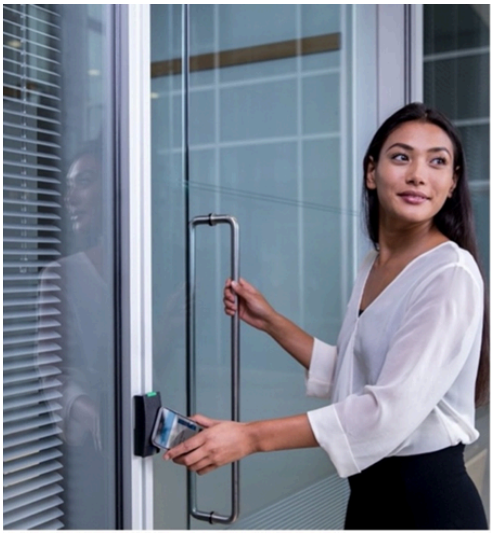
The Basics of Physical Access Control

By Anjanette Brennan, Director, End User Business Development, HID

The Purpose of Physical Access Control Systems



Before we dive into the basics of physical access control systems, let's start with their purpose. It's essential to recognize the pivotal role that this type of security technology plays in enhancing security measures while offering a higher degree of adaptability and accountability compared to traditional physical keys.

At its core, a physical access control system (PACS) is installed to monitor and enforce physical security, preventing unauthorized access to specified areas within a building or its premises. However, in today's security environment, the dynamic nature of these systems allows it to do so much more.

While its primary function is to prevent the wrong people from getting into a restricted space, it is also used to make sure that the right people can get in. Compared to a physical key, PACS allows for quick and secure changes to things like access levels. Using the backend of the system, designated system administrators can quickly add or revoke access to doors following employee changes or in response to lost or stolen credentials. So, if someone's role changes, for example, permissions associated with their credential (whether a smart card, key fob, or mobile device) can be easily changed as well.

In addition to managing access levels, administrators can also use these systems to identify what is happening within their building. These events, alarms, or transactions, denoted by phrases like "Access Granted" or "Door Forced Open," allow teams to keep a running log of activity while identifying potential threats. Administrators can run reports on these transactions and filter these reports based on transaction type, location, specific individuals, and timeframes, to facilitate a comprehensive overview of system activities and access events.

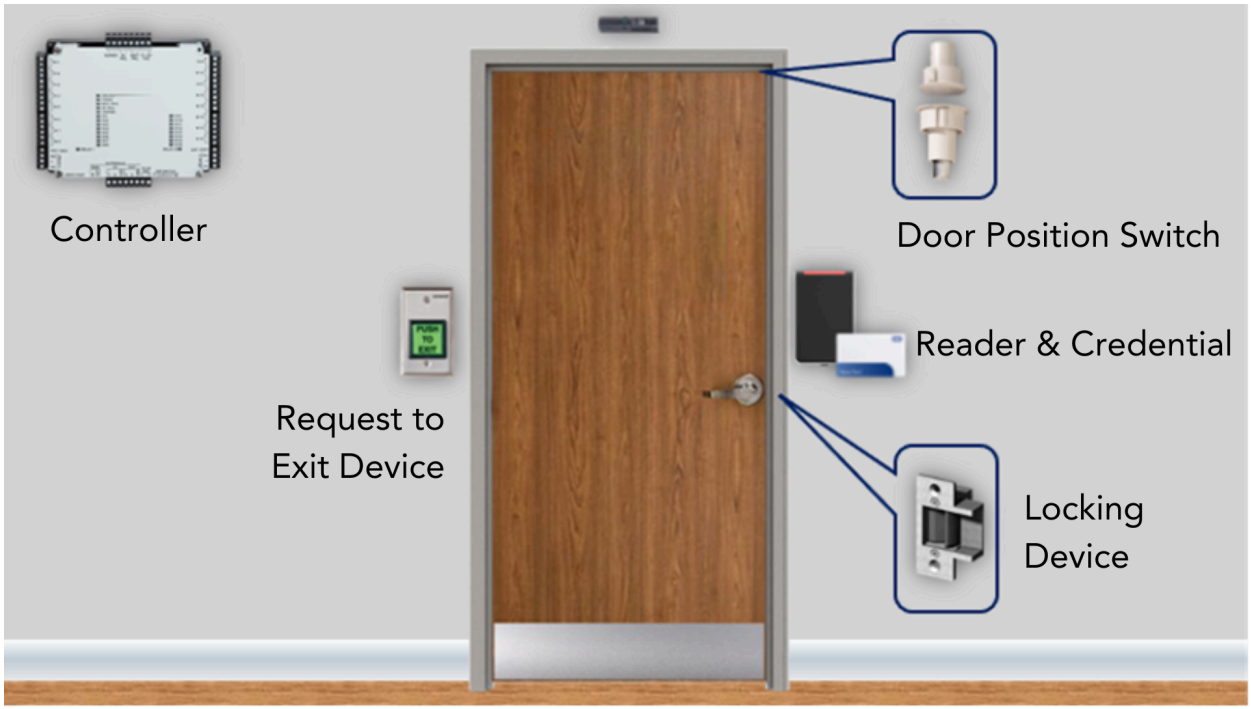
Overview of Physical Access Control Components

A basic physical access control system includes a credential, a reader, a locking device, a door position switch (DPS), a request to exit (RTE) device, and a controller.

Credentials

Credentials refer to the physical or digital items used to verify and grant access to secure areas, systems, or information. They work by authenticating the identity of the individual seeking access against pre-registered data within the access control system. This process verifies the person's identity and permissions to determine if they are allowed entry. There are various types

of credentials used in access control systems, including smart cards, key fobs, and mobile credentials.



Readers

Readers come in many different form factors such as card readers, USB readers, keypad readers, two-factor or multi-factor authentication readers, and biometric readers (such as fingerprint readers).

The purpose of the reader is to gather information from a presented credential and send that data to a controller to determine whether access should be granted or denied. Regardless of the format, when a credential is presented to a reader, credential data is transmitted as a string of ones and zeros from the reader to the controller. The controller then provides the person with access if the credential has permission to access that door at that time.

Locking Devices

Locking devices, such as electric strikes or magnetic locks, physically secure doors and grant or restrict access based on commands received from the controller.

Door Position Switches (DPS)

Door position switches or sensors provide real-time indications of whether the door is open or closed and is located within the door frame.

Request to Exit Devices (RTE)

Request to exit devices, such as motion sensors or push bars, allow individuals to exit a secured area easily while ensuring the door remains secure from the outside.

Controllers

The controller in an access control system is a critical component responsible for managing and overseeing various functions that ensure the security and proper functioning of the system. The controller makes real-time decisions regarding granting or denying access to specific areas or resources. It enforces access control policies defined within the system, including user permissions, time-based access restrictions, and visitor access rules. A controller can be connected to one or multiple sets of door components.

Several devices can be wired to an access control system controller for proper functioning. These devices include:

- Readers — Proximity readers, smart card readers, biometric readers, keypad readers, etc.
- Door Locks — Electric strikes, magnetic locks, or other locking mechanisms that can be controlled by the access control system
- Exit Buttons — Devices that allow individuals to exit a secured area by triggering the door release mechanism
- Sensors — Motion detectors, door position switches, and other sensors used for monitoring and security purposes

Controllers communicate with connected devices via wired or wireless connections. Wired connections typically include Ethernet, RS-485, or Wiegand protocol for data transmission between the controller and devices. Wireless technologies like Wi-Fi, Bluetooth®, Z-Wave, or Zigbee can also be used for communication, depending on the system design and requirements.

The controller in an access control system often requires software for configuration, user management, access control policy setup, reporting, and monitoring. The software used to manage the access control system interfaces with the controller to manage access rights, review access logs, and make changes to the system settings. The software may be installed on a computer or accessed through a web interface, depending on the system's design.

An example of a specific configuration that may be programmed between the software and controller is called public access - when the building entrance doors are to be unlocked during normal business hours. In these instances, the controller will unlock the entrance doors at the beginning of the business day, and lock them at the end of the day, after which access is only granted by presenting a valid credential.

Other Critical Components

All physical access control systems installations require a physical access control systems application, a database and a graphical user interface (GUI) used to configure and monitor the system. In a small system, these components may be hosted on a single machine, whereas a large enterprise-wide physical access control system might have servers distributed across multiple countries.

System Integrations

Access control systems can be integrated with various technologies and have a range of features to enhance security, efficiency, and convenience in different environments. Some

common integrations and additional functionalities that can be implemented with access control systems include video surveillance, intrusion alarms, event notifications and alerts, visitor management, building management systems, and reporting analytics. By integrating access control systems with these additional capabilities, organizations can create robust security solutions tailored to their specific requirements, enhance operational efficiency, and maintain a safe and secure environment for their facilities.