DOCUMENTO TECNICO

Maggio 2025

Sommario

Sebbene Wiegand rimanga un'interfaccia comune nelle applicazioni di controllo degli accessi, sta rapidamente diventando obsoleta a causa dei suoi difetti di sicurezza. Le organizzazioni che danno priorità alla sicurezza dovrebbero passare a OSDP per una migliore protezione contro gli attacchi. OSDP fornisce comunicazioni crittografate e supervisionate, rendendolo la scelta migliore per gli ambienti sicuri. L'aggiornamento del sistema di controllo degli accessi a OSDP garantisce una maggiore sicurezza oggi, ma anche una protezione futura contro le minacce in evoluzione.

Indice

1 Introduzione

Un aspetto critico dei sistemi di controllo degli accessi è rappresentato dai protocolli di comunicazione utilizzati.

Questo libro bianco analizza i due principali protocolli di comunicazione utilizzati tra il lettore e il door controller nei sistemi di controllo degli accessi. Analizziamo i loro vantaggi e svantaggi dal punto di vista della sicurezza e discutiamo su come iniziare la migrazione verso l'opzione più sicura.

2 Il controllo degli accessi nelle soluzioni per la sicurezza fisica

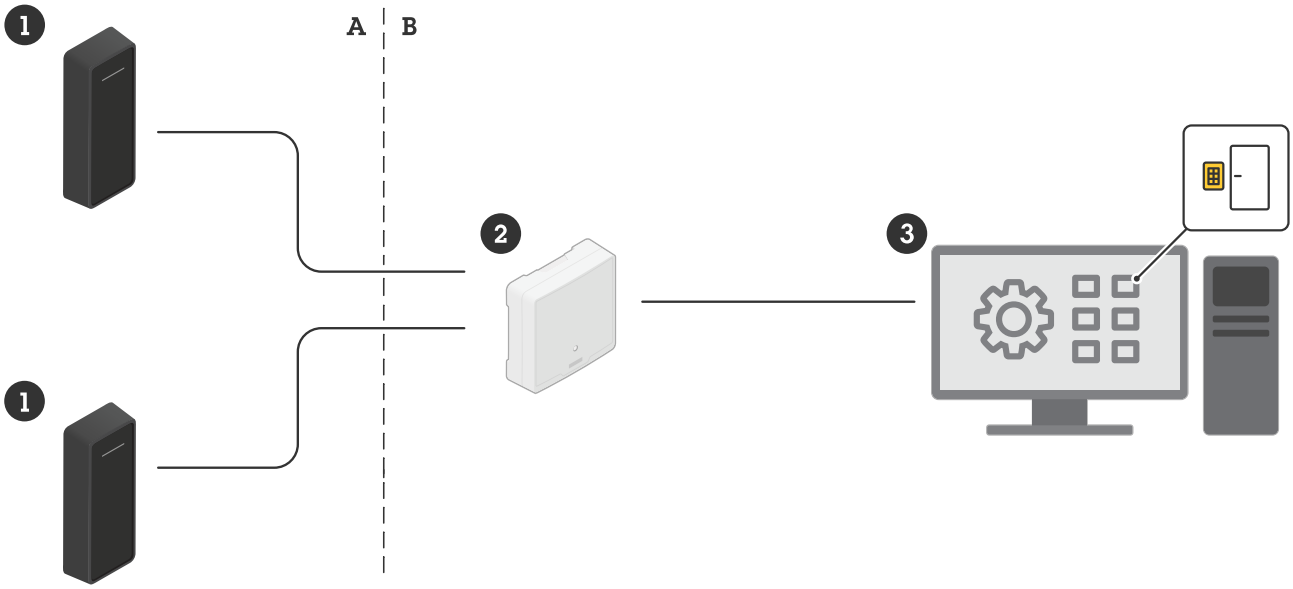
I sistemi di controllo degli accessi sono essenziali per proteggere edifici, beni e persone. Assicurano che solo le persone autorizzate possano accedere alle aree protette, riducendo i rischi per la sicurezza e migliorando l'efficienza operativa. Questi sistemi sono ampiamente utilizzati in diversi settori, tra cui uffici aziendali, centri dati, istituti sanitari e istituzioni pubbliche.

Un tipico sistema di controllo degli accessi è costituito da tre componenti chiave.

1 Lettori di controllo degli accessi: i dispositivi che leggono le credenziali degli utenti e trasmettono i dati delle credenziali a un controllore. Le tipiche credenziali dell'utente includono keycard, credenziali mobili, PIN e biometrici.

2 Door controller: le unità decisionali che elaborano i dati delle credenziali di processo e determinano se concedere o negare l'accesso.

3 Software di gestione: l'interfaccia in cui gli amministratori della sicurezza configurano i criteri di accesso, monitorano le attività e gestiscono gli utenti.



Nel sistema di controllo degli accessi, i lettori (1) sono installati all'esterno della porta (area non sicura, A) e comunicano con un door controller (2) installato all'interno (area sicura, B).

3 Protocolli di comunicazione lettore-controllore

Nel tempo, i protocolli di controllo degli accessi si sono evoluti, migliorando la sicurezza, la funzionalità e la facilità di integrazione. Analizziamo più da vicino i due protocolli principali.

3.1 Lo standard legacy: Wiegand

Wiegand trasmette i dati delle credenziali dal lettore al controllore utilizzando due linee dati. Il Wiegand esiste da decenni e rimane ampiamente utilizzato, soprattutto grazie alla sua semplicità e alla compatibilità con i sistemi legacy.

Lo svantaggio principale di Wiegand è la scarsa sicurezza. In particolare, manca la crittografia. I dati vengono trasmessi in chiaro, il che li rende vulnerabili agli attacchi di intercettazione e clonazione.

3.2 L'alternativa sicura: OSDP

Il protocollo OSDP (Open Supervised Device Protocol) è stato sviluppato dalla Security Industry Association (SIA) per migliorare l'interoperabilità tra i sistemi di controllo degli accessi e i prodotti di sicurezza. OSDP è stato approvato come standard internazionale dalla Commissione Elettrotecnica Internazionale e introduce la crittografia AES-128, la comunicazione bidirezionale e il monitoraggio dei dispositivi in tempo reale. Poiché OSDP consente al controllore di inviare comandi al lettore, permette anche di attivare funzioni come il controllo dei LED, l'attivazione del segnale acustico e il rilevamento delle manomissioni.

Una caratteristica fondamentale di OSDP è la modalità Secure Channel, che consente la trasmissione sicura dei dati grezzi delle credenziali tra i lettori di smart card e i controller. Ciò è particolarmente utile per i metodi di autenticazione avanzati, come la convalida biometrica e delle credenziali mobili.

3.2.1 OSDP Verificato

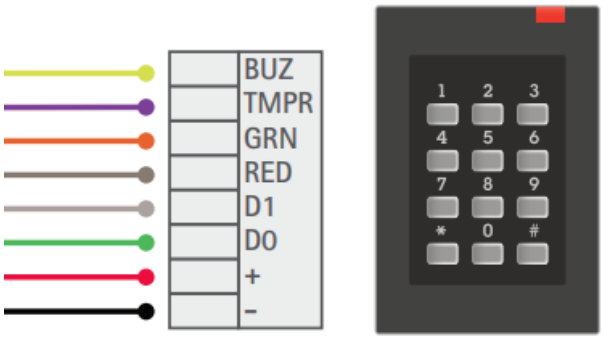
Il programma SIA OSDP Verificato è un'iniziativa di test completa che convalida la conformità di un dispositivo allo standard OSDP e ai relativi profili di prestazione. SIA mantiene un elenco di dispositivi verificati che sono stati testati e hanno dimostrato di soddisfare i criteri dello standard e dei profili indicati nell'elenco. I dispositivi dell'elenco possono utilizzare il marchio OSDP Verificato nei materiali di marketing.

Il marchio OSDP Verificato favorisce la fiducia di integratori, prescrittori e professionisti riguardo al fatto che i dispositivi OSDP funzionino come previsto per vari tipi di sistemi di controllo degli accessi.

4 Lettori Wiegand e OSDP a confronto

I lettori presentano punti di forza e di debolezza diversi a seconda del protocollo di comunicazione utilizzato.

4.1 Lettori Wiegand



Un lettore Wiegand e il relativo cablaggio, compresi i cavi supplementari per il segnale acustico, il rilevamento manomissione e i LED.

Vantaggi:

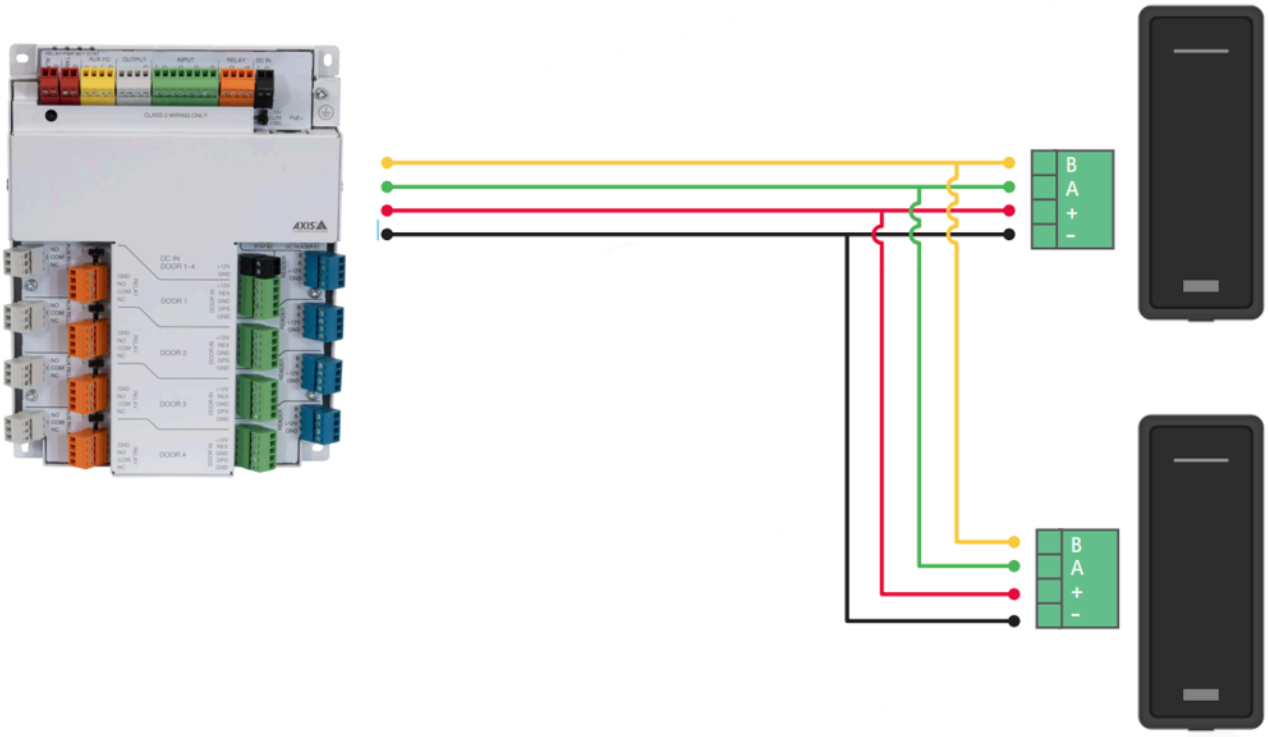
- Semplice e ampiamente compatibile con i sistemi più vecchi.

Svantaggi:

- Nessuna crittografia. I dati vengono trasmessi in chiaro e sono quindi facilmente intercettabili.

- Comunicazione a senso unico. Il controllore non può inviare comandi al lettore. Ciò significa che non c'è modo di rilevare se un lettore è stato manomesso o sostituito: il lettore non è supervisionato.
- Cablaggio complesso. Un lettore che utilizza i protocolli Wiegand necessita di cavi aggiuntivi per il segnale acustico del lettore, il rilevamento manomissione e i LED.
- La distanza massima del cavo è di 500 piedi (~150 metri).

4.2 Lettori OSDP



Lettori OSDP (a destra) e loro cablaggio con un door controller (a sinistra). Funzioni come il controllo dei LED, l'attivazione del segnale acustico e la supervisione del lettore non richiedono cavi aggiuntivi.

OSDP utilizza il cablaggio RS-485. Si tratta di uno standard di comunicazione seriale per la trasmissione di dati su lunghe distanze mediante cavi doppino. È comunemente utilizzato nei sistemi che richiedono una comunicazione affidabile e multipunto. Le caratteristiche principali includono la trasmissione a lunga distanza e la capacità di multi-drop.

Vantaggi:

- La comunicazione criptata impedisce l'intercettazione delle credenziali.
- OSDP consente al controllore di inviare comandi al lettore. Questo scambio di dati bidirezionale consente la supervisione e la configurazione a distanza. Inoltre, semplifica il cablaggio.
- Il cablaggio RS-485 consente una maggiore distanza massima del cavo.
- Il multi-drop consente a più lettori di condividere una connessione singola.

4.3 Usabilità

Tabella 4.1 *Confronto di usabilità con i lettori Wiegand e OSDP.*

	Wiegand	OSDP
Sicurezza	Nessuna crittografia, vulnerabile agli hackeraggi	Crittografia AES-128, rilevamento delle manomissioni
Comunicazione	Unidirezionale (dal lettore al controllore)	Bidirezionali
Lunghezza dei cavi	fino a 500 piedi (~150 metri)	fino a 4000 piedi (~1200 metri)
Multi-drop	No, un dispositivo un bus	Sì, più dispositivi supportati su un unico bus
Rilevamento manomissione	No, necessita di un cablaggio aggiuntivo	Sì
Supervisione	No, necessita di un cablaggio aggiuntivo	Sì
Integrità dei dati	Suscettibile agli attacchi di riproduzione delle credenziali	Trasmissione criptata e sicura
Complessità dell'installazione	Cablaggio complesso (D0/D1 e LED, manomissione, segnale acustico)	Facile (RS-485, A e B)
Scalabilità	Limitato da vincoli di cablaggio	Può collegare più lettori in una catena a margherita
Il miglior caso d'uso	Sistemi obsoleti, esigenze di sicurezza ridotte	Moderne installazioni sicure in settori come enti/autorità pubbliche o imprese

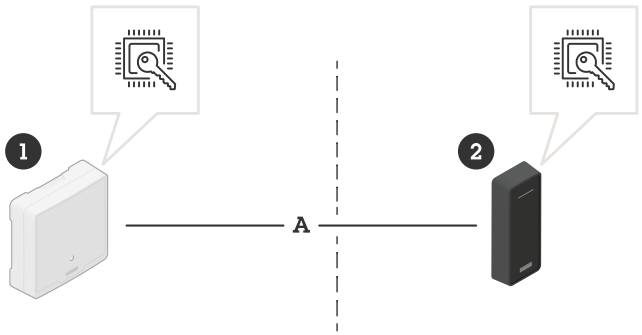
4.4 Sicurezza

La sicurezza deve costituire la priorità assoluta nella scelta di un protocollo di controllo degli accessi. La mancanza di crittografia di Wiegand lo rende suscettibile a diversi tipi di attacchi.

- Intercettazione delle credenziali. Gli aggressori possono intercettare le linee di dati e catturare le credenziali.
- Attacchi per riproduzione di credenziali. Una volta acquisita, la stessa credenziale può essere riprodotta per ottenere un accesso non autorizzato.
- Antimanomissione. Il sistema non è in grado di rilevare se un lettore è rimosso o sostituito.

Al contrario, OSDP attenua questi rischi crittografando i dati con AES-128 (Secure Channel) e fornendo la supervisione del dispositivo. In questo modo il controllore è in grado di rilevare se un lettore è stato manomesso e quindi di impedire l'accesso non autorizzato.

La crittografia rende sicuri i dati, ma la protezione delle chiavi rende sicura la crittografia. Senza una forte protezione delle chiavi, l'intero sistema può essere a rischio. Per questo motivo le chiavi di Secure Channel devono essere tenute al sicuro, in uno speciale chip hardware a entrambe le estremità: controller e lettore. Queste aree hardware sicure, come gli elementi sicuri, sono costruite per impedire agli aggressori di ottenere le chiavi anche se riescono ad accedere fisicamente al dispositivo.



Sicurezza end-to-end con l'archivio chiavi sicuro nel controllo accessi. La Master Key e la singola Secure Channel Base Key (SCBK) sono memorizzate in archivi chiavi sicuri nei dispositivi su ogni lato della porta.

1 *Door controller installato sul lato sicuro della porta*
2 *Lettore installato sul lato non sicuro della porta*
3 *A: Comunicazione tramite canale sicuro OSDP*

Tabella 4.2 *Confronto degli aspetti di sicurezza con i lettori Wiegand e OSDP.*

	Wiegand	OSDP
Crittografia	Nessuno, dati in chiaro	Crittografia AES-128
Intercettazione dei dati	Facilità di intercettazione credenziali	Crittografato per impedire l'intercettazione
Attacchi per riproduzione di credenziali	Le credenziali possono essere copiate/riprodotte	Impedito dalla crittografia
Rilevamento manomissione	No, non è in grado di rilevare lettori manomessi	Sì, il controllore monitora lo stato del lettore
Supervisione	No, il controllore non può verificare lo stato del lettore	Sì, supervisione in tempo reale
Compliance	Non consigliato per ambienti sicuri	Soddisfa i moderni standard di sicurezza

5 Raccomandazioni

Nell'attuale panorama della sicurezza, Wiegand non è più un'opzione praticabile per le nuove installazioni. Le organizzazioni dovrebbero passare ai lettori OSDP per una maggiore sicurezza, affidabilità e scalabilità futura.

- Valutare l'attuale infrastruttura di controllo degli accessi. Se attualmente si utilizza Wiegand, iniziare a pianificare una strategia di migrazione. Stabilire se l'opzione migliore è una migrazione OSDP completa o un convertitore da Wiegand a OSDP.
- Per le nuove installazioni, scegliere i lettori OSDP ogni volta che è possibile per garantire una comunicazione criptata e resistente alle manomissioni.
- Collaborare con i professionisti della sicurezza per implementare un sistema di controllo degli accessi sicuro e moderno che protegga dalle minacce.

6 Migrazione da Wiegand a OSDP

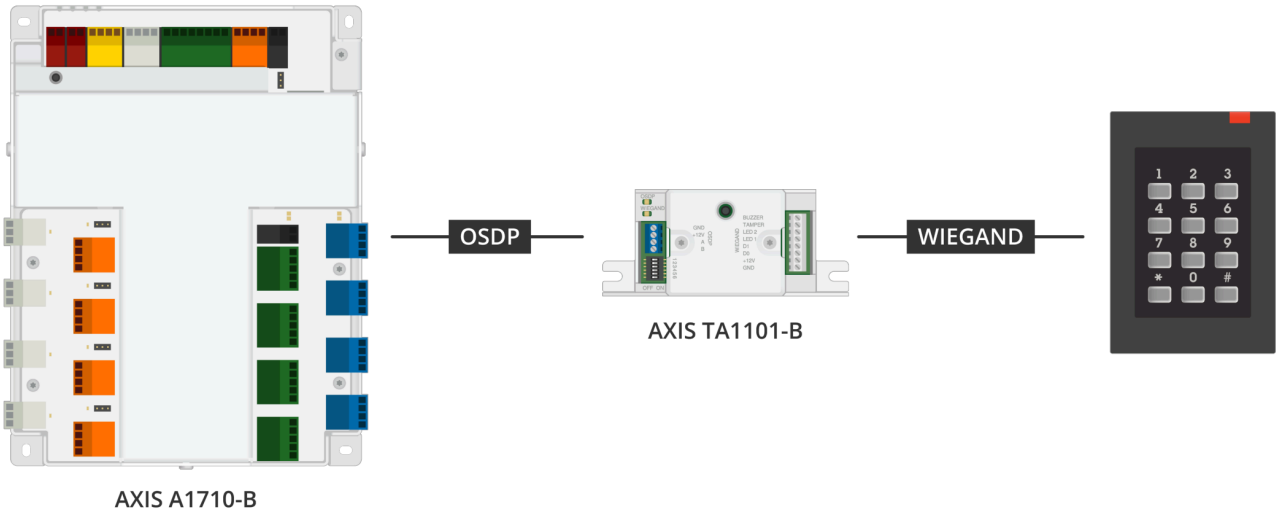
Molte organizzazioni si affidano ancora ai lettori Wiegand, ma vogliono migliorare la sicurezza senza sostituire l'intero sistema. Esistono due pratici percorsi di migrazione. Entrambe le opzioni migliorano la sicurezza, ma l'implementazione diretta dell'OSDP è il miglior investimento a lungo termine per le organizzazioni che vogliono essere a prova di futuro nei loro sistemi di controllo degli accessi.

6.1 Opzione 1: sostituzione dei lettori Wiegand con lettori OSDP

Si tratta della migliore soluzione a lungo termine. Sostituendo i lettori Wiegand obsoleti con modelli conformi a OSDP, le organizzazioni possono beneficiare della crittografia, della comunicazione bidirezionale e della supervisione del lettore. Tuttavia, è necessario assicurarsi che il pannello di controllo degli accessi supporti l'OSDP.

6.2 Opzione 2: utilizzare un convertitore Wiegand-OSDP

Per le organizzazioni che non sono in grado di sostituire immediatamente tutti i lettori, un convertitore Wiegand-OSDP rappresenta un'alternativa economicamente vantaggiosa. Questo dispositivo cripta i dati Wiegand prima di inviarli a un controller compatibile con OSDP, migliorando la sicurezza senza richiedere una revisione completa dell'hardware.



È possibile migliorare la sicurezza utilizzando un convertitore Wiegand-OSDP (al centro).

Informazioni su Axis Communications

Axis permette di creare un mondo più intelligente e sicuro migliorando la sicurezza, la protezione, l'efficienza operativa e la business intelligence. In qualità di azienda leader nelle tecnologie di rete, Axis offre videosorveglianza, controllo accessi, intercom e soluzioni audio, che supporta con applicazioni analitiche intelligenti e una formazione di alta qualità.

Axis ha oltre 5000 dipendenti in più di 50 paesi e collabora con partner tecnologici e integratori di sistemi in tutto il mondo per fornire soluzioni ai clienti. Fondata nel 1984, Axis è una società con sede a Lund, in Svezia.