ANALOG DEVICES

La Cybersecurity Industriale, Demistificata

VISITA ANALOG.COM/CYBERSECURITY

L' EDGE AFFIDABILE DELLA MODERNA FABBRICA DIGITALE

La trasformazione digitale è stata un catalizzatore del cambiamento nell'industria, con la digitalizzazione che produce sempre più dati per consentire il processo decisionale in tempo reale, per aumentare il livello di automazione e migliorare l'efficienza dei processi. Per massimizzare l'uso di questi dati, le imprese digitali sono diventate sempre più connesse, il che richiede la convergenza delle reti OT (Operational Technology) e IT (Information Technology) aziendali. Questo rapido progresso tecnologico ha sbloccato la potenza dell'intelligent edge, rendendo possibili le operazioni di connessione dall'edge al cloud senza soluzione di continuità. Con la crescente adozione della tecnica di connettività digitale, che porta una maggiore larghezza di banda e l'accesso alle informazioni da tutti i punti dell'impianto di processo e della fabbrica, è necessario considerare un livello più elevato di vulnerabilità della cybersecurity. Con l'indirizzabilità IP di tutti i nodi e l'eliminazione dei dispositivi gateway, introdotta dalle nuove infrastrutture tecnologiche dell'Ethernet industriale, la protezione dei dispositivi e dei sistemi dagli attacchi informatici è di fondamentale importanza. Non solo i costi potenziali di questi attacchi sono estremamente elevati, ma possono anche mettere in pericolo delle vite nel caso di sistemi di controllo legati alla sicurezza.

Oggi le aziende devono pensare a come operare in un mondo in cui i sistemi di controllo automatizzati industriali (Industrial Automated Control Systems, IACS) siano resilienti ai cyberattacchi. I sistemi di controllo gestiscono i comandi, regolano il comportamento di altri dispositivi e, se attaccati, rappresentano una minaccia per l'intera infrastruttura produttiva. Gli attacchi informatici possono essere invasivi o non invasivi. In un attacco invasivo, un criminale informatico apre l'involucro del dispositivo per manipolarne il contenuto della memoria, sostituire il firmware o sondare le piste dei circuiti stampati. Gli attacchi non invasivi sono di solito eseguiti in remoto attraverso le porte di comunicazione e mirano alle falle di sicurezza nel firmware del dispositivo.

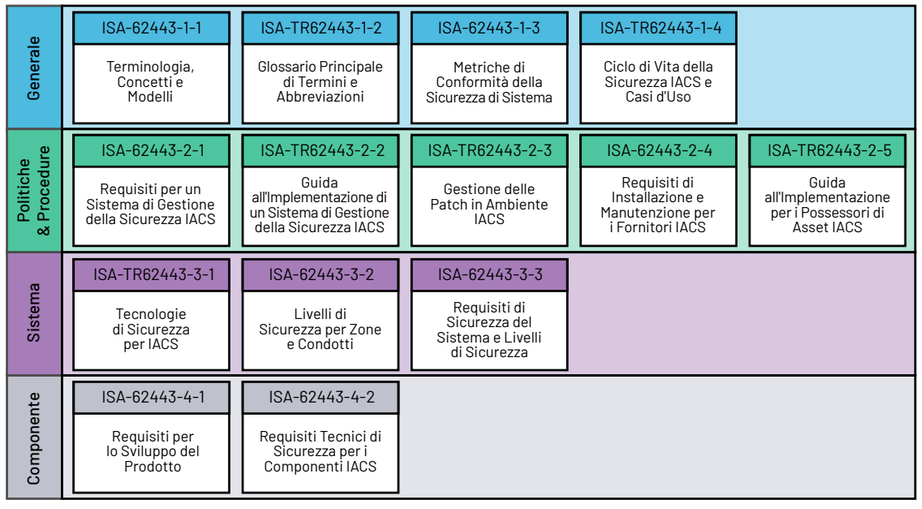
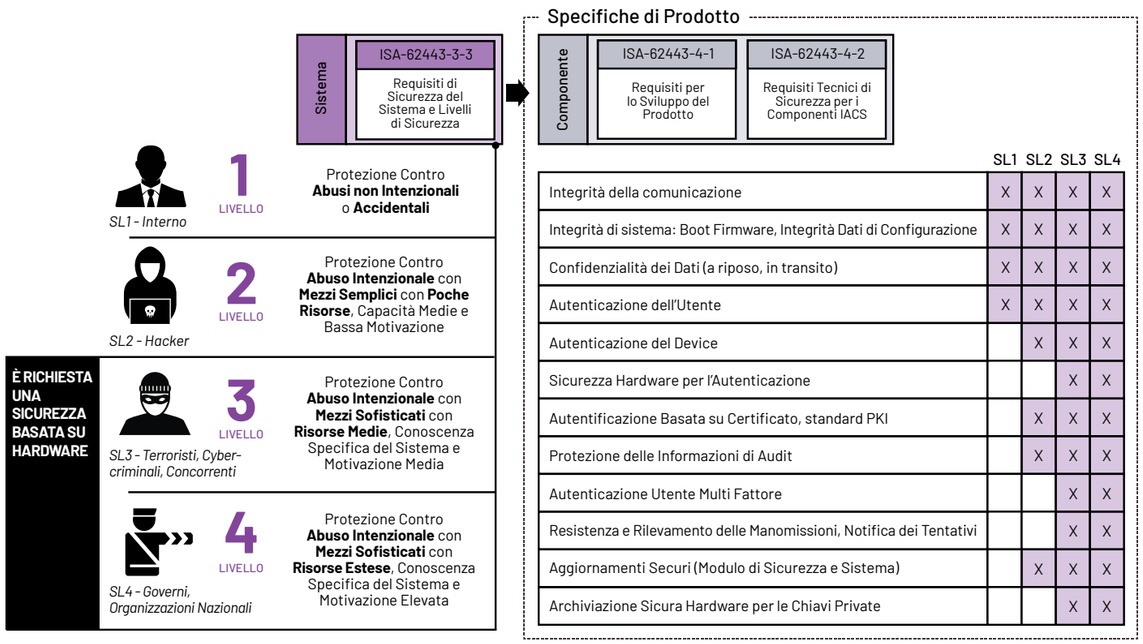


Figura 1:
Serie di Standard di Sicurezza IEC 62443

Il Cyber Resilience Act (CRA) dell'UE è una nuova legge europea che disciplina la sicurezza informatica dei prodotti digitali venduti nell'UE con un impatto globale su produttori, sviluppatori e venditori di "prodotti con elementi digitali" (Products with Digital Elements, PDE) destinati al mercato dell'UE, compresa l'introduzione di marchi CE obbligatori per questi prodotti entro il 2027. Ciò ha fatto sì che le considerazioni sulla sicurezza siano state inserite in via prioritaria nei cicli di sviluppo dei nuovi prodotti poiché, in caso contrario, quelli in fase di sviluppo oggi non saranno conformi agli standard richiesti per essere venduti sul mercato dell'UE dopo il 2027.

VUOI SAPERNE DI PIÙ? Leggi l'Articolo Tecnico di Analog Devices *"The IEC 62443 Series of Standards: How to Defend Against Infrastructure Cyberattacks"*

Per facilitare l'adozione delle disposizioni del CRA, l'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) ha mappato i requisiti del CRA dell'UE nello standard IEC 62443-4. La serie di standard IEC 62443 è progettata per affrontare la cybersecurity della tecnologia operativa nei processi di automazione e controllo. Questo standard di riferimento offre un ampio livello di sicurezza per prevenire gli attacchi e mitigarne gli effetti. È organizzata in quattro livelli e categorie: argomenti "generali" comuni all'intera serie; "Politiche e procedure" si concentra su metodi e processi associati alla sicurezza IACS; "Sistema" delinea i requisiti a livello di sistema e "Componente" fornisce requisiti dettagliati per i prodotti IACS.



	SL1	SL2	SL3	SL4
Integrità della comunicazione	X	X	X	X
Integrità di sistema: Boot Firmware, Integrità Dati di Configurazione	X	X	X	X
Confidenzialità dei Dati (a riposo, in transito)	X	X	X	X
Autenticazione dell'Utente	X	X	X	X
Autenticazione del Device		X	X	X
Sicurezza Hardware per l'Autenticazione			X	X
Autentificazione Basata su Certificato, standard PKI		X	X	X
Protezione delle Informazioni di Audit		X	X	X
Autenticazione Utente Multi Fattore			X	X
Resistenza e Rilevamento delle Manomissioni, Notifica dei Tentativi			X	X
Aggiornamenti Securi (Modulo di Sicurezza e Sistema)		X	X	X
Archiviazione Sicura Hardware per le Chiavi Private			X	X

Figura 2:
Requisiti dei Componenti IEC 62443 mappati ai Livelli di Sicurezza del Sistema desiderati

Per progettare un componente sicuro, è importante decidere innanzitutto il livello di sicurezza richiesto da un dispositivo, eseguendo una valutazione del rischio. Il risultato della valutazione chiarirà se un dispositivo deve resistere ad attacchi di Livello 1 "Interno", che sono tipicamente violazioni della sicurezza non intenzionali o accidentali. Livello 2 "Hacker" che cercano intenzionalmente di fare danni con risorse limitate; fino al livello 3 "Cyber-criminali" e al livello 4 "Governi" che intendono fare danni e dispongono di risorse sofisticate per attaccare i sistemi.

La combinazione di ISA-62443-3-3 "System Security Requirement and Security Levels" e delle specifiche a livello di componente (ISA-62443-4-1, ISA-62443-4-2) prescrive come progettare componenti sicuri in grado di resistere ai cyberattacchi. In base ai livelli di sicurezza desiderati, è necessario soddisfare requisiti specifici nell'ambito della progettazione. Tutti i livelli richiedono la riservatezza dei dati identificati come sensibili. L'autenticazione del dispositivo è richiesta per i livelli di sicurezza SL2-SL4, mentre l'archiviazione hardware sicura delle chiavi private è specificata per qualsiasi dispositivo che voglia raggiungere un funzionamento a livello SL3-SL4. Il ciclo di vita dello sviluppo di prodotti sicuri di ADI è certificato secondo la norma IEC-62441-4-1:2018.

COMPRENDERE LE VULNERABILITÀDELLA SICUREZZA INDUSTRIALE

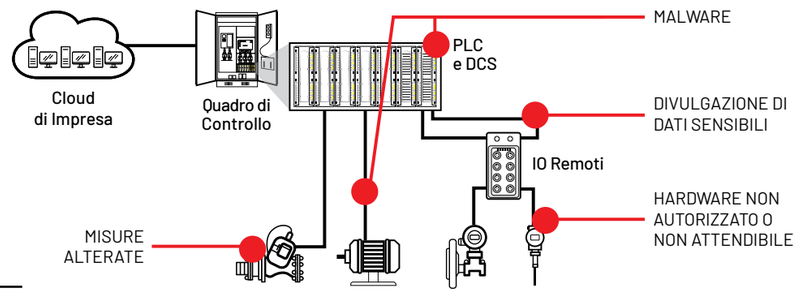


Figura 3:
Vulnerabilità di Sicurezza Comuni nelle Applicazioni Industriali

In un contesto industriale, esistono diverse aree di vulnerabilità che devono essere protette per garantire l'integrità dell'infrastruttura operativa. Prendiamo in considerazione quattro aree comuni, che possono essere protette con circuiti integrati sicuri "chiavi in mano", incorporando meccanismi essenziali come la memorizzazione sicura delle chiavi e sollevando gli sviluppatori di componenti IACS dall'investire risorse nella progettazione di complesse primitive di sicurezza. L'aggiunta di un IC sicuro a un sistema non sicuro aumenta il livello di sicurezza del sistema senza costringere a riprogettare l'architettura. Un dispositivo di questo tipo deve essere specializzato, incorporando funzioni di crittografia forti, ma sufficientemente flessibile da supportare una varietà di funzioni di sicurezza a livello di sistema. Per raccomandazioni specifiche sui prodotti, consultare le Tabelle di Selezione.

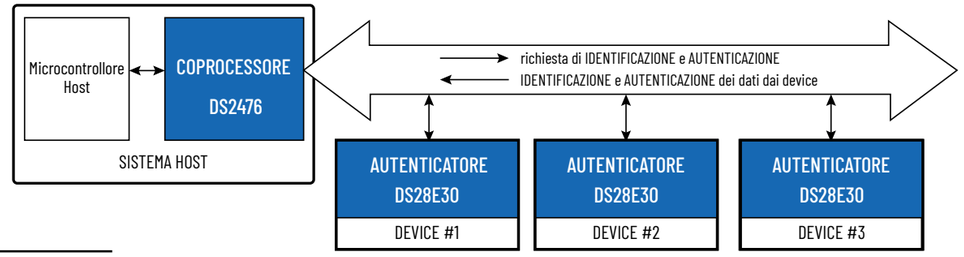


Figura 4:
Come gli Autenticatori e i Coprocessori Sicuri possono Semplificare la Crittografia

HARDWARE NON AUTORIZZATO O NON ATTENDIBILE

Per stabilire la fiducia tra i dispositivi si può utilizzare l'autenticazione challenge-response, che si basa su una chiave segreta condivisa nel caso dell'autenticazione simmetrica o su una coppia di chiavi private/pubbliche per l'autenticazione asimmetrica. Mentre la chiave pubblica è progettata per essere conosciuta pubblicamente, sia la chiave segreta che quella privata rappresentano un rischio per la sicurezza: se vengono rubate, la sicurezza dell'intera rete è a rischio.

Anche se la chiave pubblica non deve essere tenuta segreta, è importante sapere che sia autentica. La chiave pubblica e l'ID del dispositivo possono essere certificati da un'autorità di certificazione (Certificate Authority, CA) di terze parti, che rilascia un certificato digitale. Durante il processo di autenticazione delle chiavi, la chiave pubblica della CA può essere utilizzata per verificare che la chiave pubblica fornita dal dispositivo sia autentica.

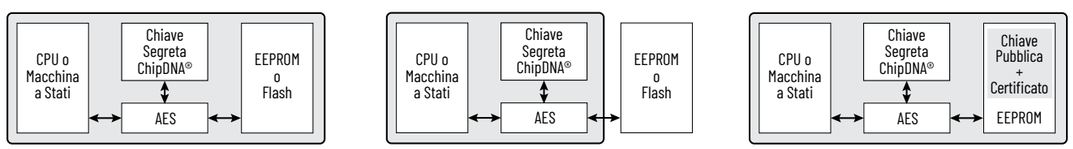
L'autenticazione challenge-response si basa sulla capacità di generare un flusso di bit casuale vero e proprio, denominato nonce. L'uso di un nonce forte generato casualmente in ogni scambio protegge dalla possibilità di un "attacco replay". Gli autenticatori sicuri possono essere utilizzati come soluzioni di autenticazione chiavi in mano in grado di eseguire l'autenticazione challenge-response.

DIVULGAZIONE DI DATI SENSIBILI

La protezione dei dati a riposo all'interno di un dispositivo o in transito durante la comunicazione con altri sistemi in rete si basa sulla crittografia. Utilizzando metodi di crittografia collaudati, come lo standard di crittografia avanzato (Advanced Encryption Standard, AES), è possibile evitare la divulgazione di dati sensibili.

Nelle situazioni in cui gli attacchi avvengono a livello di dispositivo, dove i dati sono considerati a riposo, l'archiviazione sicura della memoria garantisce che, anche se si accede alla memoria, tutti i dati siano crittografati con metodi che utilizzano le caratteristiche casuali del singolo dispositivo al momento della produzione per creare una funzione fisicamente non clonabile ("Physically Unclonable Function, PUF). Negli autenticatori sicuri ChipDNA® basati su PUF di Analog Devices, ogni chiave è generata come una precisa caratteristica analogica del circuito integrato e non viene mai memorizzata, rendendola immune a tutti gli strumenti e le capacità di attacco invasivo conosciuti.

Quando i dati sono in transito, la crittografia dei messaggi garantisce che nessuna informazione sensibile venga rivelata a chi sta spiando la rete. Il protocollo Transport Layer Security (TLS) è il più utilizzato per proteggere i dati in transito, garantendo autenticità, integrità e riservatezza della comunicazione.



Crittografia della Memoria Interna *Crittografia della Memoria Esterna* *Generazione Chiave di Autenticazione*

Figura 5:
Configurazioni ChipDNA® con Sicurezza PUF

MALWARE

Qualsiasi dispositivo connesso a una rete non sicura, come Internet, può essere vulnerabile agli attacchi di malware. I dispositivi che richiedono aggiornamenti da parte dei produttori hanno bisogno di un mezzo per verificare che l'aggiornamento sia autorizzato e non modificato. Le firme digitali garantiscono che venga accettato solo il firmware verificato. I dispositivi dotati di funzionalità di boot sicuro garantiscono l'autenticazione del firmware del dispositivo all'accensione. Se nel dispositivo è stato introdotto un firmware modificato, il sistema si rifiuterà di avviarsi poiché il firmware non corrisponde più a quello originariamente implementato dal produttore sul dispositivo e la firma digitale non è valida.

MISURAZIONI ALTERATE

La manipolazione dei dati o l'alterazione delle misurazioni del dispositivo edge possono determinare una percezione distorta dello stato di salute di un sistema. Con l'automazione di un numero sempre maggiore di sistemi, la capacità di garantire che le decisioni basate sui dati vengano prese da misurazioni affidabili è fondamentale. Se un malintenzionato sta cercando di influenzare il funzionamento del dispositivo edge o di manomettere i messaggi di stato, la verifica dei comandi attraverso le firme elimina la possibilità che le misurazioni alterate influenzino le operazioni.

CONSIDERAZIONI FONDAMENTALI

Affinché un sistema sia sicuro, i dispositivi devono essere in grado di creare connessioni affidabili utilizzando l'autenticazione. I dispositivi devono garantire la riservatezza delle informazioni utilizzando la crittografia e la decrittografia ed essere in grado di verificare l'integrità dei comandi per ridurre al minimo i potenziali punti di attacco che un malintenzionato potrebbe sfruttare per ottenere il controllo dei processi industriali. Gli IC sicuri "chiavi in mano" di Analog Devices forniscono queste funzionalità, aumentando la sicurezza del sistema senza costringere a riprogettare l'architettura IACS.

CERTIFICATI DIGITALI E PROVISIONING

Un messaggio firmato da una firma digitale del mittente può essere utilizzato per dimostrare che il messaggio è stato inviato dal mittente ed è inalterato. Tuttavia, una firma digitale da sola non può provare l'identità del mittente. La prova dell'identità si ottiene utilizzando un certificato digitale. Questo documento digitale contiene informazioni sulla chiave pubblica e sull'ID che possono essere utilizzate per verificare la proprietà della chiave. Come servizio, i certificati e le chiavi possono essere programmati da ADI per conto del cliente. Sfruttando i certificati digitali e le pratiche di provisioning sicuro, le organizzazioni industriali possono migliorare significativamente la loro infrastruttura di cybersecurity, garantendo l'integrità, la riservatezza e l'autenticità dei loro sistemi e dati critici.

Certificazione Digitale

Documento di verifica della proprietà della chiave

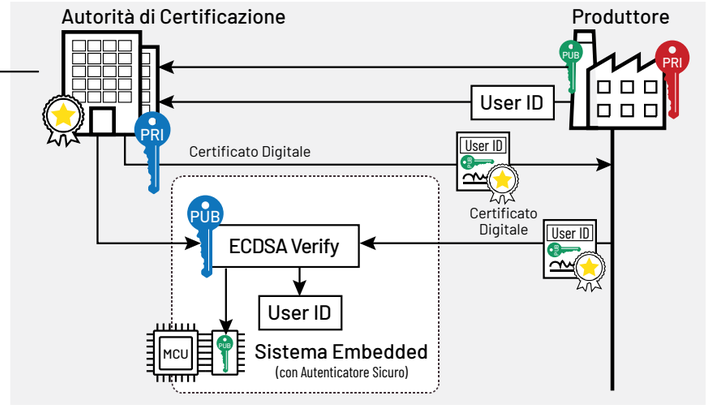


Figura 6: *Utilizzo di un'autorità di certificazione per generare un certificato digitale*

AGGIORNAMENTO DEL FIRMWARE

Gli aggiornamenti critici del firmware possono essere distribuiti ai dispositivi sul campo utilizzando messaggi firmati, garantendo che il firmware sia autentico e non modificato.

Messaggi Firmati

Garantiscono autenticità e integrità dell'informazione

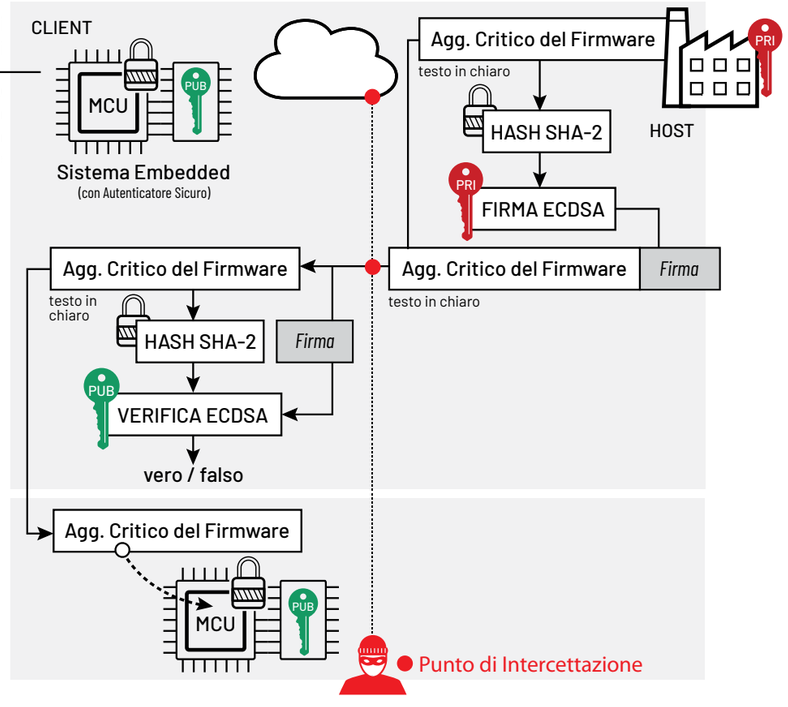


Figura 7: *Processo di aggiornamento del firmware*

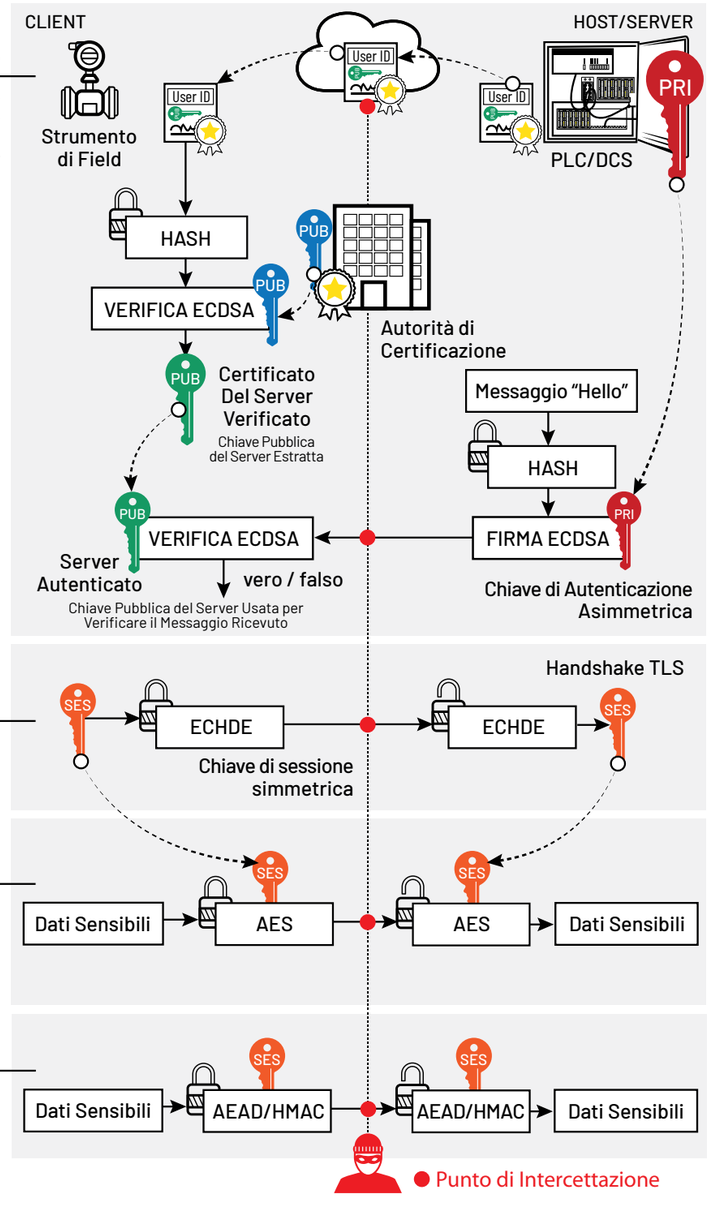
AUTENTICAZIONE HARDWARE E COMUNICAZIONE SICURA

Un processo di autenticazione hardware inizia con uno scambio di coppie di chiavi tra un host (PLC) e un client (strumento sul campo). Di seguito è illustrato un processo di autenticazione basato sulla certificazione che avviene in due fasi: innanzitutto il client verifica il certificato dell'host/server utilizzando la chiave pubblica della CA, in modo che la chiave pubblica dell'host sia attendibile. La chiave pubblica viene quindi utilizzata per verificare la firma di un nonce (in questo caso, i dati "Hello" scambiati in precedenza) calcolato dall'host. Nel protocollo TLS, una volta che il server è stato autenticato, utilizzando l'algoritmo simmetrico ECDH o ECDHE, viene creata una chiave di comunicazione condivisa (nota anche come chiave di sessione). Questa chiave di sessione viene poi utilizzata per crittografare i dati di payload, in modo che il server e il client possano scambiarsi informazioni riservate. TLS garantisce l'integrità mediante crittografia autenticata (ad esempio, AES GCM o AES CCM) o mediante l'aggiunta di un HMAC (Hash-based Message Authentication Code). Al termine della comunicazione, le chiavi di sessione vengono eliminate.

Figura 8: *Autenticazione dell'hardware e processo di comunicazione*

Autenticazione Server TLS

Verifica e Autenticazione Certificato del Server



Per I termini di cybersecurity di uso più comune, guarda questo glossario.

ADI Assure™ è una suite di prodotti che fornisce una solida protezione contro le minacce alla sicurezza per offrire uno stato di garanzia persistente. Con le nostre soluzioni trusted edge, il confine della sicurezza è più vicino all'origine dei dati, con conseguente maggiore fiducia nella loro autenticità e affidabilità. Ci impegniamo ad aiutare i nostri clienti a soddisfare rapidamente gli standard di cybersecurity del settore e i requisiti normativi e a rafforzare le loro difese contro le minacce alla sicurezza in continua evoluzione per tutta la durata dei loro prodotti. Le nostre tecnologie all'avanguardia, come il **ChipDNA® PUF**, l'archiviazione delle chiavi a prova di manomissione e gli algoritmi di crittografia avanzati, migliorano le architetture di sicurezza e offrono una maggiore resistenza contro gli attacchi invasivi e non invasivi. Il nostro ricco portafoglio di soluzioni di sicurezza scalabili e flessibili, con root of trust basati su hardware e servizi software, offre una protezione continua e una facile integrazione, salvaguardando i sistemi, accelerando il percorso di certificazione della cybersecurity e consentendo una resilienza a lungo termine.

SELEZIONE DEI DISPOSITIVI PER L'AUTENTICAZIONE HARDWARE, L'ANTICONTRAFFAZIONE, LA CALIBRAZIONE E IL CONTROLLO D'USO

AUTENTICATORE	Chiave Segreta SHA-2	Chiave Segreta SHA-3	Chiave Pubblica ECDSA	Chiave Segreta SHA-2 & Chiave Pubblica 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		
COPROCESSORE				
I2C	DS2465	DS2477*		DS2476 DS2478
NFC	MAX66300	MAX66301		

** ChipDNA® PUF Technologie*

IC SICURO PER IL BOOT SICURO, GLI AGGIORNAMENTI DEL FIRMWARE SICURI, LA COMUNICAZIONE SICURA E IL SUPPORTO TLS

SECURE ELEMENT		ECDSA	ECDH	AES 128/256	Certificati	Stack Software TLS
SPI	DS28S60*	X	X	X	Personalizzati	
SPI	MAXQ1065*	X	X	X	x.509	OpenSSL, mbedTLS, WolfSSL

** ChipDNA® PUF Technologie*

ANALOG DEVICES

VISITA ANALOG.COM/CYBERSECURITY