Conceptos básicos del control de acceso físico

Por: Anjanette Brennan, Directora de desarrollo empresarial para usuarios finales, HID

El propósito de los sistemas de control de acceso físico

Antes de profundizar en los conceptos básicos de los sistemas de control de acceso físico, comencemos por su propósito. Es esencial reconocer el papel fundamental que juega este tipo de tecnología de seguridad en el fortalecimiento de las medidas de seguridad, al mismo tiempo que ofrece un mayor grado de adaptabilidad y responsabilidad en comparación con las llaves físicas tradicionales.

En esencia, un sistema de control de acceso físico (PACS) se instala para monitorear y garantizar la seguridad física, impidiendo el acceso no autorizado a áreas específicas dentro de un edificio o sus instalaciones. Sin embargo, en el entorno de seguridad actual, la naturaleza dinámica de estos sistemas les permite hacer mucho más.

Si bien su función principal es evitar que personas no autorizadas ingresen a un espacio restringido, también se utiliza para garantizar que las personas autorizadas puedan ingresar. En comparación con una llave física, el PACS permite realizar cambios rápidos y seguros en aspectos como los niveles de acceso. Mediante la parte oculta y en segundo plano (backend) del sistema, los administradores designados pueden agregar o revocar rápidamente el acceso a las puertas tras cambios en el personal o en respuesta a la pérdida o robo de credenciales. Así, si cambia el rol de alguien, por ejemplo, los permisos asociados a su credencial (ya sea una tarjeta inteligente, un llavero electrónico o un dispositivo móvil) también se pueden modificar fácilmente.

Además de gestionar los niveles de acceso, los administradores también pueden utilizar estos sistemas para identificar lo que está sucediendo dentro de su edificio. Estos eventos, alarmas o transacciones, indicados por frases como “Acceso concedido” o “Puerta forzada”, permiten a los equipos mantener un registro actualizado de la actividad al mismo tiempo que identifican posibles amenazas. Los administradores pueden generar informes sobre estas transacciones y filtrarlos según el tipo de transacción, ubicación, personas específicas y períodos de tiempo para facilitar una visión general completa de las actividades del sistema y los eventos de acceso.

Descripción general de los componentes de control de acceso físico

Un sistema básico de control de acceso físico incluye una credencial, un lector, un dispositivo de cierre, un sensor de puerta (DPS), un dispositivo de solicitud de salida (RTE) y un panel de control.

Credenciales

Las credenciales son los elementos físicos o digitales que se utilizan para verificar y otorgar acceso a áreas, sistemas o información. Funcionan autenticando la identidad de la persona que solicita el acceso comparándola con los datos pre-registrados en el sistema de control de acceso. Este proceso verifica la identidad y los permisos de la persona para determinar si se le permite el ingreso.

Existen varios tipos de credenciales que se utilizan en los sistemas de control de acceso, entre ellas las tarjetas inteligentes, los llaveros electrónicos y las credenciales móviles.

Lectores

Los lectores se presentan en diversos formatos, tales como lectores de tarjetas, lectores USB, lectores con teclado, lectores de autenticación en dos fases o multifactor y lectores biométricos (como los lectores de huellas dactilares).

El propósito del lector es recopilar información de una credencial presentada y enviar esos datos a un panel de control para determinar si se debe otorgar o denegar el acceso. Independientemente del formato, cuando se presenta una credencial ante un lector, los datos de la credencial se transmiten como una cadena de unos y ceros desde el lector al panel de control. Después, el panel de control otorga acceso a la persona si la credencial tiene permiso para acceder a esa puerta en ese momento.

Dispositivos de cierre

Los dispositivos de cierre, como los cerrojos eléctricos o las cerraduras magnéticas, aseguran físicamente las puertas y otorgan o restringen el acceso según las órdenes recibidas del panel de control.

Interruptores de posición de puertas (DPS)

Los interruptores o sensores de posición de puerta proporcionan indicaciones en tiempo real sobre si la puerta está abierta o cerrada y se encuentran dentro del marco de la puerta.

Dispositivos de solicitud de salida (RTE)

Los dispositivos de solicitud de salida, como los sensores de movimiento o las barras de empuje, permiten a las personas salir fácilmente de un área segura, al mismo tiempo que garantizan que la puerta permanezca segura desde el exterior.

Paneles de control

El panel de control de un sistema de control de acceso es un componente crítico responsable de gestionar y supervisar diversas funciones que garantizan la seguridad y el correcto funcionamiento del sistema. El panel de control toma decisiones en tiempo real respecto a otorgar o denegar el acceso a áreas o recursos específicos. Hace cumplir las políticas de control de acceso definidas dentro del sistema, incluyendo permisos de usuario, restricciones de acceso basadas en el tiempo y reglas de acceso para visitantes. Un panel de control puede conectarse a uno o varios conjuntos de componentes de puerta.

Se pueden conectar varios dispositivos al panel de control de un sistema de control de acceso para garantizar su correcto funcionamiento. Estos dispositivos incluyen:

- Lectores: lectores de proximidad, lectores de tarjetas inteligentes, lectores biométricos,
- lectores de teclado, etc.
  Cerraduras para puerta: cerraduras eléctricas, cerraduras magnéticas u otros mecanismos
- de cierre que pueden ser controlados por el sistema de control de acceso.
  Botones de salida: son dispositivos que permiten a las personas salir de un área segura al
- activar el mecanismo de liberación de la puerta.
  Sensores: detectores de movimiento, interruptores de posición de puerta y otros sensores utilizados con fines de monitoreo y seguridad.

Los paneles de control se comunican con los dispositivos conectados a través de conexiones cableadas o inalámbricas. Las conexiones cableadas suelen incluir los protocolos Ethernet, RS-485 o Wiegand para la transmisión de datos entre el panel de control y los dispositivos. También se pueden utilizar tecnologías inalámbricas como Wi-Fi, Bluetooth®, Z-Wave o Zigbee para la comunicación, dependiendo del diseño y los requisitos del sistema.

El panel de control de un sistema de control de acceso suele requerir software para la configuración, la administración de usuarios, la configuración de políticas de control de acceso, la generación de informes y el monitoreo. El software utilizado para administrar el sistema de control de acceso se integra con el panel de control para gestionar los derechos de acceso, revisar los registros de acceso y realizar cambios en la configuración del sistema. El software puede instalarse en una computadora o accederse a través de una interfaz web, dependiendo del diseño del sistema.

Un ejemplo de una configuración específica que se puede programar entre el software y el panel de control es el llamado «acceso público», que consiste en que las puertas de entrada al edificio permanezcan desbloqueadas durante el horario normal de atención. En estos casos, el panel de control desbloqueará las puertas de entrada al inicio de la jornada laboral y las bloqueará al final del día; a partir de ese momento, el acceso solo se otorgará al presentar una credencial válida.

Otros componentes esenciales

Todas las instalaciones de sistemas de control de acceso físico requieren una instalación de control de acceso físico, una base de datos y una interfaz gráfica de usuario (GUI) que se utiliza para configurar y monitorear el sistema. En un sistema pequeño, estos componentes pueden estar alojados en una sola máquina, mientras que un sistema de control de acceso físico a nivel de toda gran empresa podría tener servidores distribuidos en varios países.

Integraciones de sistemas

A los sistemas de control de acceso se le pueden integrar diversas tecnologías y además cuentan con una amplia variedad de características para mejorar la seguridad, eficiencia y comodidad en distintos entornos. Algunas integraciones comunes y funcionalidades adicionales que pueden implementarse junto con los sistemas de control de acceso incluyen videovigilancia, alarmas contra intrusos, notificaciones y alertas de eventos, gestión de visitantes, sistemas de gestión de edificios y analítica de informes. Al integrar los sistemas de control de acceso con estas capacidades adicionales, las organizaciones pueden crear soluciones de seguridad sólidas adaptadas a sus necesidades específicas, mejorar la eficiencia operativa y mantener un entorno seguro y protegido en sus instalaciones.