Control de Accesos
Elementos de Identificación

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

Resumen de capítulos anteriores

En el número anterior planteamos los bloques básicos constitutivos del control de accesos deducidos a partir de un ejemplo.

Si los quisiéramos graficar en forma genérica, diríamos que un control de accesos está formado por un *"Elemento de Control y Toma de Decisión"*, que es quien toma las acciones necesarias en función de las programaciones que recibió del *"Software de control"* y de los sucesos que se van produciendo en tiempo real, informados por los *"Elementos de Identificación"* y las *"Entradas Adicionales"*. Los *"Elementos de Salidas y Alarmas"* serán quienes traduzcan las decisiones del controlador en acciones físi-

Continúa en página 160

Viene de página 156

cas concretas, como por ejemplo activar una cerradura, encender una lámpara, activar una alarma audible, etc.

Los elementos de identificación son aquellos dispositivos que, de una manera u otra, identifican con mayor o menor precisión a las personas que los portan o conocen. Dentro de este bloque estarán las lectoras y tarjetas, los equipos biométricos, etc.

Comenzamos a desarrollar este capítulo con un análisis más detallado de cada uno de estos bloques, considerándolos como partes constitutivas de un control de accesos.

Ahora bien, en algunos casos es posible encontrar dispositivos autónomos construidos a partir de un *"Elemento de Identificación"*. Por ejemplo, es posible adquirir teclados que generen salidas para ser conectados a controladores, es decir que funcionen como periféricos de un controlador de accesos, y otros como unidades independientes que sean capaces de tener una lista de claves almacenadas y que accionen un relé de salida cuando el pin ingresado coincida con el que tienen almacenado.

Por lo tanto, el análisis de cada *"elemento de identificación"* se hará en tres partes: la tecnología en sí misma, una descripción de un equipo autónomo basado en dicha tecnología y la descripción de un equipo periférico basado en esa tecnología.

Capítulo 5. Dispositivos de identificación

Como se mencionó anteriormente, el objetivo de estos dispositivos es el de identificar a su portador. Si bien hacia el final del artículo abordaremos como la utilización de más de un dispositivo de diferentes tecnologías utilizados en forma simultánea aumenta la seguridad en la identificación, por ahora haremos un análisis independiente de cada uno comparándolos contra los demás.

Estos dispositivos generalmente tienen una relación inversa entre el costo y el grado de certeza con el que son capaces de identificar a una persona, es por eso que todos pueden utilizarse, dado que no siempre es necesaria una identificación fehaciente, por ejemplo en puertas interiores de una empresa.

5.1. Teclados PIN

Están entre los más económicos y a la vez los que brindan el menor nivel de seguridad. Constan de un teclado, generalmente numérico de 12 teclas distribuidas como en un teclado telefónico, donde el "*" es considerado como la función borrar y generalmente el "#" como enter. Solo algunos fabricantes poseen modelos que distribuyen las teclas numéricas en forma aleatoria cada vez que se los utilizan.

Estos teclados son muy vulnerables dado que un observador puede reconocer la secuencia de teclas con sólo mirar a alguien ingresarla. Una forma teórica de aumentar la seguridad sería la de asignar códigos de muchos dígitos y cambiarlos periódicamente, pero en la práctica esto solamente complica el normal funcionamiento más que elevar el grado de seguridad.

5.1.1. Teclados PIN como dispositivos autónomos

En la aplicación autónoma estamos en presencia del dispositivo más económico del mercado. Generalmente son capaces de almacenar una cantidad limitada de claves programables y se las utiliza con el concepto de *"clave pública"*, es decir todo el mundo utiliza la misma clave. Este concepto es correcto ya que no llevan registros de eventos, no se puede saber que claves se ingresaron, por lo que carece de sentido tener varios códigos.

Generalmente se los programa con una longitud fija de números, por ejemplo 4 dígitos. Suele ser posible colocar claves de 3 dígitos o menos, pero en ese caso se deberá pulsar la tecla *"#"* luego del número elegido cumpliendo la función de *"Enter"*.

Otra característica típica de los teclados es que sólo admiten un tiempo prefijado entre teclas y si se produce una pausa mayor a un par de segundos, el número ingresado se anula y debe reiniciarse la secuencia, como si se hubiera pulsado la tecla de borrar *"*"*.

5.1.2. Teclados PIN como dispositivos periféricos de controles de accesos

Cuando se necesita colocar un teclado como periférico de un controlador de accesos, deberá seleccionarse un dispositivo que esté homologado por el fabricante del controlador. Antiguamente los controladores aceptaban teclados organizados en forma matricial, por ejemplo de 3x4, pero cada vez más frecuentemente los controladores sólo aceptan teclados con salida Wiegand (protocolo descripto aparte). De esta forma, utilizan el mismo puerto con el que se comunican con las lectoras de proximidad o las Smartcards y sólo es necesario configurarlos por software, indicándoles que en lugar de tener una lectora tienen colocado un teclado.

Muchos teclados tienen la posibilidad de almacenar 4 o 5 teclas y luego generar un paquete de datos en formato Wiegand 26 bits. Si se utiliza este tipo de teclados, deberá cablearse al teclado como si fuera una lectora con formato de salida 26 bits Wiegand, dado que el controlador no tendrá forma de saber si el paquete que el teclado le transmite proviene de una lectora real o de un controlador de teclado emulando ser una lectora.

5.2. Tarjetas y lectores

5.2.1. Generalidades

Desde siempre han sido los elementos de identificación que entregan la seguridad mínima aceptable.

En nuestra región se popularizó el uso de las tarjetas magnéticas para control de acceso y las de códigos de barras para presentismo. Otras tecnologías, como las tarjetas de efecto Wiegand, no alcanzaron popularidad habiendo sólo muy pocos sistemas instalados en el país que las utilicen.

Desde hace unos 10 años, las tarjetas de proximidad se adoptaron como estándar para el control de acceso y hoy se están introduciendo las tarjetas inteligentes (Smartcards) como el próximo paso tecnológico.

Desde el punto de vista de los lectores, los hay de los más variados diseños, rangos de lectura y factores de forma conforme a su ubicación (para ser colocados en marcos de puertas, cajas de luz, montados sobre vidrio, para largo alcance, etc.).

5.2.2. Clasificación por tecnología

5.2.2.1. De banda magnética

El mercado de control de accesos adoptó esta tecnología de la industria bancaria y es por eso que las normas que se utilizan responden a la ABA (American Banking Association).

Las tarjetas utilizadas son las tradicionales de PVC con su banda magnética. En la mayoría de los casos se utiliza la pista 2 (Track II) especificada por la norma para almacenar la información básica que se emboza, aunque algunos fabricantes, si bien utilizan la pista 2 no respetan el formato especificado por la norma, provocando que una vez que las tarjetas fueron inicializadas sólo puedan ser utilizadas en sus sistemas.

La tecnología de banda magnética parte de la base de tener una tarjeta que posea una banda con propiedades mag-

Continúa en página 164

Viene de página 160

netizables, tal que es posible codificar una información binaria en forma magnética longitudinal en la banda consistente en magnetizar los sucesivos dominios magnéticos. Si bien entre la cabeza lectora y la banda de la tarjeta hay una distancia mínima, el contacto es inevitable y por ende el desgaste. Puede decirse que adoptar esta tecnología implica entender que deberá efectuarse mantenimiento periódico de las lectoras y reemplazos frecuentes de las tarjetas.

Comparando la vida útil de una tarjeta magnética bancaria y una del mismo tipo de control de acceso, se va a encontrar que la de la aplicación de control de accesos se deteriora mucho más rápido y eso es por el mayor uso y el mal trato al que se las someten, no siendo así con las tarjetas bancarias (tarjetas de crédito o débito). Otro inconveniente que frecuentemente se presenta es la *"desmagnetización"*, que se produce cuando una tarjeta se somete a un campo magnético. Para minimizar este inconveniente, existen las bandas de alta coercitividad (4000 Oersted), mientras que las de baja coercitividad (300 Oersted) son más económicas pero se desmagnetizan con menor energía. Cabe mencionar que las lectoras de banda magnética son independientes de la coercitividad y que ésta debe tenerse en cuenta al momento de grabar la banda.

La ventaja más remarcable de esta tecnología es la facilidad de disponibilidad de las tarjetas magnéticas, su bajo costo y la posibilidad de imprimirlas.

5.2.2.1.1. Controladores de accesos autónomos con tarjetas de banda magnética

Estos dispositivos, que prácticamente no existen más, constaban de una lectora de banda magnética capaz de reconocer un número programable grabado dentro de la banda. En pocas palabras, esa lectora reconocía sólo una tarjeta con la que accionaba un relé de salida para el manejo de la cerradura. Dicho número se configuraba con dip switches o jumpers dentro del equipo y se grababan tantas tarjetas con ese código como eran necesarias.

Existieron también otros controladores autónomos que aceptaban rangos de tarjetas.

5.2.2.1.2. Lectores de tarjetas magnéticas como dispositivos periféricos de controles de accesos

Los controladores de accesos suelen traer interfases para la conexión de lectores de banda magnética. En este caso, en general cumplen con las recomendaciones de la ABA.

El protocolo ABA al igual que el protocolo Wiegand es de tipo unidireccional, la información fluye de la lectora hacia el controlador y posee 3 señales básicas, además de las de alimentación y señalización: Card Present, Clock y Data.

La señal de Card Present adopta valor verdadero cuando la cabeza lectora detecta una tarjeta con banda sin importar la información grabada en ella. Esta señal se utiliza para informarle al controlador que en breve, el lector comenzará a enviar una ráfaga de pulsos de *"clock"* que el controlador deberá utilizar para sincronizar los datos que se informan con la señal "data". El ancho de cada pulso de reloj dependerá de la velocidad con que el usuario deslice la tarjeta por la lectora.

En términos generales, cualquier lectora de banda magnética que cumpla con los estándares ABA funciona adecuadamente con los controles de accesos. Lo único que debe verificarse es que originalmente las señales eran de tipo *"Open colector"* y algunos lectores modernos entregan las mismas señales pero invertidas.

Desde el punto de vista de cual de las 4 pistas grabadas en la banda se utiliza para control de acceso, podría afirmarse que en la mayoría de los casos se utiliza la pista 2 (Track II). Lo que debe tenerse en cuenta es que esta pista admite un máximo de 37 caracteres y muchas veces los controladores de acceso no soportan cadenas de caracteres tan largas, por lo que la información que debe grabarse en la pista 2 debe estar limitada a la capacidad máxima que soporta el control de acceso, usualmente no más de 10 caracteres.

Estos problemas aparecían con mucha frecuencia en aquellas aplicaciones de tipo campus o empresas de gran porte, generalmente promovidas por bancos, donde pretendía usarse la banda magnética de la tarjeta de débito o crédito como tarjeta de control de acceso. Actualmente este problema se soluciona con tarjetas tipo Smartcard para el control de acceso, a las cuales se les coloca una banda magnética para ser utilizada para aplicaciones bancarias. Esto es lo que se denomina una tarjeta de múltiple tecnología, Smartcard + banda magnética.

5.2.2.2. Códigos de barras

Esta tecnología se adoptó de la industria de la identificación y alimentación y a diferencia de las de banda magnética, donde existe una única norma, aquí hay varios códigos/formatos que se utilizan. La mayoría de los fabricantes de control de acceso y presentismo imprimen las tarjetas utilizando codificaciones propias.

La ventaja principal de las tarjetas de código de barras son su bajo costo y la posibilidad de imprimirlas en casi cualquier lugar y con cualquier tipo de impresora.

Entre los problemas que tiene esta tecnología está la baja seguridad que ofrecen, dado que basta una simple fotocopia para duplicarlas.

Se intentó una solución para aumentar la seguridad que consiste en *"esconder"* la información de las barras bajo un filtro infrarrojo y utilizar una lectora capaz de leer esa longitud de onda, pero si bien se alcanza en parte el objetivo, no es suficiente para darle batalla a la tecnología de proximidad.

Debido a esto continúan siendo populares solo en aquellas áreas donde pueden aprovecharse sus ventajas sin preocuparse de sus desventajas, como en estacionamientos tarifados o sistemas de presentismo.

5.2.2.2.1. Lectores de tarjetas de códigos de barras como dispositivos periféricos de controles de accesos

La mayoría de las lectoras industriales de código de barras fueron diseñadas para aplicaciones de tipo supermercados, por lo que sus protocolos de salida son de tipo serie, por ejemplo RS-232 o protocolo de teclado de PC y estos protocolos no son comunes en las controladoras de control de acceso para la interconexión de lectores, por lo que, en el caso de utilizar lectoras de código de barras, se recomienda comprar los lectores recomendados por el fabricante de la placa de control de accesos.

5.2.2.3. Efecto Wiegand

Esta tecnología nació en Estados Unidos como una alternativa *"segura"* a las tarjetas de banda magnética. Se fabrican de PVC y adoptan la forma de tarjetas o llaveros dentro de los cuales, y como parte del proceso de fabricación, se colocan unos *"imanes"* orientados de forma tal que al desplazar dicha tarjeta en las proximidades de una lectora magnética, es posible obtener una información binaria que representa a un número. Esta tecnología mejora casi todos los problemas de las tarjetas magnéticas ya que no se desmagnetizan y no es necesario el contacto para efectuar la lectura, aunque los rangos de lectura son muy bajos (menos de 1 cm).

Continúa en página 168

Viene de página 164

Es una tecnología patentada y propietaria de *HID Corp.* por lo que la imposibilidad de falsificación y no duplicidad de la numeración está garantizada por el único fabricante.

Esta tecnología está siendo discontinuada dado que los sistemas por proximidad la mejoran ampliamente y con un costo más conveniente, pero todavía es posible encontrar sistemas que la utilizan.

Lo que esta tecnología nos dejó y se ha transformado en un estándar universal es el protocolo de comunicaciones entre las lectoras y los controladores, llamado protocolo Wiegand.

5.2.2.3.1. Lectores de tarjetas Wiegand como dispositivos autónomos de controles de accesos

Se desconoce que existan dispositivos abre puertas autónomos que tengan incorporados lectores de efecto Wiegand. Sí existen equipos de este tipo que tengan una entrada Wiegand donde se puede colocar una lectora de esta tecnología, pero estos van a ser tratados más extensamente por separado.

5.2.2.3.2. Lectores de tarjetas Wiegand como dispositivos periféricos de controles de accesos

Estos lectores poseen varios factores de forma, por ejemplo para ser colocados en paredes, sobre molinetes o de embutir en el frente un gabinete.

Su salida es Wiegand y son los que se denominan *"pass through"*, es decir, su salida refleja el formato que tienen la tarjeta. En otras palabras, si se presenta una tarjeta que fue programada en Wiegand 26 bits, la lectora entregará una salida de 26 bits. Si a continuación se presenta una tarjeta programada en Wiegand 37 bits, la lectora le enviará los 37 bits al controlador.

El protocolo Wiegand

El protocolo Wiegand es una forma de comunicación que fue definida e introducida al mercado por la empresa *Sensor (hoy HID®)*, hace ya más de 15 años, es esencialmente unidireccional y permite el traspaso de datos entre una lectora y una controladora.

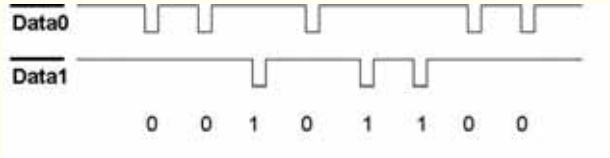
El protocolo establece líneas de datos, alimentación y señalización.

Las líneas de señalización son las que se utilizan para manejar el o los leds que poseen las lectoras así como el buzzer. De esta forma se tiene una línea llamada *"LED Rojo"* y otras llamada *"LED verde"*. En el siguiente cuadro puede verse el comportamiento del LED bicolor que traen las lectoras dependiendo del valor de estas líneas.

LED Rojo	LED Verde	Estado del LED
Falso	Falso	LED apagado
Falso	Verdadero	LED de color verde
Verdadero	Falso	LED de color rojo
Verdadero	Verdadero	LED de color ámbar

Las líneas de datos llamadas **Data0** y **Data1** tal que cuando se necesita enviar un *"1"* lógico, se coloca un pulso negativo de un ancho mínimo de 50 microsegundos en la línea llamada *"data1"* y cuando se necesita transmitir un *"0"* lógico, se envía un pulso negativo del mismo ancho en la línea llamada *"data0"*. La separación mínima entre dos pulsos consecutivos en cualquier orden es de 1 milisegundo.

En el ejemplo de abajo se puede observar como se transmite la palabra digital binaria 00101100.

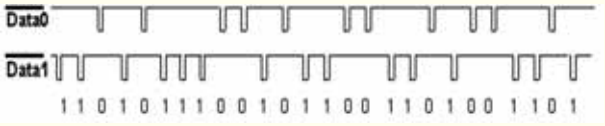


En la jerga del protocolo Wiegand, esta cadena de unos y ceros sería llamada Wiegand 8.

Ahora bien, esta cadena de 8 bits podría interpretarse de muchísimas formas, por ejemplo podría decirse que ese Wiegand 8 está formado por un primer pulso considerado como start y otro de stop, que en este caso ambos valen 0. La cadena restante sin dichos pulsos es 010110, donde podría decirse que representa al número hexadecimal 16 o decimal 22.

Si ahora tomamos el Wiegand 26 bits, denominado estándar, veremos que se trata de una cadena de 26 bits donde el primer bit es la paridad par de los próximos 12 bits. A los siguientes 8 bits se los llama *"Facility Code"* y representan un número que va desde 0 hasta 255; a los siguientes 16 bits se los llama Identificación, que pueden valer entre 0 y 65535. El último bit es la paridad impar de los últimos 12 bits excluyendo al de paridad. Una manera de expresar esto la siguiente:

```
Formato general  PFFFFFFFFDDDDDDDDDDDDDDDI
Paridad  par     PXXXXXXXXXXXX.............
Facility Code    .FFFFFFFF
Identificación   .........DDDDDDDDDDDDDDDD.
Paridad Impar    ............XXXXXXXXXXXXI
```



Supongamos una tarjeta que genera un código como el siguiente: 1101011100101100110100 1101

Si lo separamos en los campos lógicos quedará así:
1 10101110 0101100110100110 1 Donde el
FC = 10101110 = 0xAE (Hexadecimal) = 174 (decimal)
ID = 0101100110100110 = 0x59A6 = 22950

Para entender el cálculo de las paridades reescribimos la cadena coloreando el lugar de cálculo 1101011100101100110100 1101. La paridad par se calculó sobre los 101011100101 y dado que contiene 7 *"1"*, la paridad debe valer 1. La paridad impar del final se calcula sobre 100110100110 y como se trata de 6 *"1"* la paridad también vale 1.

¿Entonces, Wiegand es un protocolo de comunicación o una forma de codificar una tarjeta?

La realidad es que es ambas cosas. Las tarjetas se codifican en formato Wiegand y las lectoras se comunican con los controladores siguiendo el protocolo Wiegand. Lo que sucede es que si la tarjeta está codificada en Wiegand 37 bits va a ser necesario que se transmitan como mínimo 37 bits, por eso se suele confundir el formato Wiegand con el protocolo Wiegand.

En general, al decir que una tarjeta está codificada en Wiegand xx bits, se está afirmando también, que en el caso de que dicho lector se comunique utilizando el protocolo Wiegand, dicha comunicación también será de xx bits. ■