关键任务设施的物理安全

第 82 号白皮书

版本 2

作者 Suzanne Niles

> 摘要

物理安全 – 控制人员对设施的访问 –对实现数据中心可用性目标来说的至关重要。随着像生物识别技术和对安保数据进行远程管理等技术被越来越广泛地应用，传统的门禁卡和门卫构成的安保架构正逐渐被能够在数据中心内部和周围提供主动识别和追踪人员活动的安保系统所取代。 在对设备进行投资之前，IT 经理们必须仔细评估具体安保需求并为自己负责管理的设施选择最合适和最经济的安保措施。本白皮书将概述人员身份验证的基本原理并介绍安保系统的基本要素和流程。

目录

点击内容即可跳转至具体章节

APC 白皮书现收录于施耐德电气白皮书资料库
由施耐德电气**数据中心科研中心**发表，
DCSC@Schneider-Electric.com

Schneider Electric

简介

人员：一项亟待管理的风险

当提及数据中心安全时，人们的第一反应通常是要防止恶意破坏、阴谋间谍活动或是数据盗窃。抵御外部闯入者以及他们的蓄意破坏行为，其必要性不言而喻。然而，数据中心内工作人员的日常工作也有可能造成伤害，对于大多数设施来说，这种随时可能出现的风险危害往往更大。

人员对数据中心的运营至关重要，但是也有研究显示，60%的意外和失误造成的数据中心宕机都是直接人为造成的 — 程序不当、设备标识错误、物品坠落或飞溅、命令输入错误、以及其它或大或小的意外。有人存在的地方，就不可避免地可能出现人为失误，因此尽量控制和减少人员进出设施是风险管理的一个关键环节，即使是恶意破坏的可能性非常小的时候。

识别技术伴随其所保护的设施、信息和通信的发展也在同步快速变化更新。随着新设备和新技术的不断涌现，很容易让一个长期存在的问题变得模糊起来，那就是如何禁止未经许可或是有不良企图的人员进入他们本不应该进入的场所，这种技术所要解决的问题既不含有技术性，操作起来也并不复杂。第一步：在划定设施内的安全区域和制定准入制度时是需要制作分层的和较复杂的布局图，但是这并不是非常困难的事情。IT 经理通常都知道人员的准入权限。真正的挑战在于第二步：决定应用何种合适的技术让整个计划以最好方式得以实现。

> 数据中心物理基础设施

物理安全是数据中心物理基础设施（DCPI）的一部分，因为它直接关系着系统可用性（“正常运行时间”）能否得到最大化。它可以减少由于无关人员或有不良企图的人员进入数据中心而导致的事故或破坏，从而减少宕机。

其它 DCPI 元素是电源、制冷、机柜、线缆和消防。

你是谁，以及你为什么出现在这里？

尽管各种安保技术层出不穷并且看似神秘，比如指纹和手部扫描、瞳孔扫描、智能识别卡、面部几何识别等，安全保护的目的却自始自终从未发生改变，它既不复杂而且为我们大家所熟悉：那就是回答这样一个问题“你是谁，以及你为什么出现在这里？”

第一个问题“你是谁”，在设计自动化安保系统时可谓是头号难题。当前流行的技术都试图通过某种方法评估人员的身份。根据成本投入的不同，其精确度也相应不同。比如，门禁卡的成本较低，但其身份识别结果相对模糊（不能确定是谁在使用这张卡）；而虹膜扫描仪非常昂贵，但却可以准确识别人员身份。在精确性和购买成本之间找到恰当的平衡点是安保系统设计的核心所在。

第二个问题“你为什么出现在这里？”，这个问题也可以理解为“你进入这个场所是要做什么？”，问题的答案可以是身份识别后所给出的提示（“这是 Alice Wilson，我们的布线专家，她负责线缆敷设相关的工作，让她进来”），也可以以许多不同方式出现：一个人“是谁”和“为什么出现在此”的信息可以同时写入门禁卡的磁条里，比如，一个人的身份信息可以激活其在电脑文件里相对应的准入权限信息；或者进入设施内的不同区域可以实施不同的准入措施，根据不同进入目的决定是否放行。有时“为什么出现在这里？”是唯一的问题，“你是谁”其实无关紧要，这种情况主要针对维修和清洁人员。

结合各种专业知识，寻求最佳解决方案

IT 经理们了解其设施内都有“谁”以及这些人员“为什么出现在此”，但是他们可能并不熟悉如何使用当前的安保方法或技术的细节，其实他们也不需要知道。而他们所知道的是自己的预算限制，也了解在自己所管理的设施内各种安全违规行为的潜在风险。

另一方面，安保系统顾问，虽然他们不知道设施内的具体状况，但是他们熟悉当前安保技术的功能、缺点和成本。他们也拥有在其它安保系统设计上积累的丰富经验，因此能够通过提出针对性的问题帮助澄清、提炼或简化对“谁” 和“为什么”的要求。

只有结合来自 IT 经理和安保系统顾问这两方面的专业知识才能够平衡准入的要求、可接受的风险、可应用得方法和预算限制，完成对安保系统解决方案的设计。

问题的定义

安全禁区：哪些区域需要受到保护？

第一步，我们需要制定一个安保规划 — 绘制一张物理设施地图，然后标识出各个区域和入口的相应准入规则，或者叫**安保级别**。

这些区域可能是层层相套的边界：

- 场地周边
- 楼宇周边
- IT 区域
- 机房
- 设备机柜

也可能是并排相连的边界

- 访客区
- 办公区
- 动力间

> “物理安全”还意味着...

*物理安全*也包括防止设备设施免遭灾难（水灾、火灾、地震、爆炸）或设备失效或故障（停电，暖通空调故障）。

本文内容仅涉及对人员进出现场所造成的风险的保护。.

层层相套的区域能够采取不同或严格程度渐进明细的门禁规则，提供层层累加的保护，称之为“**安保纵深**”。具有安保纵深，使内部的区域不仅受到本区域的准入措施的保护，而且受到包围这个区域的其它区域的措施的保护。此外，任何人员在违规进入外层区域后，仍将受到下一内层区域的门禁管束。

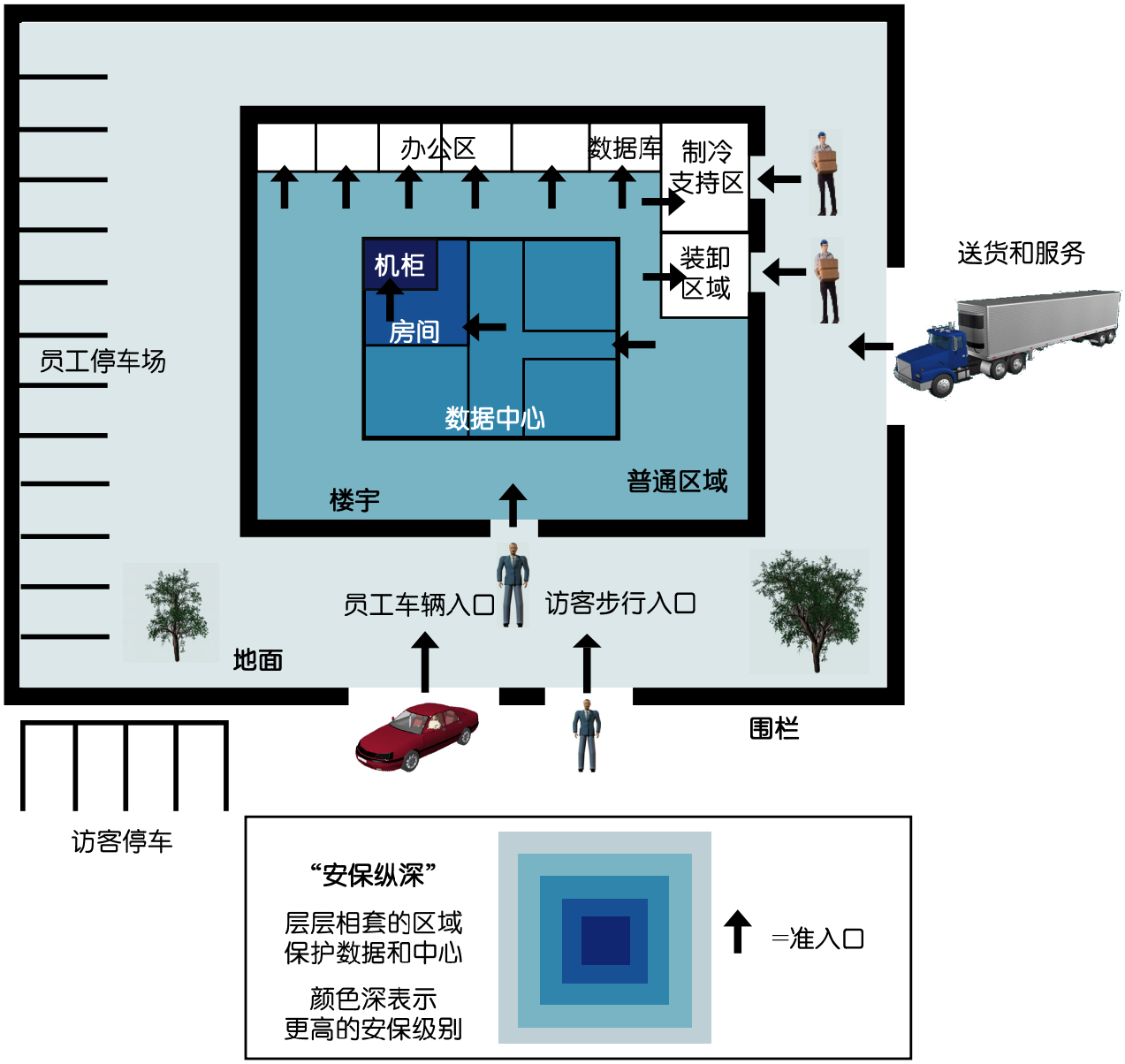

图 1

安保示意图：“安保纵深”

机柜级安保： “安保纵深”的最里层 — 比数据机房还要更近一层 — 就是机柜。机柜锁还没有被广泛地应用，但是如果使用的话，它们将是阻止未经授权访问关键设备的最后一道屏障。不是所有进入机房内的人员都有必要被授权接触每一个机柜，机柜锁可以让只有管理服务器的人员能够接触到服务器，只有通信人员能够接触到通信设备，等等。可管理的”机柜锁可以实现远程配置，从而只有在必要时才同意指定的人员在指定的时间进行访问。这样就减少意外事件、蓄意破坏或在未经授权的情况下安装额外通信设备，其可能导致耗电量异常增加和机柜温度异常升高。

基础设施安保： 安保地图不仅需要包含设施内放置 IT 功能设备的区域，同时也应包含放置物理基础设施的区域。这些设备如果存在风险，也将可能导致宕机。比如，暖通空调设备可能突然意外停机或被蓄意关停，发电机的电池可能被盗窃，或者系统管理控制台可能被恶意误导而激活消防喷淋器。

准入规则：哪些地方允许哪些人进入?

一个人进入安全禁区的权限可以建立在不同基础上。除了常见的“身份”和“目的”，下列两个也是常常作为权限确定的基础 — 当然此外还有一些需要特殊处理的其它情况，比如“知道的必要性”

个人身份：设施内的某个人需要进入设施内与其工作相关的区域。比如，安保主管可以在设施内的大部分区域活动，但是不能进入存储客户数据的地方。计算机操作部的主管可以进入计算机机房和操作系统，但是却无权进入放置电源和 HVAC 设备的房间。公司 CEO 可以进入安保主管和 IT 工作人员的办公区以及公共区域，但是不能进入计算机机房或支持区。

在场的原因：市电维修人员，无论其是 Joe Smith 还是 Mary Jones，都可能只有权限进入支持区和公共区域。而对于清洁人员来说，由于人员经常变化，它们只有权限进入公用区，而不能进入其它任何地方。网络交换机专家只有权限接触放置交换设备的机柜，而不能接触放置服务器或存储设备的机柜。在网络服务器设施内，客户的系统维护人员可能只有权限进入“客户网络访问室”，他们可以在这里连接到他们的个人服务器进行管理工作。

> 对问题分而治之

识别技术不应干扰安保地图最初制定的规则。首先，请划定您设施内的安全区域并制定安保规则，然后进行成本/效果/风险分析，需找它们之间的平衡点，并最终确定最佳技术执行方案。.

知道的必要性：进入特别敏感区域的权限可以出于特殊目的授予特殊人员 — 也就是说，如果他们“有必要知道”时，可以授予他们进入权限，同时也仅限于他们在这种需求下拥有此权限。

技术的应用

识别方法：可靠性 vs.成本

人员身份识别的方法现在主要分为三类，它们的可靠性依次增强，但设备成本也成正比升高：

- **你有什么**
- **你知道什么**
- **你是谁**

你有什么：可靠性最低（可被借用或盗用）
“你有什么”是指你穿的或携带的某种物品 — 比如钥匙、卡片或小物品（**凭证**），这些东西可以戴在身上或挂在钥匙圈里。它可以是老式的金属钥匙，也可以是能够与读卡器交换信息的“智能”识别卡（**智能卡**）。它可以是写有您个人信息的磁条卡（比如我们所熟悉的银行 ATM 卡）；也可以是带有发射器和/或接收器能够与读卡器近距离交换信息的卡片和证件（**感应卡**或**感应凭证** — 比如 Mobil Speedpass®）

“你有什么”是可靠性最低的一种识别形式，因为它不能保证被正确的人使用 — 可以借给别人，被他人盗用，或在丢失后被他人捡到使用。

你知道什么：可靠性较佳（不能被盗窃，但是可能会被告知他人或被记录下来）
“你知道什么”是用于某个装置的一组密码、代码或程序，比如开启密码锁，读卡器验证，或计算机的键盘输入。密码/代码在安保方面处于两难局面：如果太容易被记住，那么很可能被他人猜出；如果很难记住，可能不容易被猜出 — 但是很可能会被写下来，安保作用也会降低。

“你知道什么”比“你有什么”的可靠性高一些，但是密码和代码仍然可能会被告知他人，并且如果被记录下来，也存在安保风险。

你是谁：可靠性最高（基于某些只属于你的身体特征）

“你是谁”是指通过唯一身体特征进行的身份识别 — 也就是人员识别其他人的自然方式，几乎不会出现差错。当用技术来执行这一识别过程时，它被称作“生物识别方法”。通过大量测量和分析，我们已经针对人类多种特征开发出生物识别扫描技术。

指纹
虹膜（色素）
视网膜（血管形状）
声音
手掌（手指形状和手掌厚度）
面部（眼睛、鼻子和嘴巴的位置）
笔迹（用笔的力度）

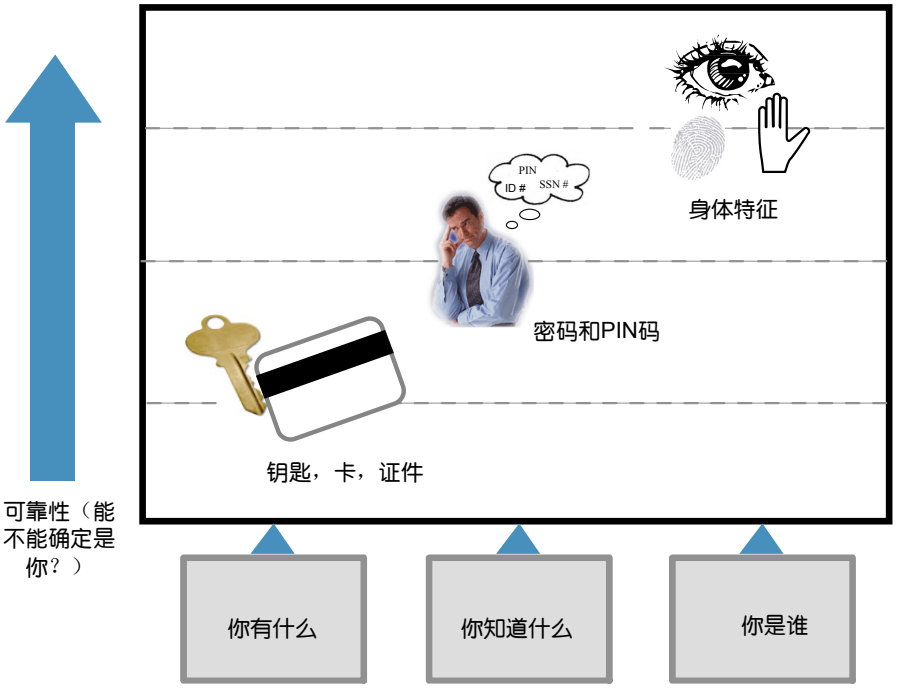

图 2

“你有什么”，“你知道什么”和“你是谁”

生物识别装置一般非常可靠，如果识别通过 — 也就是说，如果生物识别装置认为是你，那么基本上可以肯定就是你。生物识别技术的不可靠性主要不是源自识别失败或者冒名顶替，而是合法用户可能不被识别通过（即“错误拒绝”）。

多种方法综合使用，提高可靠性

常见的安保方案是从外层（敏感度最低）区域到内层（敏感度最高）区域采用不同安保方法，其可靠性和成本逐渐提高和增加。比如，楼宇入口可能需要刷卡+PIN 码；计算机机房门口可能需要使用键盘密码+生物识别。在一个入口结合使用多种识别方法可以提高可靠性；在一个区域使用多种识别方法可以很大程度上提升内层区域的安全，因为每个区域不但受到自身识别方法的保护同时也受到外层识别方法的预先保护。

>对问题分而治之

识别技术不应干扰安保地图最初制定的规则。首先，请划定您设施内的安全区域并制定安保规则，然后进行成本/效果/风险分析，需找它们之间的平衡点，并最终确定最佳技术执行方案。

安保系统管理

一些门禁装置 —比如读卡器和生物识别扫描仪 —能够捕捉人员出入的数据，包括出入人员的身份以及他们出入的时间。如果联网，这些装置还能将这些信息传送到远程管理系统以供监控和记录（谁在进出这个区域），设备控制（允许某人在某时可以进出），以及发出告警（通知有人在验证失败后重复尝试进入该区域或设备故障）。

门禁装置

卡和凭证：“你有什么”

目前用于门禁的卡片和凭证有很多种类，从简单的到复杂的都有，其功能也有高有低：

- 能够重新编程
- 防伪技术
- 与读卡器的互动方式：刷卡式，插入式，平面接触式，非接触式（“感应”）
- 方便性：物理形态以及如何携带/佩戴
- 所携带的数据大小
- 计算能力
- 卡片成本
- 读卡器成本

无论这些技术本身的安保作用和可靠性如何，这些实体“物品”都不能保证一定能够被正确授权的人员使用。因此，通常会将其与其它识别技术结合使用，比如密码或生物识别方法。

磁条卡是最常见的卡片种类，磁条上面写有识别数据。当在读卡器前面刷卡时，磁条上的信息就会被读取，并与数据库上的信息进行核对。这个系统价格不贵并且易于使用；缺点是卡片相对容易复制伪造以及卡片上的信息容易被盗取。

钡铁氧体卡（也称“磁点卡”），它与磁条卡类似，但是能够提供更高安全性，并且无需增加太多成本。它包含一张磁性材料制成的薄片，上面用圆点组成一定图案。这种卡无需扫描或刷卡，只需接触读卡器即可。

韦根卡是磁条卡的演变，卡上内置有一组经过特殊处理并携带独特磁性签名的电线。当在读卡器前刷卡时，感应线圈就会探测到这个签名，并将其转换成比特串。这种卡的复杂设计有一个优点，那就是卡不能被复制；缺点则是也不能重新编程。利用这种技术，卡无需与读卡器直接接触；因此读卡器的磁头可以密封，从而支持户外安装。和感应卡以及磁条卡的读卡器不同，韦根卡的读卡器不受射频或电磁场的干扰。读卡器的这种稳定性以及卡片难以复制的特点让韦根卡系统非常安全（就“你有什么”安保方法范围内而言），但是也更昂贵。

条码卡携带一组条码，当卡片从读卡器扫过时可以被读取。这种系统价格非常低廉，但是也非常容易伪造 — 一台普通的复印机就可以复制条码并骗过条码读卡器。条码卡适用于安保要求较低的应用，特别是需要在设施内遍布大量读卡器时或者交通流量特别大的入口。它不太像是一个安保系统，而只能说是一种便宜的进出监控方法。（有种说法是条码卡只适用于“防君子而不防小人”。）

红外阴影卡通过在 PVC 塑料层之间设置条码增强了条码卡的安全性。读卡器发射红外光穿透卡片，条码的阴影就会被另一侧的感应器读取。

感应卡提升了卡片的方便易用性，无需刷卡或解除读卡器。和它的名字一样，感应卡只需靠近读卡器即可。这种卡采用了 RFID（射频识别）技术，读卡器的电磁场会作用于卡片。目前最流行的设计是距离读卡器 10 厘米（4 英寸）读卡；还有一种设计 — 称为**近距型卡** — 其读卡距离可达到约 1 米（3 英尺）。

智能卡是最新开发的门禁卡技术，并且正快速被许多新装置所用。卡片内置有硅片，可以存储数据和/或进行计算。芯片可以接触读卡器（接触式智能卡），也可远距离与读卡器互动（即非接触式或感应智能卡，其所采用的技术与感应卡和近距型卡的技术相同），从而实现与读卡器的数据交换。芯片的直径约一厘米，它不一定要装在卡片上，而是可以附带在带照片身份卡上，安装在钥匙链里，或者纽扣或首饰上（比如 iButton®）。携带这种芯片的物体从术语上讲一般称作“智能媒体”。

智能卡为门禁提供极大的灵活性。比如，芯片可以被安装在老式卡片上与已有系统完全整合，或者可以将持卡人的指纹或虹膜扫描数据保存在芯片以供读卡器进行生物特征验证——从而将识别水平从“您有什么”提高到“你是谁”。非接触式智能卡支持“近距”读取，可以最大程度的方便用户：卡片无需取出钱包，瞬间即可完成读取工作。

小键盘和密码锁：“你知道什么”

小键盘和**密码锁**被广泛应用于门禁系统。它们非常可靠，而且属于用户友好型技术，但是其安全性有限，因为密码容易被告知和破解。它们采用和手机一样的按钮，用户通过按钮输入代码——如果每个用户拥有自己的唯一代码，那么可以称之为个人访问代码（PAC）或者个人识别代码（PIN）。小键盘通常可以接受大量不同代码，每个用户一个；密码锁通常只有一个密码供所有用户使用。定期修改密码可以提高小键盘和密码锁的安全性，这需要系统能够通知用户并散发新密码。密码锁如果不修改密码则在按钮上出现明显磨损痕迹时间定期更换键盘。和门禁卡一样，小键盘如果结合生物识别来确认用户身份，其安全性得到提高。

生物识别：“你是谁”

生物识别技术目前发展很快，并且越来越成熟，价格也越来越便宜。高可靠性且价格合理的生物识别技术 — 特别是指纹识别 — 正逐渐成为安保解决方案的主流技术。许多供应商现在可以提供种类繁多的生物识别装置供用户选择，当生物识别技术与传统的“你有什么”和“你知道什么”安保方法结合使用时，可以使现有安保措施得到最优化。

生物识别技术一般通过与用户数据库的信息搜索匹配完成身份识别，但是不用先使用“你有什么”或“你知道什么”安保措施，然后再验证结果 — 比如，先使用门禁卡/PIN 码，然后用指纹扫描仪验证结果。随着生物识别技术的性能和可靠性的提高，它现在已经成为可以独立使用的身份识别技术，无需携带卡片或记住密码。

生物识别技术的故障主要有两个：

- *错误拒绝：*无法识别合法用户。虽然有人会争辩说这样可以高度保证受保护区域的安全，但是合法用户因为扫描仪无法识别他们而不能进入安全区域，也是让人无法忍受的错误。
- *错误准入：*识别发生错误，或者是将一个用户认作另一个用户，或者是将非法用户认作合法用户。

>为什么不只使用生物识别技术？

问：如果入口既使用了门禁卡，PIN 码又使用了生物识别技术，既然生物识别技术如此可靠，为什么不干脆只使用生物识别技术呢？

答：因为（1）如果需要在数据库里扫描大量用户而不是单个用户，生物识别的处理时间不在可接受的范围内（2）如果数据库内不只一个用户，生物识别可能出现错误拒绝和错误准入的情况，结合其它安保方法使用，可以降低这种风险。

虽然生物特征几乎不可能被伪造，但这种技术存在匹配错误的风险。

错误率可以通过调节匹配精确度临界值（“精确度达到多少可以被接受”）进行调整，但是一个错误率降低了，另一个错误率又会增加。

在选择生物测量技术时需要考虑的因素包括设备成本、错误率（错误拒绝和错误准入）、用户可接受程度，即可感知的干扰程度，不方便性，或者危险性。比如，视网膜扫描仪的用户可接受程度通常较低，因此眼睛需要靠近扫描仪至 1-2 英尺的位置并接受 LED 光源的照射。

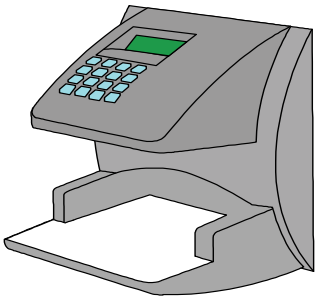

图 3

手部扫描仪

其它安保系统要素

安保系统设计的重点在于放在入口处对人员个体进行识别和筛选的装置，即“门禁”。如果识别可靠性能达到 100%，人员的进入意图安全可信，并且墙壁、门窗、锁具和天花板牢不可破，那你将无任何后顾之忧。但是鉴于自身缺陷或恶意皮坏，事情往往并不能如此完美。因此，安保系统一般还需要结合其它保护、监控和灾备等措施一起发挥作用。

楼宇设计

当新建一处设施或翻新原有设施时，物理安全可以彻底重新做起，综合利用建筑和施工措施预防或阻止恶意行为。在建筑的结构和布局方面，安保需要考虑的事项主要与潜在的进入路线和离开路线以及进入关键物理基础设施的通道有关，比如 HVAC 和布线，还有就是可供恶意进入者藏身的场所。请参见附录罗列了一些相关设计考虑因素。

伴随和尾随：双门互锁装置

门禁系统的一个常见的漏洞是未经授权人员可能会跟在一名得到授权人员的后面从检查点进入安全区域。（如果获得授权的人员知情，这种行为称之为“**伴随**”，即，他会帮助开门；如果获得授权的人员不知情，则称为“**尾随**”，即未经授权人员趁人不察时悄悄溜入）。传统的解决方案是一种气闸式的双门互锁装置，叫做“**捕获装置**”，上面分别安装了入口门和出口门，两扇门之间的空间只能容纳一个人。双门互锁装置可在入口门和出口门都设置门禁，或者只在出口门设置门禁。这种情况下，如果无法从这个装置中出去，入口门也会锁闭，同时装置会发出警报，通知未经授权的闯入者已经被控制。此外还可以安装专门的脚印探测地坪，以确认一次只有一个人通过。

现在已经开发出一种解决这个问题的新技术，即在天花板上安装摄像头，在人员通过检查点时进行跟踪和标记，一旦发现一次通过多人的情况就会发出警报。

摄像监控

固定摄像机可以用于在车辆驶入点记录汽车牌照，或者结合脚步感应器使用以记录关键位置的进出人员。

闭路电视（CCTV）摄像机，采用暗装或明装可以提供内部或外部监督、发挥威慑作用以及在发生事故后进行追溯检查。摄像机的种类多样，包括有固定式，旋转式或远程控制。在安装摄像头时需要注意的一些事项：

- 摄像机画面里的人是否需要清晰可辨？
- 是否只需要确定房间内有没有人？
- 是否需要能够监督资产有没有被搬走？

- 摄像头是不是只需要发挥威慑作用？

如果 CCTV 信号存有记录，那么就以下事项制定相应程序：

- 录影带如何编号和分类以便检索查看？
- 录影带在现场内保存还是在现场外保存？
- 谁有权接触这些录影带？
- 使用这些录影带需要办理什么手续？
- 录影带需保存多久才能被销毁？

目前正在开发一种新技术，它可以自动完成之前由保安进行的工作 — 观看 TV 监控器 — 即使用软件探测屏幕上的图像变化（活动）。

安保警卫

就物理安全而言，除运用先进技术外，专家们认为高素质的警卫团队是为门禁系统提供支持和补充的最佳手段。安保警卫人员可以充分利用所有感官进行安全监督，同时还能够运用智慧灵活应对和处理可疑、异常或灾难性事件。

国际保安基金会（IFPO）是一个非盈利组织，旨在促进保安人员的培训和认证。他们的《保安培训手册》可作为保安及其雇主的参考指南。

传感器和告警器

我们每个人都熟悉传统的房屋和建筑警报系统及其传感器 — 动作传感器，热量传感器，接触（闭门）传感器等等。数据中心警报系统可能还会使用其它种类的传感器 — 激光传感器、脚步传感器、触摸传感器和振动传感器。数据中心内的一些区域可能会选用静音告警器而不是发声传感器以便抓获作案中的犯罪份子。

如果传感器联网，它们可由管理系统远程监控，也包括来自门禁装置的个人活动数据（参见之前的**安保系统管理**章节）。

访客

安保系统设计时必须考虑如何处理访客。一般的解决方案是发放可进入低安全级别区域的临时胸牌或通行卡并在陪同下进入高安全级别区域。如果使用双门互锁装置（防止两个人使用同一授权通过入口），则需要提供临时证或提供访客证才能通行。

人为因素

技术不能自行完成所有工作，特别是一些最好由人来完成的工作：评估人员身份和意图。人是安保问题的一个重要成因，同时人也是解决方案中不可或缺的要素 — 容易出错的特性使我们即是最薄弱的安保环节，但是同时人的智慧也能够为安保提供最强大的支持。

人员：最薄弱的环节

除了错误和事故，人类天性中的友好和信任也伴随着固有的风险。一个你认识的人进入设施，而他/她可能是心怀不满的员工或者有所企图；因为是熟人所以违反规定或跳过程序可能会造成灾难性的后果；安保失效的主要形式之一就是“内部人员作案”。即使是陌生人有时也能成功越过安保防线 — 他们往往非常狡猾聪明，擅长利用诡计和欺骗手段来获取通行，它还有正式称呼

“**社交途径**”。安全保护区域的人员应当接受相关培训，不仅针对操作和安保规则，还应了解如何抵御层出不穷的通过人际交往进行突破的手段。

人员：最强大的支持

安全防护措施往往被意外因素所干扰，任何技术手段都不如保持高度警惕的人可靠。如果时刻警惕被操纵利用并且坚决不走捷径，这样的人对安保来说将是技术之外的无价补充。

除了保持警惕性之外，工作人员的眼睛、耳朵、大脑和灵活性也非常有用，因此人是安保计划中不可忽略的要素之一。传统的警卫人员。在入口设置门卫以及在物业和建筑内设施巡逻岗，虽然花费较贵，但可以在安保技术手段发生故障或被入侵时提供保护。警卫人员在感到“事情不妙”时的快速反应可能是抵抗潜在安保的最后防线。

在防止意外和蓄意伤害方面，警卫人员的贡献也同样重要：时刻保持警惕并且严格遵守规章制度。只允许相关人员进入设施，工作人员均经过完善培训，遵循预定规则和程序是一个有效物理安全系统最后的“防火墙”。

选择合适的解决方案：风险承受能力 vs.成本

恰当的安保系统是可以想到的最佳折中方案，它应当能够尽可能的平衡因人员误入而引起的风险和潜在的损坏与安保措施的成本和繁复程度之间的关系。

安保违规的潜在成本

尽管每个数据中心都有其独特的特点，加上可能受损失的具体情况也各有不同，大部分的数据中心还是都需要考虑以下几点：

- *物理损失* — 意外，蓄意破坏或盗窃对房间和设备的损害。
- *IT 生产力损失* — 设备维修或重置，数据重建或清理系统问题时会分散工作人员对主要工作的注意力
- *公司业务损失* — 由于宕机造成业务中断
- *信息损失* — 数据丢失，被误用或盗窃
- *声誉和客户好感度损失* — 严重或反复安保失效的后果：业务损失、股价下滑、涉诉。

安保系统设计中的考虑事项

安保系统设计需要考虑许多变量，非常复杂。虽然安保系统设计的具体策略不在本白皮书的讨论范围内，但是任何设计方案都需要考虑以下事项：

- *设备成本* — 预算限制通常会使选用昂贵的高保密级别识别设备受到限制。通常的解决办法是针对不同的安保级别选用相应保密级别的的技术。
- 多种技术结合使用 —对于任何安保级别的区域，结合使用低成本技术都可以提高识别结果的可靠性。最内层的安全区域可以受益于所有同心外层区域的技术保护。
- *用户接受程度* —（“损害”因素）。识别技术的简单易用和可靠性非常重要，这可以避免让安保系统成为制造麻烦的源头或者让人认为有机可乘。
- *可扩展性* —设计是否可以根据需要，投入成本和技术的安全等级进行扩展?

> **>花钱不一定就能解决问题**
>
> 即使成本不是问题，盲目在设施内布置最先进的安保技术，大多数情况下，其结果往往是不受认可，生硬和繁琐。每个受保护的区域都应当实事求是地根据该区域内有什么以及什么人需要进入该区域评估其具体的安保需求。

- *逆向兼容性* — 新设计是否可以与旧系统中的已有要素兼容？保留使用全部或部分现有系统可以极大降低部署成本。

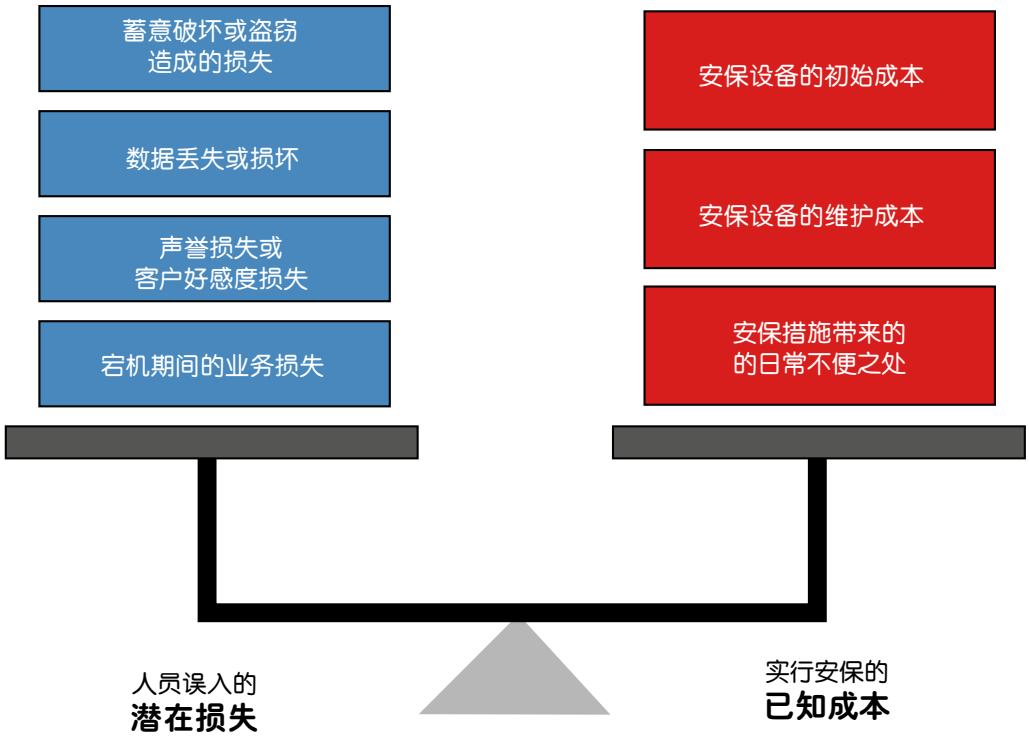

图 4

潜在损失和已知安保成本之间的平衡

结论

随着数据中心和托管服务设施的不断增加，设施的物理安全需求变得和网络计算机安全需求一样强烈和迫切。伪造身份或有所企图的闯入者可能造成巨大的破坏，比如破坏关键物理设备或者攻击软件。即使正常工作人员的普通失误也对数据中心的运行存在威胁。控制这些风险的办法就是尽量只让相关人员在安全控制区域内进出。

基于“**你有什么**”，“**你知道什么**”和“**你是谁**”的识别原则，我们可以综合运用各种技术，在优化成本的基础上，构建各种不同的解决方案。通过风险接受度评估以及对门禁要求和可用技术的综合分析，我们可以设计出在保护力度和成本之间力求平衡的有效安保系统。

关于作者

Suzanne Niles 是施耐德电气数据中心科研中心的高级战略研究员，加入数据中心科研中心之前，Suzzane 在卫斯理女子学院（Wellesley College）从事数学方面的研究，而后 在麻省理工学院（MIT）获得计算机科学学士学位，并发表关于手写输入识别的毕业论文。Suzzane 拥有超过 30 年针对不同阶层听众，包括上至软件说明书，摄影图片，下至儿歌的多元化的教学经验。

资源

点击图标打开相应参考资源链接

数据中心设施选址
第 81 号白皮书

浏览所有 白皮书
whitepapers.apc.com

浏览所有 TradeOff Tools™ 权衡工具
tools.apc.com

联系我们

关于本白皮书内容的反馈和建议请联系：

数据中心科研中心
DCSC@Schneider-Electric.com

如果您是我们的客户并对数据中心项目有任何疑问：

请与您的 **施耐德电气**销售代表联系

附录

建筑设计中需要考虑的安保事项

当新建一处设施或翻新原有设施时，物理安全可以彻底重新做起，综合利用建筑和施工措施预防或阻止恶意行为。在建筑的结构和布局方面，安保需要考虑的事项主要与潜在的进入路线和离开路线以及进入关键物理基础设施的通道有关，比如 HVAC 和布线，还有就是可供恶意进入者藏身的场所。请参见附录罗列了一些相关设计考虑因素。

资源连接
第 81 号白皮书
数据中心设施选址

设施选址时需要考虑的安保事项，请参见第 81 号白皮书《数据中心设施选址》。

- 数据中心门的位置应当巧妙设计，仅供授权人员靠近。
- 使用钢制门和门框，利用实心门代替中空门。确保门的铰链或合页不能从外面被拆除。
- 数据中心的墙壁应当使用比一般内墙板更坚固的材质。感应器应当埋入墙体内，以探测恶意行为。
- 用作数据中心的房间不能邻接外墙。.
- 门卫室或数据中心内的摄像头应当确保视线监控范围大且清晰。.
- 设置障碍物，确保从外面不能看见入口或者其他敏感区域。这样做可以防止恶意人员从远处窥察建筑的布局或安保措施。
- 注意通风管、维修通道、货梯以及其它可能的开口位置，确保其不会被恶意人员用作进入安全区域的途径。所有宽度超过 30 厘米的开口都应安装防护格栅以防止恶意人员进入。
- 避免创造能够供人或物隐藏的空间。比如，高架地板下面的空间就容易被用作隐蔽场所。确保所有潜在隐藏位置都经过安保处理，并且不会被经过设施的人员轻易发现。
- 屋顶上所有可被闯入的位置都必须安装锁和门告警器，以便有人试图闯入时可以立即发出告警。尽量不要在屋顶设置入口。.
- 留意所有外部水管、电线、HVAC 管路等，并提供相应的保护。如果不部署保护措施，恶意人员无须越过安保措施即可破坏这些基础设施。
- 切断接触设施内的电线、水管和通风管的路径。即使您的数据中心得到了彻底的保护，如果恶意人员在走廊里行走就能找到通往电力电缆和数据电缆的途径，数据中心也将处于危险中。
- 无论翻新现有设施还是在已有建筑内新建数据中心，都应当仔细考虑位置布局。注意避免选择易受攻击的位置或者人为风险大的位置。比如，避免将数据中心设置在厨房、大型生产设备、停车场或者人流量或车流量大的位置的下方或附近。厨房起火、汽车炸弹、交通事故等等，这些都可能造成威胁。
- 用防弹玻璃包围中央安保监控台，保护其不受损害。
- 如果数据中心位于单独的建筑内，请注意建筑的外墙上应当保持素净。不要使用识别标记，比如公司名称或标识，那样会暗示数据中心就在里面。
- 使用混凝土路障或其它障碍物防止未经许可的车辆靠近建筑，将其挡在规定距离之外。

术语表

文中用**粗体字**显示的术语定义如下。

门禁

利用自动化设备读取物体上的信息，比如卡片（**你有什么**），接收代码或密码（**你知道什么**）或通过生物分析识别身体特征（**你是谁**），从而人员进入建筑、房间和机柜以及使用键盘和设备。

入口

安全区域边界上的一处位置，装有门或者一些**准入**措施，用于筛选试图进入该区域的用户。

可用性

网络的“正常运行时间”百分比。对于关键任务设施来说，目标是达到 99.999%——相当于每年的宕机时间少于 5 分钟。

条码卡

一种使用条码存储信息的**门禁**卡；在读卡器上刷卡读取信息。

钡铁氧体卡

一种利用磁点图案存储信息的**门禁**卡；将卡平放在读卡器上读取信息。也称作“磁点卡”。

生物识别锁

由生物识别扫描仪控制的锁。

生物识别技术

利用身体或行为特征识别人员身份的技术，比如指纹。

密码锁

以特定顺序按键开启的锁具。不同于**编码锁**，它只有 4-5 个按键的，每个按键只能按一次。密码锁使用金属按键，是今天采用类似手机键盘的电子编码锁的先驱，

编码锁

在键盘上输入代码进行开启的锁。

接触式智能卡

必须与读卡器接触的智能，与其相对的是**非接触式智能卡**。

非接触式智能卡

智能卡使用 **RFID** 技术，因此无需接触读卡器也能使用。根据所使用的 RFID 标准的不同，与读卡器的最大距离分别为 10 厘米/4 英寸（**感应卡**）或者 1 米/3 英尺（**近距型卡**）。

安保纵深

层层相套的安保分区，各区采取不同或严格程度不断渐进的门禁规则。内层区域既受本区域门禁规则的约束，同时也受外围区域门禁规则的约束，必须先进入外层区域才能进入内层区域。

面部几何识别

可通过生物识别技术测定的身体特征之一，例如眼睛、鼻子和嘴巴的相对位置。

错误准入

在生物识别中，将不在数据库中的某人误认的结果。它是两种生物识别出错的其中一种；另一种是**错误拒绝**。

错误拒绝

在生物识别中，无法识别数据库中已知人员的结果。它是两种生物识别出错的其中一种；另一种是**错误准入**。

FAR

*错误准入率。对一台生物识别装置来说，**错误准入**的发生率。*

FRR

*错误拒绝率、对一台生物识别装置来说，**错误拒绝**的发生率。*

手部扫描

一种测量手部三维几何图形的生物识别技术 — 手指的形状和手的厚度。

iButton®

一种与**智能卡**中所用芯片类似的微型芯片，但是它装在一个直径约半寸的圆形不锈钢纽扣内，可以别在钥匙链或首饰上。iButtons 非常坚固耐用，但是（截止 2004 年 5 月）还不能结合 **RFID** 技术支持非接触式应用。

IFPO

国际保安基金会。它是一个非盈利组织，旨在促进保安人员的培训和认证。他们的《保安培训手册》是保安及其雇主的参考指南。

红外阴影卡

门禁卡的一种，塑料夹层间有一组条形码。读卡器向卡片发射红外光，另一侧的感应器就会读取到卡上条形码的阴影。

虹膜扫描

一种测定眼睛虹膜色素分布的生物识别技术。

安保等级

安全保卫的范围，从低到高，以叠层的安全分区为例 — 最外层的区域安保等级最低（比如建筑入口），最内层的区域安保等级最高（比如机柜通道）。

磁条卡

门禁卡的一种，利用磁条存储信息；刷卡以便读卡器读取上面的数据。

可管理性

可被远程监控。可管理的**门禁**装置能够与远程管理通信以促进监督（出入人员及其相应时间），控制（让设备在特定时间允许特定人员进入），和发出告警（通知有人在验证失败后重复尝试进入该区域或设备故障）。

管理

与远程装置进行自动化通信以促进监督、控制和发出警报。传统的叫法是“楼宇自动化”或“住宅自动化”，新的术语“管理”表达的是数据中心内所有元素基于网络的通信，包括 IT 设备本身（服务器、存储装置、通信装置、和网络设备）以及物理基础设施（电源、制冷、消防、和安保）。

捕获装置

一种气闸式的双门互锁装置，上面分别安装了入口门和出口门，两扇门之间的空间只能容纳一个人。它主要是解决安保漏洞 —“伴随”或“尾随”，即未经授权人员跟随授权人员通过门禁进入安全区域。

DCPI

数据中心物理基础设施。确保数据中心物理基础设施（不同于 IT 基础设施，比如路由器和存储管理器）保持不间断运行，可以直接有助于提高**可用性**。DCPI 包括电源、制冷、消防和**物理安全**。

知道必要性

这是非常高级的安保等级，针对由于特殊和即时需求而要进入安全区域的人员（比如，存取数据）发放准入许可，但仅在该需求存在期间有效。

数据中心物理基础设施 — 参见 DCPI

PAC

*个人存取代码。PIN（个人识别码）的别称——一组用于在**入口处**识别用户的代码或密码。*

物理安全

保护物理设施免受未经授权人员或恶意人员造成的意外事故或蓄意破坏的影响。物理安全系统通常包括入口处用于自动化筛选的门禁装置，加上基于感应器的警报系统。其它保护可能还包括摄像头监控和门卫。（物理安全有时还涉及更广，包括防止各种物理伤害，比如天气、地震和爆炸）。在本白皮书中，物理安全仅限于防止未经授权人员进入设施后引起麻烦。）

伴随

一种安全违规行为，授权人员开门后有意让未经授权人员跟随他/她通过检查点。（类似的违规行为还有“**尾随**”，未经授权人员趁授权人员不察时尾随其通过检查点。）

感应卡

一种装有 **RFID** 发射器/接收器的**门禁**卡，可以在最远 1 米（3 英尺）外于读卡器交换信息。

感应智能卡

一种在芯片里采用 **RFID** 技术的**智能**卡，因此它可以在最远 10 厘米（4 英寸）外与读卡器交换信息。因此也称作**非接触式智能卡。**

视网膜扫描

一种测定视网膜内血管分布的生物识别技术。

RFID

*无线射频识别。*无需物理接触，即可完成卡与读卡器之间信息通信。RFID 技术是感应卡、近距型卡和非接触式智能卡得以实现的基础。RFID 芯片由读卡器内的电磁场驱动，因此无需电池。

智能卡

一种在微型芯片内存储信息的**门禁**卡。芯片不仅存储数据，而且可以进行计算并且与读卡器交换数据。卡片需要接触读卡器才能读取。另请参见**非接触式智能卡**。

智能媒体

含有与**智能卡**所用芯片相同芯片的小物件，可以为任何形状。智能媒体一般为小物件（**证件**），可以挂在钥匙链上或别在首饰上。

社交途径

运用诡计和欺诈手段让人放松安全警惕性 — 比如，透露密码，出借钥匙或开门。

尾随

一种安保违规行为，未经授权人员在授权人员开门时趁其不察跟在后面溜过检查点。（类似的违规行为还有**伴随**，即授权人员作为同谋，有意打开门让未经授权人员通过）。

模板

在**生物识别技术**中由对扫描结果的计算转换而来 — 模板对个人来说仍然具有唯一性但是占用的存储空间小得多。在**入口处**用于与现场扫描结果进行比对的是模板，而不是存储在用户数据库或**智能卡**芯片上的原始扫描结果。

阈值

在运用**生物识别技术**时，这是一种可供用户调整的参数，它能够帮助调节生物识别的错误率（**错误准入**和**错误拒绝**）。由于它代表“精确度达到多少可以被接受？”，一种错误率下降，另一种错误率就会自动提高。

凭证

一种带有微型芯片的小物件，芯片上写有您的个人身份信息。证件可以接触读卡器进行读取，如果具备 **RFID** 功能，还可以在一定距离外读取。

近距型卡

一种安装有 **RFID** 发射器/接收器的**门禁**卡。它可以在最多 1 米（3 英尺）外与读卡器通信。

声纹

一种在**入口处**利用用户声纹数字模板与用户现场讲话进行对比的**生物识别技术**。

韦根卡

一种采用特制和磁化内置电线的**门禁**卡，电线上携带有信息；刷卡读取。

你有什么

在**门禁**系统中，基于你所持有的物件进行身份识别的门禁方法，比如卡片或**凭证**。它适用于最低等级安保识别，因为不能保证用于识别的物件被正确的人使用。

你知道什么

在**门禁**系统中，基于你所知道的信息进行身份识别的门禁方法。它比“**你有什么**”更安全，但是仍然可能被他人盗用或者记录和破解。

你是谁

在**门禁**系统中，基于您的生物或行为特征进行身份识别的门禁方法。它是最安全的身份识别办法，因为很难伪造，比如身体特征。但是，这种方法也不是 100%可靠，它存在读取或判断风险。这种门禁方法的另一种叫法是“**生物识别**”。