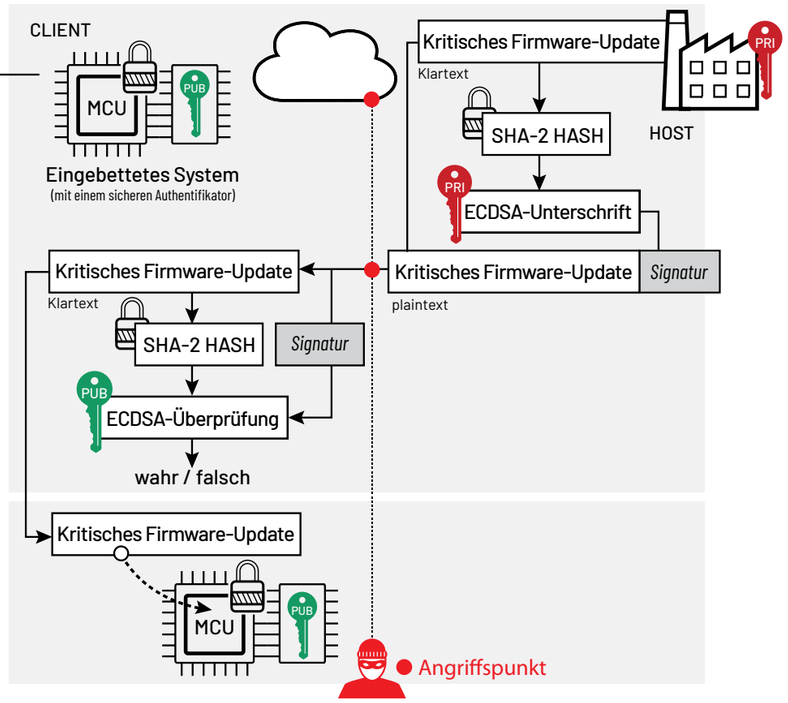


Abbildung 7:
Firmware-Update-Prozess

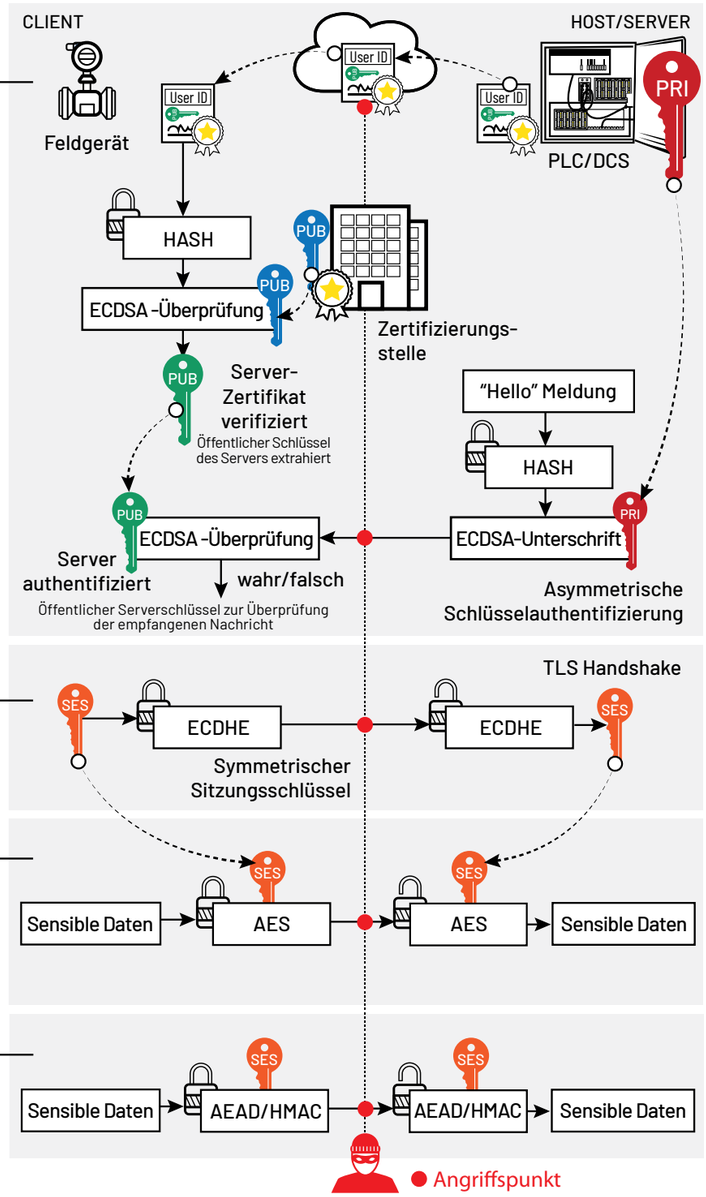
HARDWARE-AUTHENTIFIZIERUNG UND SICHERE KOMMUNIKATION

Ein Hardware-Authentifizierungsprozess beginnt mit dem Austausch eines Schlüsselpaars zwischen einem Host (SPS) und einem Client (Feldinstrument). Nachfolgend ist ein zertifizierungsbasierter Authentifizierungsprozess dargestellt, der in zwei Phasen abläuft: Zunächst überprüft der Client das Host-/Server-Zertifikat mithilfe des öffentlichen Schlüssels der Zertifizierungsstelle, sodass der öffentliche Host-Schlüssel als vertrauenswürdig eingestuft wird. Danach wird der öffentliche Schlüssel verwendet, um die Signatur einer Nonce (in diesem Fall die zuvor ausgetauschten „Hello"-Daten) zu überprüfen, die vom Host berechnet wurde. Im TLS-Protokoll wird nach der Authentifizierung des Servers mithilfe des symmetrischen ECDH- oder ECDHE-Algorithmus ein gemeinsamer Kommunikationsschlüssel (auch als Sitzungsschlüssel bezeichnet) erstellt. Dieser Sitzungsschlüssel wird anschließend zur Verschlüsselung von Nutzdaten verwendet, sodass Server und Client vertrauliche Informationen austauschen können. TLS gewährleistet die Integrität entweder durch authentifizierte Verschlüsselung (z.B. AES GCM oder AES CCM) oder durch Anhängen eines HMAC (Hash-based Message Authentication Code). Nach Beendigung der Kommunikation werden die Sitzungsschlüssel verworfen.

Abbildung 8:
Hardware-Authentifizierungs- und Kommunikationsprozess

TLS-Server-Authentifizierung

Server-Zertifikats-überprüfung und -authentifizierung



Häufig verwendete Begriffe aus dem Bereich Cybersicherheit finden Sie in diesem Glossar.

ADI Assure™ ist eine Produktreihe, die einen widerstandsfähigen Schutz vor Sicherheitsbedrohungen bietet, um einen dauerhaften Sicherheitsstatus zu gewährleisten. Mit unseren vertrauenswürdigen Edge-Lösungen liegt die Sicherheitsgrenze näher am Ursprung der Daten, was zu einem höheren Vertrauen in ihre Authentizität und Glaubwürdigkeit führt. Wir haben uns dazu verpflichtet, unsere Kundinnen und Kunden dabei zu unterstützen, die branchenüblichen Cybersicherheits-Standards und behördlichen Anforderungen schnell zu erfüllen und ihre Abwehrmaßnahmen gegen sich entwickelnde Sicherheitsbedrohungen während der gesamten Lebensdauer ihrer Produkte zu stärken. Unsere Spitzentechnologien wie **ChipDNA® PUF**, manipulationssichere Schlüsselspeicherung und fortschrittliche Kryptoalgorithmen verbessern Sicherheitsarchitekturen und bieten einen erhöhten Widerstand gegen invasive und nichtinvasive Angriffe. Unser umfangreiches Portfolio an skalierbaren und flexiblen Sicherheitslösungen mit hardwaregestützter Vertrauensbasis und Softwarediensten bietet nachhaltigen Schutz und einfache Integration, schützt Systeme, beschleunigt die Cybersicherheits-Zertifizierung und ermöglicht langfristige Resilienz.

GERÄTEAUSWAHL FÜR HARDWARE-AUTHENTIFIZIERUNG, FÄLSCHUNGSSCHUTZ, KALIBRIERUNG UND NUTZUNGSKONTROLLE

AUTHENTIFIZIERER	Geheimer Schlüssel SHA-2	Geheimer Schlüssel SHA-3	Öffentlicher Schlüssel ECDSA	Geheimer Schlüssel SHA-2 & öffentlicher Schlüssel ECDSA
I2C	DS28C22	DS28C50* DS28C16	DS28C36* DS28C39*	DS28C40
1-Wire	DS28E(L)25 DS28E(L)22 DS28E(L)15	DS28E50* DS28E16	DS28E38* DS28E39* DS28E30	DS28E36 DS28E40
NFC	MAX66240 MAX66242	MAX66250		
COPROZESSOREN				
I2C	DS2465	DS2477*		DS2476 DS2478
NFC	MAX66300	MAX66301		

** ChipDNA® PUF Technologie*

SICHERE ICs FÜR SECURE BOOT, SICHERE FIRMWARE UPDATES, SICHERE KOMMUNIKATION UND TLS-UNTERSTÜTZUNG

SECURE ELEMENT		ECDSA	ECDH	AES 128/256	Zertifikate	TLS Softwarestack
SPI	DS28S60*	X	X	X	Individuell	
SPI	MAXQ1065*	X	X	X	x.509	OpenSSL, mbedTLS, WolfSSL

** ChipDNA® PUF Technologie*

ANALOG DEVICES

BESUCHEN SIE: ANALOG.COM/CYBERSECURITY