

접근 제어에서 Wiegand 대신 OSDP를 선택해야 하는 이유

5월 2025

요약

Wiegand는 접근 제어 애플리케이션에서 일반적인 인터페이스로 남아 있지만 보안 결함으로 인해 빠르게 구식이 되고 있습니다. 보안을 우선시하는 조직은 공격에 대한 보호를 강화하기 위해 OSDP로 전환해야 합니다. OSDP는 암호화되는 감시형 통신을 제공하므로 보안 환경에 가장 적합한 선택입니다. 접근 제어 시스템을 OSDP로 업그레이드하면 현재 보안을 강화할 뿐만 아니라, 미래에도 진화하는 위협으로부터 조직을 보호할 수 있습니다.

목차

1	서론	4
2	물리적 보안 솔루션의 접근 제어	4
3	리더-컨트롤러 통신 프로토콜	4
3.1	레거시 표준: Wiegand	4
3.2	안전한 대안: OSDP	5
3.2.1	OSDP Verified	5
4	Wiegand 리더와 OSDP 리더의 비교	5
4.1	Wiegand 리더	5
4.2	OSDP 리더	6
4.3	사용성	6
4.4	보안	7
5	권장 사항	8
6	Wiegand에서 OSDP로 마이그레이션하기	8
6.1	옵션 1: Wiegand 리더를 OSDP 리더로 교체	8
6.2	옵션 2: Wiegand-OSDP 컨버터 사용	8

1 서론

접근 제어 시스템의 중요한 측면은 사용하는 통신 프로토콜입니다.

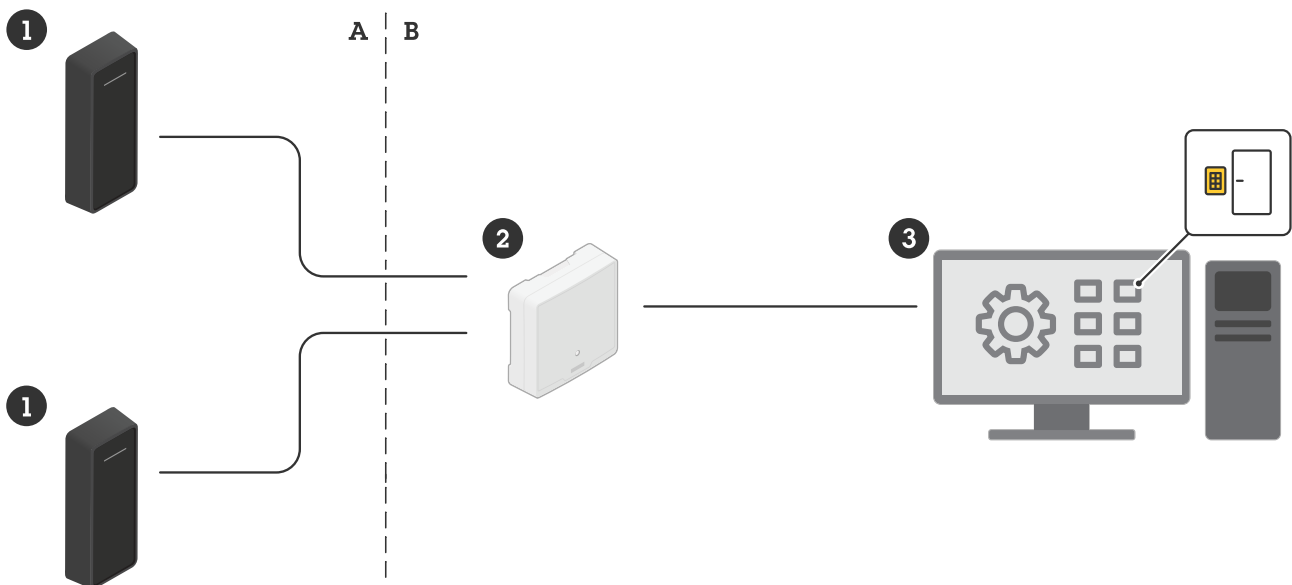
이 백서에서는 접근 제어 시스템에서 리더와 도어 컨트롤러 간에 사용되는 두 가지 주요 통신 프로토콜을 살펴봅니다. 보안 관점에서 장단점을 살펴보고 더 안전한 옵션으로 마이그레이션할 수 있는 방법에 대해 설명합니다.

2 물리적 보안 솔루션의 접근 제어

접근 제어 시스템은 건물, 자산, 사람을 보호하는 데 필수적입니다. 권한이 있는 사람만 보안 구역에 출입할 수 있도록 하여 보안 위험을 줄이고 운영 효율성을 높입니다. 이러한 시스템은 기업 사무실, 데이터 센터, 의료 시설, 정부 기관 등 다양한 분야에서 널리 사용되고 있습니다.

일반적인 접근 제어 시스템은 세 가지 주요 구성 요소로 구성됩니다.

- 1 접근 제어 리더: 사용자 자격 증명을 읽고 자격 증명 데이터를 컨트롤러로 전송하는 장치입니다. 일반적인 사용자 자격 증명에는 키 카드, 모바일 자격 증명, PIN 및 생체 인식이 포함됩니다.
- 2 도어 컨트롤러: 자격 증명 데이터를 처리하고 액세스 허용 또는 거부를 결정하는 의사 결정 장치입니다.
- 3 관리 소프트웨어: 보안 관리자가 액세스 정책을 구성하고 활동을 모니터링하며 사용자를 관리하는 인터페이스입니다.



물리적 접근 제어에서, 리더(1)는 도어 외부(비보안 구역, A)에 설치되어 내부(보안 구역, B)에 설치된 도어 컨트롤러(2)와 통신합니다.

3 리더-컨트롤러 통신 프로토콜

시간이 지남에 따라 접근 제어 프로토콜은 보안, 기능 및 통합 용이성을 개선하면서 발전해 왔습니다. 두 가지 주요 프로토콜에 대해 자세히 살펴보겠습니다.

3.1 레거시 표준: Wiegand

Wiegand는 두 개의 데이터 회선을 사용하여 리더에서 컨트롤러로 자격 증명 데이터를 전송합니다. Wiegand는 수십 년 동안 사용되어 왔으며 주로 단순성과 레거시 시스템 호환성으로 인해 여전히 널리 사용되고 있습니다.

Wiegand의 주요 단점은 보안이 취약하다는 것입니다. 가장 두드러진 단점은 암호화가 없다는 것입니다. 데이터가 일반 텍스트로 전송되어 가로채기 및 복제 공격에 취약합니다.

3.2 안전한 대안: OSDP

OSDP(Open Supervised Device Protocol)는 접근 제어 및 보안 제품 간의 상호 운용성을 개선하기 위해 SIA(Security Industry Association)가 개발한 프로토콜입니다. OSDP는 국제전기기술위원회(IEC)에서 국제 표준으로 승인했으며, AES-128 암호화, 양방향 통신 및 실시간 장치 모니터링 기능을 제공합니다. OSDP를 사용하면 컨트롤러가 리더에 명령을 다시 보낼 수 있으므로 LED 제어, 버저 작동 및 변조 감지와 같은 기능도 사용할 수 있습니다.

OSDP의 주요 기능은 스마트 카드 리더와 컨트롤러 간의 원시 자격 증명 데이터의 안전한 전송을 허용하는 Secure Channel(보안 채널) 모드입니다. 이는 생체 인식 및 모바일 자격 증명 유효성 검사와 같은 고급 인증 방법에 특히 유용합니다.

3.2.1 OSDP Verified

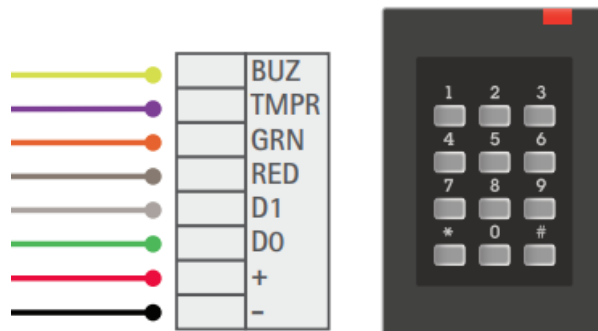
SIA OSDP Verified 프로그램은 장치가 OSDP 표준 및 관련 성능 프로파일을 준수하는지 확인하는 포괄적인 테스트 이니셔티브입니다. SIA는 테스트를 거쳐 목록에 표시된 표준 및 프로파일 기준을 충족하는 것으로 확인된 인증 장치 목록을 유지합니다. 목록에 포함된 장치는 마케팅 자료에 OSDP 인증 마크를 사용할 수 있습니다.

OSDP Verified 마크는 OSDP 장치가 다양한 유형의 접근 제어 사용 사례에 대해 의도한 대로 작동할 것이라는 확신을 통합 업체, 사양 작성자 및 실무자에게 심어줍니다.

4 Wiegand 리더와 OSDP 리더의 비교

리더는 사용하는 통신 프로토콜에 따라 다양한 장단점이 있습니다.

4.1 Wiegand 리더



버저, 변조 감지 및 LED용 추가 케이블을 포함한 Wiegand 리더와 그 배선.

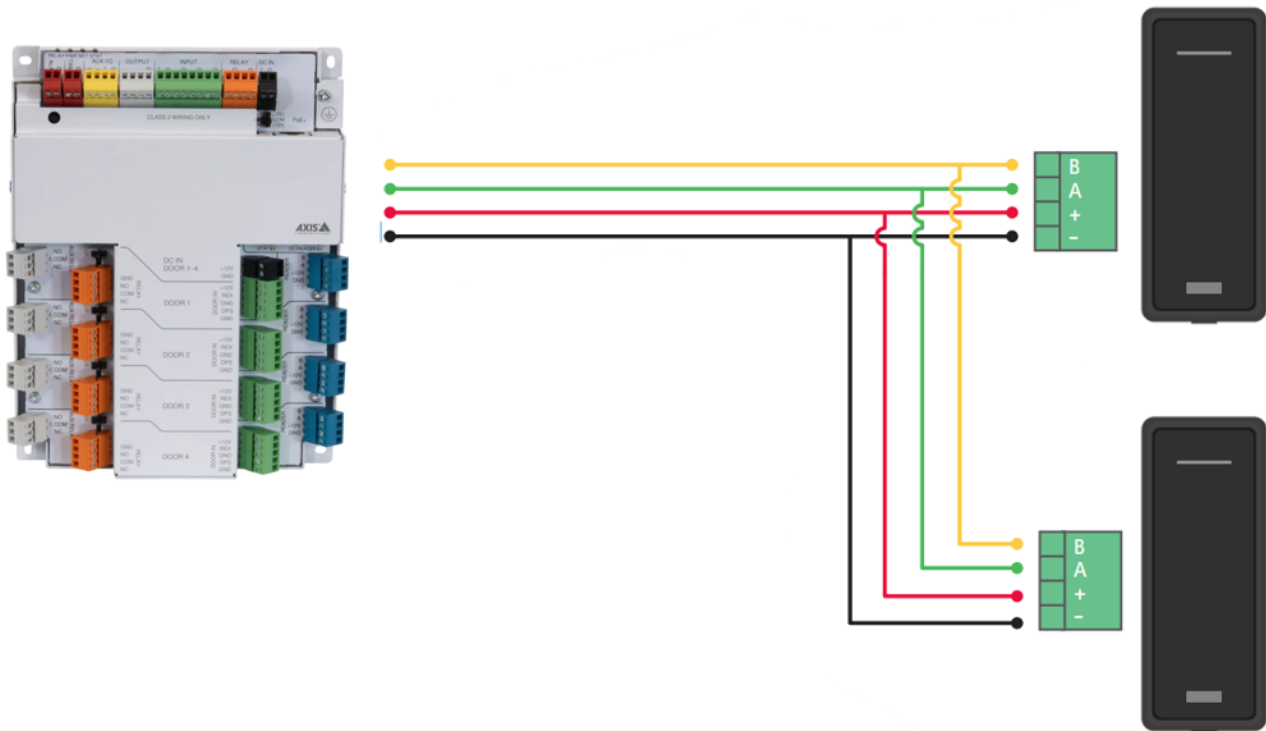
장점:

- 단순하며 구형 시스템과 폭넓게 호환됩니다.

단점:

- 암호화 없음. 데이터는 일반 텍스트로 전송되므로 가로채기가 쉽습니다.
- 단방향 통신. 컨트롤러는 리더로 명령을 다시 보낼 수 없습니다. 즉, 리더가 변조되었거나 교체되었는지 감지할 방법이 없습니다. 리더는 감시되지 않습니다.
- 복잡한 배선. Wiegand 프로토콜을 사용하는 리더에는 리더 버저, 변조 감지 및 LED용 추가 케이블이 필요합니다.
- 최대 케이블 거리는 500피트(약 150미터)입니다.

4.2 OSDP 리더



OSDP 리더(오른쪽)와 도어 컨트롤러에 연결되는 그 배선(왼쪽). LED 제어, 버저 작동, 리더 감시와 같은 기능에는 추가 케이블이 필요하지 않습니다.

OSDP는 RS-485 배선을 사용합니다. 트위스트 페어 케이블을 사용하여 장거리 데이터 전송을 하기 위한 직렬 통신 표준입니다. 안정적인 다지점 통신이 필요한 시스템에서 일반적으로 사용됩니다. 주요 기능으로는 장거리 전송 및 멀티드롭 기능이 있습니다.

장점:

- 암호화된 통신은 자격 증명 가로채기를 방지합니다.
- OSDP를 사용하면 컨트롤러가 리더에 명령을 다시 보낼 수 있습니다. 이 양방향 데이터 교환을 통해 감시 및 원격 구성이 가능합니다. 배선도 간소화됩니다.
- RS-485 배선을 이용하면 최대 케이블 거리를 늘릴 수 있습니다.
- 멀티드롭은 여러 리더가 하나의 연결을 공유할 수 있도록 지원합니다.

4.3 사용성

표 4.1 Wiegand 리더와 OSDP 리더의 사용성 비교.

	Wiegand	OSDP
보안	암호화 없음, 해킹에 취약함	AES-128 암호화, 변조 감지
소통	단방향(리더에서 컨트롤러로)	양방향
케이블 거리	최대 500피트(약 150미터)	최대 4000피트(약 1200미터)
멀티드롭	아니요, 하나의 버스에서 하나의 장치 지원	예, 하나의 버스에서 다중 장치 지원
변조 감지	아니요, 추가 배선 필요	예
감시	아니요, 추가 배선 필요	예

	Wiegand	OSDP
데이터 무결성	자격 증명 재전송 공격에 취약함	암호화된 보안 전송
설치 복잡성	복잡한 배선(D0/D1 및 LED, 변조, 버저)	간편함(RS-485, A 및 B)
탁월한 확장성	배선 제약으로 제한됨	데이터 체인 방식으로 여러 리더 연결 가능
최적 사용 사례	레거시 시스템, 낮은 보안 요구 사항	정부 또는 기업과 같은 부문의 최신 보안 설치 환경

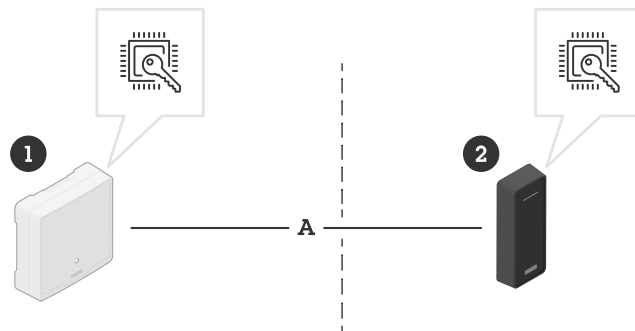
4.4 보안

접근 제어 프로토콜을 선택할 때는 보안을 최우선으로 고려해야 합니다. Wiegand는 암호화 기능이 없기 때문에 여러 유형의 공격에 취약합니다.

- 자격 증명 가로채기. 공격자는 데이터 회선을 도청하고 자격 증명을 캡처할 수 있습니다.
- 재전송 공격. 캡처한 후에는 동일한 자격 증명을 재전송하여 무단 액세스 권한을 얻을 수 있습니다.
- 탬퍼링. 시스템은 리더가 제거되거나 교체되었는지 감지할 수 없습니다.

이에 반해, OSDP는 AES-128(Secure Channel) 암호화 및 장치 감시 기능을 통해 이러한 위험을 완화합니다. 이는 컨트롤러가 리더가 변조되었는지 감지할 수 있도록 하여 무단 액세스를 방지합니다.

암호화는 데이터를 보호하지만, 키를 안전하게 보호하는 것이 암호화를 안전하게 유지하는 핵심입니다. 강력한 키 보호가 없으면, 시스템 전체가 위험에 처할 수 있습니다. 따라서 Secure Channel(보안 채널) 키는 컨트롤러와 리더 양쪽 끝의 특수 하드웨어 칩에 안전하게 보관해야 합니다. 보안 요소와 같은 이러한 보안 하드웨어 영역은 공격자가 장치에 물리적으로 액세스하더라도 키를 얻지 못하게 하도록 만들어졌습니다.



접근 제어에서 보안 키 저장소를 사용하여 엔드 투 엔드 보안을 달성합니다. 마스터 키와 개별 보안 채널 기본 키(SCBK)는 모두 보안 키 저장소에 저장되며, 도어의 양쪽의 장치에 저장됩니다.

- 1 도어의 보안 측에 설치된 도어 컨트롤러
- 2 도어의 비보안 측에 설치된 리더
- 3 A: OSDP 보안 채널 통신

표 4.2 Wiegand 리더와 OSDP 리더의 보안 측면 비교.

	Wiegand	OSDP
암호화	없음, 평문 데이터	AES-128 암호화
데이터 가로채기	자격 증명 가로채기 쉬움	가로채기 방지를 위해 암호화됨

	Wiegand	OSDP
재전송 공격	자격 증명 복사/재전송 가능	암호화로 방지
변조 감지	아니요, 변조된 리더 감지 불가	예, 컨트롤러가 리더 상태 모니터링
감시	아니요, 컨트롤러가 리더 상태를 확인할 수 없음	예, 실시간 감시
규정 준수	보안 환경에는 권장되지 않음	최신 보안 표준 충족

5 권장 사항

오늘날의 보안 환경에서 Wiegand는 더 이상 새로운 설치 환경에 적합한 옵션이 아닙니다. 조직은 더 나은 보안, 안정성 및 미래 확장성을 위해 OSDP 리더로 전환해야 합니다.

- 현재 접근 제어 인프라를 평가하십시오. 현재 Wiegand를 사용하고 있다면 마이그레이션 전략 계획을 시작하십시오. 전체 OSDP 마이그레이션 또는 Wiegand-OSDP 컨버터 중 어느 것이 최상의 대안인지 결정하십시오.
- 새로운 설치 환경의 경우, 암호화되고 변조 방지된 통신을 보장하기 위해 되도록 OSDP 리더를 선택하십시오.
- 보안 전문가와 협력하여 위협으로부터 보호하는 안전하고 현대적인 접근 제어 시스템을 구현하십시오.

6 Wiegand에서 OSDP로 마이그레이션하기

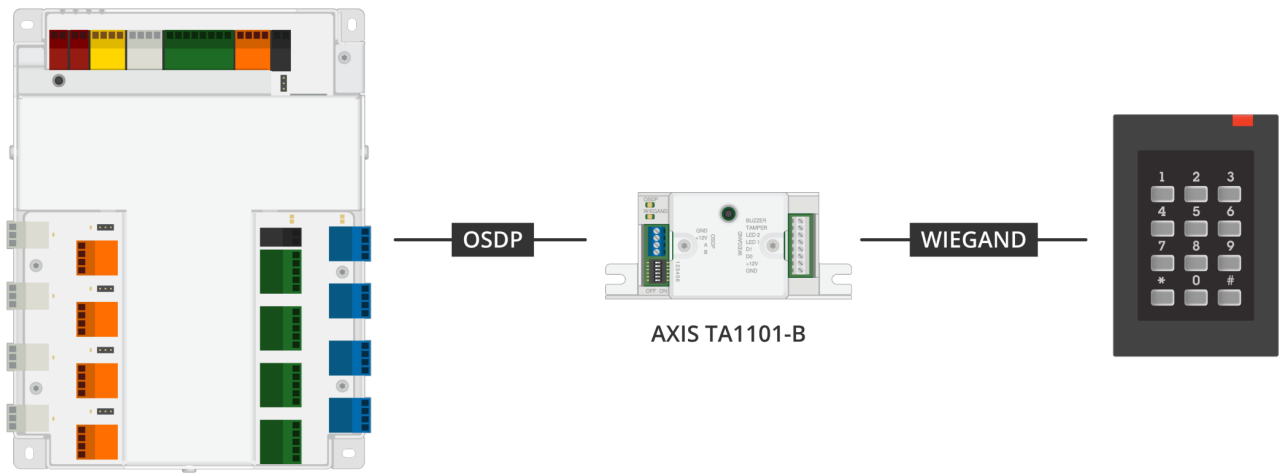
많은 조직이 여전히 Wiegand 리더에 의존하지만 전체 시스템을 교체하지 않고 보안을 강화하기를 원합니다. 두 가지 실용적인 마이그레이션 경로가 있습니다. 두 옵션 모두 보안을 향상시키지만, 직접적인 OSDP 구현은 접근 제어 시스템을 미래에도 안정적으로 사용할 수 있도록 하려는 조직에게 가장 좋은 장기적 투자입니다.

6.1 옵션 1: Wiegand 리더를 OSDP 리더로 교체

이는 최상의 장기적 솔루션입니다. 구형 Wiegand 리더를 OSDP 호환 모델로 교체함으로써 조직은 암호화, 양방향 통신 및 리더 감시의 이점을 누릴 수 있습니다. 그러나 이를 위해서는 접근 제어 패널이 OSDP를 지원하는지 확인해야 합니다.

6.2 옵션 2: Wiegand-OSDP 컨버터 사용

모든 리더를 즉시 교체할 수 없는 조직의 경우, Wiegand-OSDP 컨버터가 비용 효율적인 대안입니다. 이 장치는 Wiegand 데이터를 암호화하여 OSDP 호환 컨트롤러로 전송하므로 전체 하드웨어 점검 없이 보안을 향상시킵니다.



AXIS A1710-B

AXIS TA1101-B

Wiegand-OSDP 컨버터(가운데)를 사용하여 보안을 향상시킬 수 있습니다.

Axis Communications에 대하여

Axis는 보안, 안전, 운영 효율성 및 비즈니스 인텔리전스를 향상시켜 더 스마트하고 더 안전한 세상을 실현합니다. 네트워크 기술 회사이자 업계 선도 기업인 Axis는 영상 감시, 접근 제어, 인터콤 및 오디오 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 보완되고 고품질 교육을 통해 지원됩니다.

50개 이상의 국가에서 약 5,000명의 Axis 임직원이 전 세계의 기술 및 시스템 통합 파트너와 협력하여 고객에게 최적의 솔루션을 제공하고 있습니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다.