Control de Accesos
Unidades de Control o Controladores

Ing. Luis Cosentino
Consultor Independiente
lcosentino@fibertel.com.ar

Diseñada como una ayuda para técnicos, instaladores y estudiantes, ofrecemos a nuestros lectores una serie de conceptos y fundamentos sobre el control de accesos, sus elementos y funciones. Un detallado estudio de mercado y un ejemplo de diseño son los complementos de esta obra que seguramente será de suma utilidad para nuestros lectores.

Indice

El presente artículo explica las prestaciones de los controladores de control de accesos, tanto los autónomos como los de las placas de sistemas mayores y sus formas de interconexión. De manera general podemos decir que la unidad de control de un control de accesos es una placa autónoma que cumple las siguientes funciones:

- **Almacenar la programación de dicho acceso**
  - Tipo de acceso, ya sea puertas, barreras, molinete, etc.
  - Tiempos y tipos de cerraduras involucradas
  - Manejo de alarmas de puerta abierta o violación.
- **Almacenar la configuración de dicha área**
  - Activación o no de antipassback o rutas
  - Area con cantidad mínima o máxima de ingresos
- **Almacenar la base de datos de las personas habilitadas por esa puerta**
  - Listado de personas con sus bandas horarias (lista blanca)
- **Monitorear en tiempo real el estado del acceso**
  - Puerta cerrada, bloqueada, habilitada, abierta, etc.
- **Tomar la decisión de permitir un acceso o no en función de:**
  - Quien es la persona
  - Que restricciones que posee
  - Las restricciones que posea el acceso por el que pretende ingresar.
  - Las restricciones que posea el área a la cual pretende acceder.
- **Almacenar cronológicamente los eventos que se producen en dicho acceso**
  - Se comunica con un elemento de jerarquía superior, generalmente son programas que corren en PC's, pero también pueden ser concentradores de comunicaciones, para:
- Recibir las programaciones.
- Informar los eventos.

7.1. Tipos de controladores

En el mercado pueden encontrarse básicamente **tres tipos** de controladores, que se utilizan según el tamaño del sistema de control de accesos deseado.

- **Autónomos simples,** generalmente utilizados para controlar una o pocas puertas.
- **De sistemas distribuidos** de muchas puertas.

Continúa en página 136

Viene de página 132

- **Mixtos,** que pueden funcionar para pocas y mediana cantidad de puertas.

7.1.1. Controladores autónomos simples

Estos controladores autónomos son los recomendados para utilizar en sistemas de muy pocas puertas y tienen las siguientes características:

- Generalmente poseen incorporado el lector utilizado para identificar al usuario, por ejemplo un teclado PIN o una lectora de proximidad.
- Reciben en forma local mediante el uso de tarjetas o teclas la programación de las personas autorizadas a ganar el acceso.
- No almacenan eventos ni poseen comunicación con una instancia superior, o sea no se los puede programar por PC's ni generan reportes de eventos.
- Cuando se instalan varios de ellos es necesario dar de alta a la/s persona/s en forma manual en todas las puertas, generando situaciones de incertidumbre sobre la consistencia de la lista blanca luego de un tiempo de usarlos.

Este tipo de controlador se utiliza principalmente por su simplicidad de instalación y su bajo costo.

La forma manual de ingreso de la lista blanca de personas habilitadas no los hace recomendables para accesos de muchas personas (más de 30) porque el mantenimiento de dicha lista es engorroso al no poseer conexión a PC.

Generalmente son de tipo pasa/no pasa y no admiten bandas horarias ni alarmas de puertas abiertas, por lo que cumplen con la sola función de restringir el acceso de manera elemental.

Debe tenerse en cuenta que si van a instalarse en ingresos exteriores, el producto seleccionado debe ser de tipo "potteado" para impedir su desarme desde el exterior.

7.1.2. Controladores de sistemas distribuidos de muchos accesos

Los controles de accesos de múltiples puertas y múltiples sitios se implementan colocando varios controladores, generalmente siguiendo una topología lógica de estrella, donde cada controlador se comunica con un centro de control, en la mayoría de los casos una PC que funciona como servidor del sistema.

Estos controladores guardan una armoniosa relación entre la cantidad de puertas/lectoras que administran con la capacidad de memoria y cantidad de entradas y salidas que poseen. Dicho de otro modo, un controlador que admite un máximo de 5000 tarjetas en su lista blanca almacenará como mínimo 5000 eventos en el caso de que no tenga conexión on line con la instancia superior.

Su funcionamiento es autónomo visto desde el punto de vista del servidor, porque al momento de la configuración éste le cargó a cada controlador la lista blanca de personas habilitadas en cada puerta, las bandas horarias y, como poseen un reloj en tiempo real, son capaces de "decidir" cada situación de acceso, registrándola en su base de datos cronológica de eventos, que oportunamente comunicará al centro de control.

Históricamente la comunicación física entre dichos controladores es mediante RS-485 dentro del mismo sitio y por vía telefónica (módem), radio o TCP/IP entre sitios. Actualmente existe una tendencia a que cada controlador o grupo de controladores de un sitio se comuniquen por TCP/IP con el centro de control, aunque algunos sistemas utilizan las redes de PC ya instaladas.

Estos controladores son totalmente dependientes del centro de control para su configuración y la programación de la lista blanca de personas autorizadas.

7.1.3. Controladores mixtos

Estos controladores cumplen con una característica intermedia entre los anteriores: por un lado poseen la capacidad de programación in situ mediante el uso de tarjetas y/o teclados pero admiten bandas horarias y se comunican con un centro de control para informar los eventos y recibir las programaciones. Esta capacidad facilita el manejo de sistemas intermedios, aunque debe preverse no generar inconsistencias.

Si bien sus prestaciones son similares a las de los sistemas grandes, su capacidad de memoria y/o comunicaciones no, por lo que no se los recomienda para sistemas de más de 20 puertas en un mismo sitio o donde deba controlarse el acceso de 5000 personas.

Si bien suelen ser un poco más costosos que los controladores autónomos simples, combinan las ventajas de su simple funcionamiento, instalación y programación con la posibilidad de las bandas horarias, alarmas y el almacenamiento de eventos. De esta forma, ante un hecho delictivo, es posible leer la base de eventos para reconstruir la situación y contribuir a su esclarecimiento.

7.2. Prestaciones de los controladores

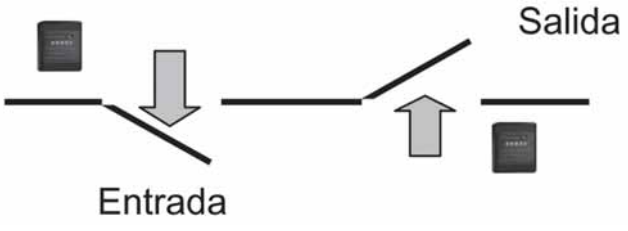
En este apartado se describen las prestaciones más comunes de los controladores de accesos, lo cual no significa que todos los productos del mercado los implementen en su totalidad. Muchas de estas prestaciones están presentes también en controladores mixtos.

En general estas características están relacionadas con hardware o son una combinación de hardware y software. Al final de cada apartado se darán algunos ejemplos de la utilización de estas prestaciones.

7.2.1. Modelos de accesos

Por modelo de acceso se entiende las diferentes acciones que el controlador realizará para administrar un ingreso exitoso, dependiendo del tipo de acceso del que se trate (una puerta, barrera, molinete, etc.). Por ejemplo, si se trata de una puerta podrían utilizarse diferentes modelos según sean las necesidades que se pretendan.

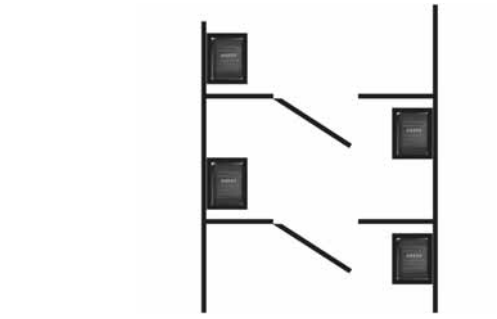
- Puerta con lectora de entrada y de salida (2 lectoras 1 cerradura).
- Puerta con lectora de entrada y botón de salida (1 lectora, una entrada adicional y una cerradura).
- Una misma puerta lógica con lectora de entrada y salida, pero que debido al alto tránsito está implementada con 2 puertas físicas, una puerta exclusiva para el ingreso y otra de egreso (2 lectoras 2 cerraduras).



- Una misma puerta lógica con lectora de entrada y salida conformando una exclusa donde sólo es posible abrir una de ellas por vez (2 lectoras, 2 cerraduras y dos sensores de puerta).

Continúa en página 140

Viene de página 136



Sin dudas todos los controladores soportan los modelos simples de puertas pero casi siempre en sistemas grandes se encuentran accesos complejos, que son los que pueden definir entre un sistema u otro y deben ser analizados cuidadosamente.

Por ejemplo, cuando es necesario resolver una situación en un garaje de un edificio de oficinas con una entrada y una salida pero donde el ingreso está limitado por conjuntos de cocheras libres asociadas a las diferentes oficinas del edificio, deberá seleccionarse un proveedor que soporte este modelo de acceso y, probablemente, esta característica sea definitoria a la hora de elegir el control de accesos para todo el edificio.

7.2.2. Lectoras/puertas, entradas y salidas

Cada modelo de acceso posee una, dos o tres lectoras asociadas (molinete con buzón recolector de tarjetas de visitantes) haciendo difícil especificar a los controladores la cantidad absoluta de puertas, por lo que se los especifica en cantidad de lectoras. Algo similar ocurre con las entradas y salidas asociadas: generalmente se dejan dos entradas y dos salidas por lectora. Como las controladoras son de al menos dos lectoras, se dispone de cuatro entradas y cuatro salidas como mínimo.

Antiguamente, cuando los controladores eran capaces de manejar muchas lectoras (8 o 16), debido a su tamaño se instalaban en tableros o salas dedicadas, por lo que había que cablear distancias considerables desde las puertas (lectoras, cerraduras, sensores de puertas, etc.) hasta esas ubicaciones. Actualmente las controladoras son de menor capacidad (2 a 4 lectoras), más pequeñas y se las distribuye a lo largo de la instalación, tratando de minimizar los cableados.

La mayoría de las lectoras soportan protocolos unidireccionales tipo Wiegand o ABA Track2. Sin embargo algunos controladores soportan protocolos bidireccionales para permitir manejar generalmente displays o biometrías con puertos RS-232 o RS-485.

Una prestación deseable es la cantidad de formatos que soporta la placa controladora, no sólo en lo que respecta a la posibilidad de que el usuario los defina a voluntad sino a cuantos formatos es capaz de manejar simultáneamente.

Por ejemplo, esta última característica es imprescindible cuando se necesita especificar un control de accesos para la planta baja de un edificio de oficinas que alberga a diferentes empresas.

Otro ejemplo se aplica a un cliente que posee su parque de tarjetas de formato estándar (Wiegand 26 bits) y pretende incrementar la seguridad pero no desea reemplazar todas las tarjetas a la vez. Si el controlador admite más de un formato simultáneo, simplemente deberá agregarse la programación del nuevo formato más seguro y a partir de allí se agregar tarjetas del nuevo formato.

7.2.3. Cantidad de memoria y manejo de las bases de datos

La memoria del controlador está definida, en general, por el tamaño de la lista blanca de tarjetas que es capaz de almacenar y los eventos que es capaz de guardar. Muchos fabricantes han optado por utilizar memorias "intercambiables", Compact Flash, SD o similares, para permitirle al usuario "crecer" con la tecnología y al controlador "adaptarse" a las necesidades de memoria requeridas por el usuario.

En términos generales, los controladores almacenan los eventos hasta que se pueden comunicar con el servidor. Dichos eventos se guardan en una lista y cuando ésta se llena, se reescribe el elemento más antiguo para almacenar el último. A esto se lo llama lista circular.

Cuando se utilizan comunicaciones RS-485 el servidor debe interrogar al controlador para solicitarle los eventos almacenados mientras que si se trata de TCP/IP el controlador transmitirá el evento ni bien se produzca. Por lo tanto, en sistemas con controladores TCP/IP y una condición de red donde los nodos están on line la mayoría del tiempo, no hay necesidad de almacenar eventos y este parámetro será muy poco importante, mientras que si la comunicación es RS-485 o por algún motivo sólo existe vinculo con el servidor en forma esporádica, este parámetro deberá ser tenido en cuenta.

Tras este análisis, se descartan aquellos controladores de baja performance que mientras informan sus eventos no pueden continuar administrando los accesos y por esto deben conectarse con el servidor durante la noche.

Un capítulo aparte merece el manejo de la lista blanca en grandes sistemas. Aquí deben tenerse en cuentas dos factores: el algoritmo de búsqueda y el tiempo de actualización de registros. Cuando se trata de sistemas de más de 25 mil usuarios no hay que omitir el análisis de los parámetros antes mencionados. Algunos controladores concebidos como medianos a los que se les expandió la memoria suelen demorar más de lo razonable para liberar el ingreso (un par de segundos), dependiendo de la ubicación de la persona dentro de la lista. Algo similar ocurre cuando se necesitan retirar registros o mucho peor aún cuando se actualiza toda la lista.

Algunos fabricante duplican la memoria asignada a la lista de manera de tener dos listas, la que está en uso y otra de trabajo. Así, ante un cambio se actualiza la segunda y ya con todas las modificaciones realizadas, a través de un comando rápido se intercambia una por la otra.

7.2.4. Entradas y Salidas

Las entradas suelen ser de potencial simple, manejadas por un contacto seco, o supervisadas. En el primer caso sólo es posible saber si la entrada está abierta o cerrada mientras que las segundas permiten, además, saber si están en cortocircuito o fueron cortadas.

Algunos fabricantes permiten definir los umbrales de dichas entradas, para colocar, por ejemplo, sensores analógicos.

Si es necesario manejar la iluminación de un hall de entrada, puede conectarse un sensor de nivel de iluminación (LDR) en una entrada de umbral definible (analógica o supervisada) donde se puede definir el umbral de luz ambiente mínima, de manera que al cambiar el estado lógico se pueda activar una salida para controlar la iluminación artificial.

Con referencia a las salidas, estas suelen ser a relé con contactos secos o "húmedos con capacidad de corriente limitada" configurables. Algunos fabricantes permiten que sus salidas manejen directamente 220VCA mientras que otros restringen la tensión de salida a 24 voltios.

Hay que ser cuidadosos con los dispositivos externos que se alimenten, porque las cargas inductivas o capacitivas ge-

Continúa en página 144

Viene de página 140

neran mucho ruido eléctrico y pueden provocar señales espurias en los controladores, que ocasionan fallas aleatorias extremadamente difíciles de resolver. Para evitar estos inconvenientes se recomienda seguir las directivas de los fabricantes en lo referente a las puestas a tierra y el uso de varistores.

7.2.5. Bandas horarias

Las bandas horarias son intervalos de tiempo a lo largo de un período. La forma más común de definirlas es con una cantidad de bandas diarias, por ejemplo dos bandas (8 a 12 y 13 a 19) combinadas en los diferentes días de la semana. De esta forma es posible aplicarlas para restringir el acceso de manera independiente para cada día de la semana, incluyendo los sábados y domingos.

La cantidad de bandas diarias, semanales y feriados depende de la envergadura del sistema, pero en general disponer de 20 bandas semanales y 20 feriados es suficientes para las aplicaciones de empresas de un solo sitio con doble turno, pese a que la mayoría de los fabricantes ofrecen 255 bandas o más.

Un capítulo aparte merecen los feriados, que se definen por día específico y tienen mayor prioridad que las bandas semanales.

Ejemplo: se pretende impedir el acceso a la empresa el día 9 de julio (asumiendo que este día caiga dentro de la semana laborable) de un empleado administrativo que trabaja de lunes a viernes de 8 a 17. Para ello deberá definir el 9 de julio como feriado, quitar la posibilidad de ingreso y asociarlo a la categoría de empleados administrativos. Así, si el empleado se presenta y pasa su tarjeta por la lectora de entrada, aunque por su horario podría tener acceso, el feriado, que posee una prioridad mayor, se lo denegará.

Otro ejemplo que puede definir el fabricante del control de accesos es la necesidad de manejo de horarios rotativos o aquellos con francos compensatorios.

No hay que confundir asignación de bandas horarias laborales de los empleados con su derecho o no a ingresar a la empresa. Si a un empleado que trabaja de 8 a 18 se le coloca esa banda horaria de acceso, no podrá ingresar a su lugar de trabajo antes de las 8:00 y deberá retirarse antes de las 18, porque sino el sistema no le permitirá hacerlo. Para evitar esto, su banda horaria de acceso deberá comenzar al menos media hora antes y de ser posible deben utilizarse controladores que admitan salida libre. Es decir que aunque la banda sea de 7:30 a 18, el empleado podrá retirarse en cualquier momento y sólo se restringirá su ingreso fuera de dicha banda horaria.

Las bandas horarias se pueden aplicar tanto a las personas como a los accesos. Por ejemplo:

- En el caso de un edificio de departamentos, el personal doméstico por horas puede tener limitado el acceso de lunes a viernes de 8 a 18 y los sábados de 8 a 13. Este es un ejemplo de restricción de horarios por categoría de los usuarios.
- En una fábrica, cierta puerta de acceso puede estar habilitada sólo los días laborales, permaneciendo deshabilitada los sábados por la tarde, domingos y feriados. En este caso, sin importar los privilegios de las personas, será la puerta quien no reconocerá a las tarjetas fuera de la banda permitida. Este es un ejemplo de una restricción horaria para un objeto (la puerta).
- La puerta de ingreso a la sala de servidores de una empresa solicitará solo la tarjeta en la banda horaria laborable y tarjeta y PIN fuera de ella. En esta situación se tiene una lectora con teclado en la puerta de la sala de servidores y el controlador exigirá el ingreso del PIN fuera de la banda horaria laborable para validar el acceso, mientras que dentro de la misma la sola presentación de la tarjeta bastará. Este también es un ejemplo de restricción horaria para un objeto, el teclado PIN, pero lo interesante del mismo es ver como se puede usar una banda horaria para incrementar la seguridad.

7.2.6. Rutas y *antipassback*

Con el objeto de efectuar un control más estricto del movimiento de las personas dentro de un predio es que aplican estos conceptos de antipassback y/o rutas.

La definición de rutas o recorridos involucra a una lista ordenada de puertas que debe atravesar una persona para llegar a un destino, de manera que cuando una persona se presenta ante una puerta, necesariamente para ganar el acceso el sistema debe tener registrado su paso por la puerta anterior de la ruta. Este criterio es muy comúnmente utilizado para visitantes.

Otros fabricantes utilizan el concepto de áreas y a ellas les asocian lectoras que permiten entrar y salir de las mismas. De esta forma no es posible entrar a un área nueva sin haber salido previamente de la adyacente. A esta función se la llama habitualmente antipassback. Para implementar esta función todos los accesos a las áreas deben tener lectoras tanto de entrada como de salida.

Otros fabricantes llaman *antipassback* a otra prestación diferente pero de objetivo similar y que consta de limitar el ingreso a un área por un tiempo definido cada vez que se produce un ingreso. O sea que no se puede utilizar la misma tarjeta para provocar ingresos sucesivos repetidos en un lapso corto de tiempo.

Siempre que se utilicen rutas o *antipassback*, deberán establecerse los recorridos y las áreas teniendo cuidado de no generar zonas negras, donde las personas no puedan seguir adelante o rutas que no le fueron definidas.

Utilizar este tipo de restricciones necesariamente implica el entrenamiento del personal, tanto del de seguridad como de los usuarios, porque siempre se producen inconvenientes. Por ello se recomienda su aplicación moderada y gradual.

Los sistemas que implementan antipassbacks tienen funciones para volver a sincronizar las ubicaciones, ya sea por determinada persona a un determinado horario del día o una determinada puerta. Volver a sincronizar significa que el sistema desconoce la ubicación de la persona y por lo tanto la próximo vez que presente su tarjeta se le permitirá el acceso.

7.2.7. Funciones de control

Si bien no es parte del objetivo primordial del control de accesos realizar funciones de control, muchas veces es deseable que algunas operaciones simples puedan ser implementadas relacionadas con los accesos, por ejemplo que se enciendan las luces en horario nocturno al ingresar a un área que está vacía o habilitar la energía de un área al detectar que el responsable está presente o habilitar el teclado de operación de una máquina sofisticada solamente al detectar que el responsable está presente, llamar al ascensor cuando los directivos de la empresa presentan su tarjeta, etc.

Para esto algunos fabricantes ofrecen una forma de programación algorítmica que involucra a los accesos, con las bandas horarias y las salidas que resulta muy útil. De no ser así, algunas veces se debe recurrir a PLC (Controladores lógicos programables) para implementar dichas funciones.

Cada fabricante posee su propia forma de implementar estas funciones pero en términos generales diríamos que poseen una lista de eventos disparadores, una lista de acciones posibles y una forma de cerrar el evento. Los eventos disparadores pueden ser un acceso válido, acceso inválido, la puerta se abrió, la puerta se cerró, el estado de alguna entrada, alguna alarma, una banda horaria, etc. Las acciones posibles suelen estar relacionadas con la posibilidad de tomar una acción sobre una salida y/o la generación de un evento en la lista de eventos, mientras que las formas típicas de cerrarlos suele ser por tiempo o por el estado de alguna entrada. ■