

白皮书

为什么在门禁控制中选择 OSDP 而不是 Wiegand

5月 2025

概述

虽然 Wiegand 仍是门禁控制器应用中的常用接口，但由于其存在安全缺陷，正迅速被淘汰。将安全放在首位的企业应过渡到 OSDP，以更好地防范攻击。OSDP 提供加密、受监控的通信，是安全环境的理想选择。将您的门禁控制器升级为 OSDP 不仅能为当前提供更好的安全保障，还能使您的企业在未来应对不断变化的威胁。

目录

1	引言	4
2	物理安全解决方案中的门禁控制	4
3	读卡器与控制器之间的通信协议	4
3.1	传统标准：Wiegand	4
3.2	安全的替代方案：OSDP	5
3.2.1	OSDP Verified	5
4	Wiegand 和 OSDP 读卡器比较	5
4.1	Wiegand 读卡器	5
4.2	OSDP 读卡器	6
4.3	可用性	6
4.4	安全	7
5	建议	8
6	从 Wiegand 迁移到 OSDP	8
6.1	选项 1：将 Wiegand 读卡器替换为 OSDP 读卡器	8
6.2	选项 2：使用 Wiegand 至 OSDP 转换器	8

1 引言

门禁控制系统的一个重要方面是其使用的通信协议。

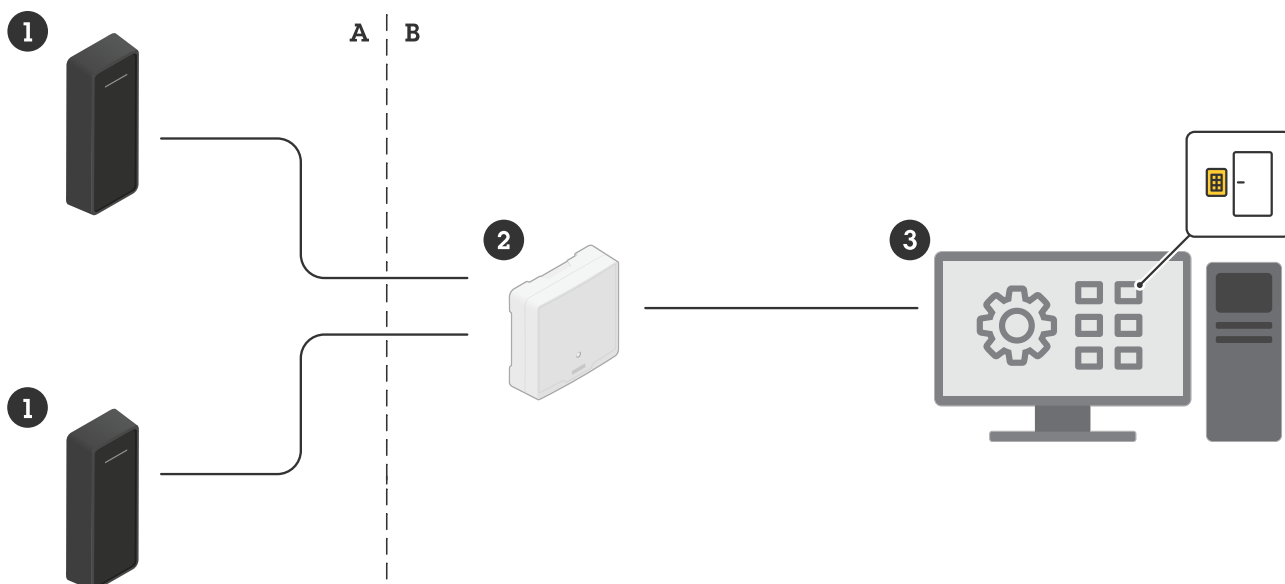
本白皮书探讨了门禁控制系统中读卡器和门禁控制器之间使用的两种主要通信协议。我们将从安全角度分析它们的优缺点，并讨论如何开始迁移到更安全的选项。

2 物理安全解决方案中的门禁控制

门禁控制系统对于保护建筑物、资产和人员非常重要。它们确保只有经授权的人员才能进入安全区域，从而降低了安全风险，提高了运营效率。这些系统广泛应用于各行各业，包括企业办公室、数据中心、医护场所和政府机构。

典型的门禁控制系统由三个关键部分组成。

- 1 门禁控制读卡器：这些设备读取用户凭证并将凭证数据传输到控制器。典型的用户凭证包括钥匙卡、移动凭证、PIN 码和生物识别。
- 2 门禁控制器：这些决策设备处理凭证数据并决定是否允许进入。
- 3 管理软件：一种界面，让安全管理员能够配置门禁策略、监视活动状况以及管理用户。



在物理门禁控制中，读卡器 (1) 安装在门外（非安全区域，A），并与安装在门内（安全区域，B）的门禁控制器 (2) 通信。

3 读卡器与控制器之间的通信协议

随着时间的推移，门禁控制协议也在不断发展，安全性、功能性和易集成性都得到了提高。让我们仔细看看以下两种主要协议。

3.1 传统标准：Wiegand

Wiegand 通过两条数据线从读卡器向控制器发送凭证数据。Wiegand 已有几十年的历史，至今仍被广泛使用，主要原因在于其简单性和与传统系统的兼容性。

Wiegand 的主要缺点是安全性差。最明显的是，它不支持加密。数据以明文传输，因此很容易被截获和遭到克隆攻击。

3.2 安全的替代方案：OSDP

开放式监控设备协议 (OSDP) 由美国安防行业协会 (SIA) 开发，旨在提高门禁控制产品与安防产品之间的互操作性。OSDP 已被国际电工委员会批准为国际标准，并引入了 AES-128 加密、双向通信和实时设备监视功能。由于 OSDP 允许控制器将命令回送至读卡器，因此还能实现 LED 控制、蜂鸣器激活和篡改侦测等功能。

OSDP 的一个主要功能是安全通道模式，它允许在智能卡读卡器与控制器之间安全传输原始凭证数据。这对生物识别和移动凭证验证等高级身份验证方法尤其有用。

3.2.1 OSDP Verified

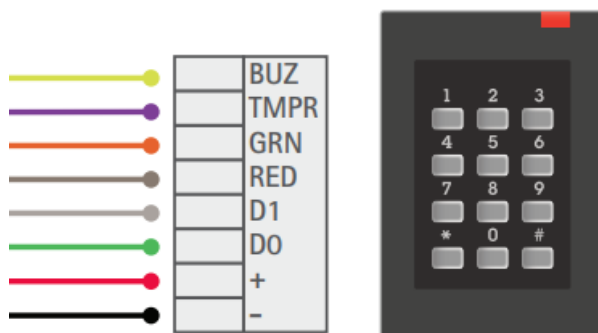
SIA OSDP Verified 计划是一项较全面的测试计划，用于验证设备是否符合 OSDP 标准和相关的性能配置文件。SIA 保留一份经过测试并与标准和列表中所示的配置文件相符的验证设备的清单。清单中的设备可在营销材料中使用 OSDP Verified 标识。

OSDP Verified 标志为集成商、规格指定者和实际操作者树立了信心，让他们相信 OSDP 设备能够在种类广泛的门禁控制器使用场合中发挥预期作用。

4 Wiegand 和 OSDP 读卡器比较

根据所使用的通信协议，读卡器有不同的优缺点。

4.1 Wiegand 读卡器



Wiegand 读卡器及其接线，包括用于蜂鸣器、篡改侦测和 LED 的额外电缆。

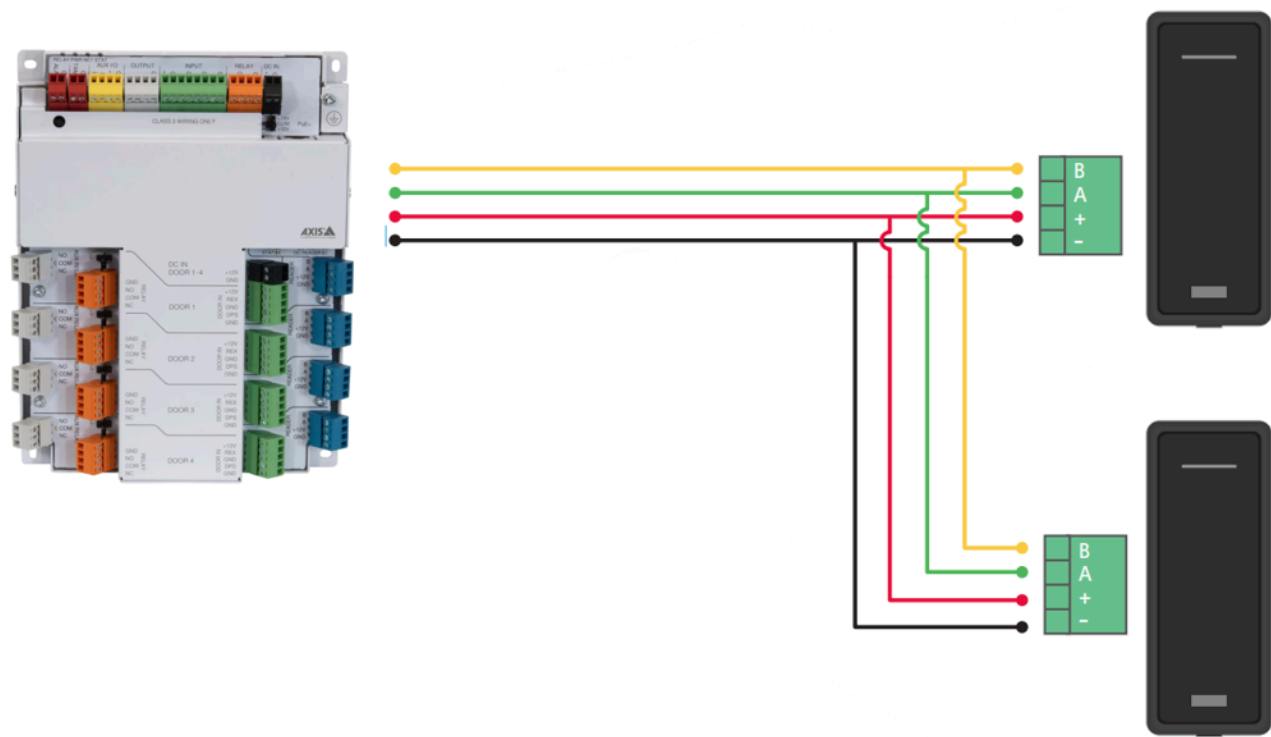
优点：

- 操作简单，广泛兼容旧系统。

缺点：

- 不加密。数据以明文传输，很容易被截获。
- 单向传输。控制器无法向读卡器回送命令。这意味着，无法侦测读卡器是否被篡改或更换——读卡器不受监控。
- 布线复杂。使用 Wiegand 协议的读卡器需要额外的电缆来连接读卡器蜂鸣器、篡改侦测装置和 LED 指示灯。
- 最大电缆连接距离为 500 英尺（约 150 米）。

4.2 OSDP 读卡器



OSDP 读卡器（右）及其与门禁控制器的接线（左）。LED 控制、蜂鸣器激活和读卡器监控等功能不需要额外的电缆。

OSDP 使用 RS-485 接线。这是一种使用双绞电缆远距离传输数据的串行通信标准。它通常用于需要可靠多点通信的系统中。主要功能包括远距离传输和多点传送功能。

优点：

- 加密通信可防止凭证被截获。
- OSDP 允许控制器向读卡器回送命令。通过这种双向数据交换，可以进行监控和远程配置。它还简化了布线。
- RS-485 接线可启用更长的最大电缆连接距离。
- 多点传送让多个读卡器能够共享一个连接。

4.3 可用性

表格 4.1 Wiegand 和 OSDP 读卡器在可用性方面的比较。

	Wiegand	OSDP
安全	无加密，易受黑客攻击	AES-128加密、篡改侦测
通讯	单向（读卡器到控制器）	双向
电缆距离	可达 500 英尺（约 150 米）	可达 4000 英尺（约 1200 米）
多点传送	否，一个设备一条总线	是，一条总线上支持多个设备
篡改侦测	否，需要额外布线	是
监控	否，需要额外布线	是
数据完整性	易受凭证复制攻击	加密，安全传输

	Wiegand	OSDP
安装复杂性	接线复杂（D0/D1 和 LED、防篡改装置、蜂鸣器）	简单（RS-485，A 和 B）
可扩展性	受接线限制	可以菊花链方式连接多个读卡器
更适用的场合	传统系统，安全需求低	政府或企业等领域的先进安全系统

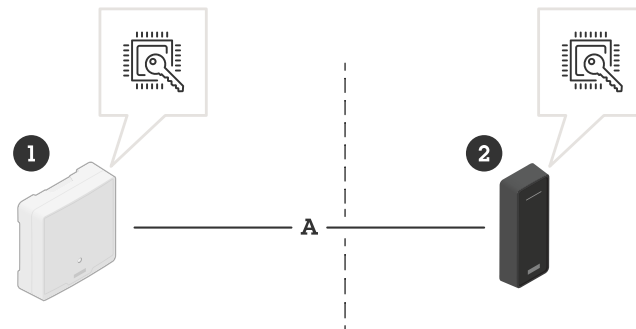
4.4 安全

在选择门禁控制协议时，应将安全性放在首位。由于 Wiegand 缺乏加密，因此容易受到多种类型的攻击。

- 凭证截获。攻击者可以窃听数据线路并获取凭据。
- 复制攻击。一旦捕获，就可以复制相同的凭据，以获取未经授权的访问。
- 篡改。系统无法侦测读卡器是否被移除或更换。

相比之下，OSDP 通过 AES-128（安全通道）加密数据，并提供设备监管，来降低了这些风险。这样可以确保控制器能够侦测读卡器是否被篡改，从而防止未经授权的访问。

加密能确保数据安全，而保护密钥则能确保加密安全。没有强大的密钥保护，整个系统都可能面临风险。因此，安全通道密钥应安全地保存在控制器和读卡器两端的专用硬件芯片中。这些安全硬件区域，如安全元件，旨在阻止攻击者即使获得设备的物理访问权限也无法获得密钥。



在访问控制中，利用安全密钥库实现端到端安全。主密钥和个体安全通道基本密钥 (SCBK) 均存储在（位于门的两侧的）设备的安全密钥库中。

- 1 门禁控制器安装在门的安全侧
- 2 读卡器安装在门的非安全侧
- 3 A：OSDP 安全通道通信

表格 4.2 Wiegand 和 OSDP 读卡器在安全方面的比较。

	Wiegand	OSDP
加密	无，明文数据	AES-128 加密
数据截获	轻松截获凭证	加密以防截获
复制攻击	凭证可被复制	通过加密防止
篡改侦测	否，无法侦测被篡改的读卡器	是，控制器监视读卡器状态

	Wiegand	OSDP
监控	否，控制器无法验证读卡器状态	是，实时监控
合规	不建议用于安全环境	符合先进的安全标准

5 建议

在当今的安全环境下，Wiegand 已不再是新装系统的可行选择。企业应过渡到 OSDP 读卡器，以获得更好的安全性、可靠性和未来可扩展性。

- 评估当前的门禁控制基础设施。如果您目前正在使用 Wiegand，请开始规划迁移策略。确定是全面迁移 OSDP 还是 Wiegand-OSDP 转换器是更好的选项。
- 对于新装系统，应尽可能选择 OSDP 读卡器，以确保加密且防篡改的通信。
- 与安防专业人员合作，部署安全、先进的门禁控制系统，防范威胁。

6 从 Wiegand 迁移到 OSDP

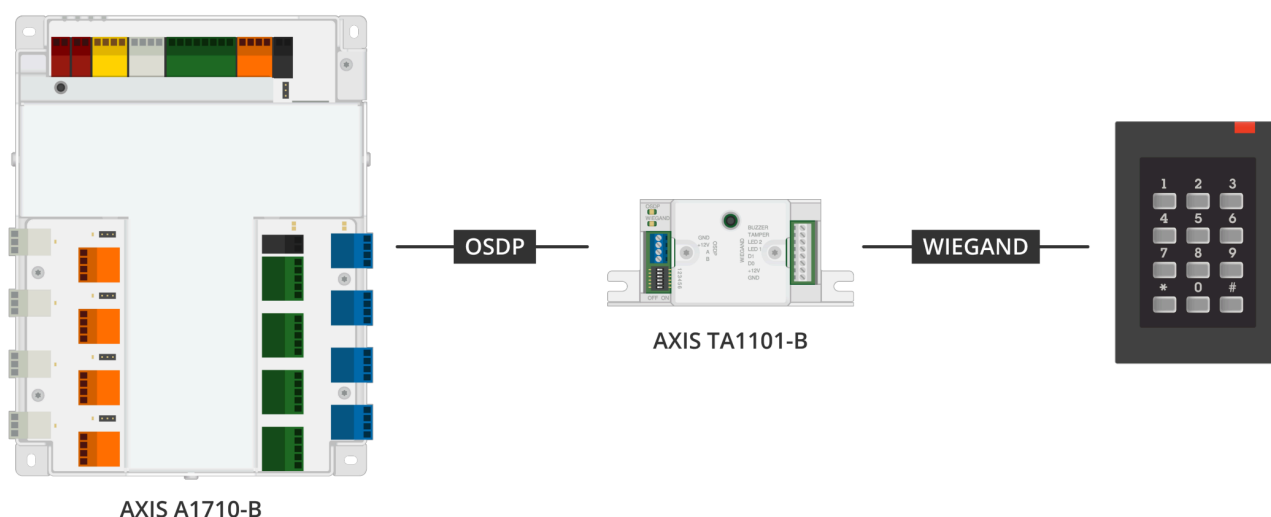
许多企业仍然依赖 Wiegand 读卡器，但希望在不更换整个系统的情况下提高安全性。有两种切实可行的迁移途径。这两种选项都能提高安全性，但对于希望门禁控制系统能够满足未来需求的企业来说，直接部署 OSDP 是更好的长期投资。

6.1 选项 1：将 Wiegand 读卡器替换为 OSDP 读卡器

这是更好的长期解决方案。将过时的 Wiegand 读卡器替换为符合 OSDP 标准的型号后，企业可以从加密、双向通信和读卡器监控中获益。不过，这需要确保门禁控制面板支持 OSDP。

6.2 选项 2：使用 Wiegand 至 OSDP 转换器

对于无法立即更换所有读卡器的企业来说，Wiegand-OSDP 转换器是一种性价比较高的替代方案。该设备可在向兼容 OSDP 的控制器发送 Wiegand 数据之前对这些数据进行加密，从而在不需要彻底改造硬件的情况下提高安全性。



使用 Wiegand-OSDP 转换器（中）可以提高安全性。

关于安讯士 (Axis Communications)

安讯士通过打造各种解决方案，提高安全水平和企业效益，旨在创建一个高度智能、更加安全的世界。作为一家网络技术公司和行业领导者，安讯士致力于推出视频监控、访问控制、内部通信和音频系统解决方案。安讯士通过智能分析应用程序增强解决方案，并提供高质量培训支持。

安讯士在全球50多个国家和地区设有办事机构，拥有超过5,000名尽职的员工，并遍布世界各地的技术和系统集成合作伙伴携手并进，为客户带来高价值的解决方案。安讯士创立于1984年，总部位于瑞典。