Integrando sistemas de seguridad

Alternativas de uso, aplicación y prestaciones

Cuando se habla de integración surgen dudas e inconsistencias. Muchos temen comprometerse a hacer algo integrado, otros simplemente dicen que lo hacen pero en realidad usan un solo tipo de integración. Otros, por el contrario, encaran una solución integrada y la afrontan sin inconvenientes.

Por Ing. Germán Alexis Cortés H.
gcortes@insetron.com

Integrar puede ser diferente a converger, también diferente a unir. Los sistemas de seguridad son parte de las redes electrónicas existentes en un edificio moderno: deben comportarse de una manera similar a las redes de comunicaciones y a las redes de control y automatización, que sólo existen en los edificios con más avanzada tecnología.

Cada subsistema de seguridad electrónica (circuito cerrado de televisión, alarmas contra intrusión, alarmas contra incendio, control de acceso para personas -empleados y visitantes-, para vehículos, para objetos, apoyo a requisas y seguridad informática, entre otros) es un mundo diferente, lleno de diversas marcas y procedencias. Poseen protocolos de comunicación distintos, cableado dispar y emplean normativa u orientaciones que difieren técnicamente.

La integración, desde el punto de vista de la seguridad, es permitir que muchos subsistemas de distintas marcas se comuniquen entre sí y puedan generar respuestas sin que sea necesaria una intervención manual.

SOLUCIONES PRÁCTICAS

Lo primero es conocer qué es la integración y definir el alcance real de lo que se busca. La integración, desde el punto de vista de la seguridad, es permitir que muchos subsistemas que, insisto, no son necesariamente de la misma marca, se comuniquen entre sí y que puedan generar respuestas sin que sea necesaria una intervención manual. ¿Para qué? Para asistir al operador en su trabajo, permitiendo que pueda concentrarse en la tarea principal de análisis y reacción ante situaciones anormales; y también para volver más eficiente el proceso de monitoreo, registro e investigación en situaciones rutinarias o de excepción.

La mejor manera de entender esto es tomando algunos ejemplos prácticos:

- Ejemplo 1: en ocasiones, el sistema de alarma puede recibir la señal de un sensor y registrar un acontecimiento anormal. En ese momento, es recomendable saber en qué situación estaban otros puntos del predio, qué personas estaban es esa zona antes de la alarma, verificar el registro de video que se tenga de las zonas que dan acceso al área y saber quiénes tienen acceso a esa información. Todo esto puede ayudar a investigar para efectivamente esclarecer lo ocurrido.

Es aquí donde un sistema de seguridad integrado puede darnos luces de todo lo registrado para hacer un análisis inmediato y eficiente. No sirven cinco subsistemas que tengan la información guardada pero que la recopilación sea imposible o tortuosamente lenta (es lo que sucede en muchos casos); especialmente cuando la alarma local dice una cosa, la estación de monitoreo otra, el sistema de acceso sugiere otra diferente y finalmente el sistema de CCTV grabó imágenes que contradicen el resto de la información. A veces, la causa de esto puede ser tan simple como una falta de sincronización en los relojes de los sistemas. Sin embargo, el tema es mucho más complejo: en muchos casos el tiempo de recopilación de la información es exagerado y su manipulación incrementa el nivel de riesgo y la confiabilidad del sistema entero.

En ocasiones, cuando el problema es sólo de relojes, a los operadores les puede resultar demasiado trabajoso buscar la información necesaria en varios lugares distintos. O, simplemente, no pueden hacerlo cada vez que sucede algo porque les llevaría demasiado tiempo, lo cual les haría descuidar sus labores en tiempo real. En estos casos, obtendríamos resultados incompletos aun habiendo hecho inversiones considerables.

- Ejemplo 2: un sensor fotoeléctrico de humo detecta una concentración de oscurecimiento importante ocasionada por una conflagración sencilla y genera una señal que puede, de manera temprana y eficiente, salvar las vidas de muchas personas. Si el sistema no es un sistema integrado, la única respuesta será un aviso sonoro en el panel de alarma contra incendio, que se silenciará fácilmente una vez que el operador oprima la tecla adecuada en el panel. El procedimiento que se lleve a cabo de aquí en adelante dependerá de las políticas, procedimientos y normativa que cada empresa tenga, así como del desempeño profesional del operador de turno. Sin embargo, pretender que una persona reaccione siempre de manera acertada y veloz ante una situación crítica es bastante ambicioso.

En este caso, un sistema de seguridad integrado podría salvar vidas al entregar instantáneamente, y sin la intervención del operador, la información adecuada para analizar y responder eficientemente frente a la situación. Este tipo de sistema podría realizar las siguientes acciones de manera simultánea (por supuesto, siempre y cuando estas respuestas hayan sido pensadas con anterioridad y programadas al sistema):

- Avisará al operador de la alarma, no sólo con un sonido en el panel de incendio sino registrando el evento en el sistema de integración.
- Se comunicará con las cámaras móviles más próximas a la zona de la conflagración para darles la orden de grabar en alta resolución y buena velocidad; no sólo a una cámara, sino a todas las que registren actividad en las zo-

nas inmediatas, de acceso y de evacuación. Las cámaras importantes en ese momento deberán desplegarse automáticamente en los diferentes monitores que controla la matriz de video, presentando la información exacta que el operador necesita para determinar si se procede a una evacuación o no.

- En caso de verificar que la situación atenta contra la integridad de los ocupantes del edificio, el sistema de integración puede evacuar el área del incendio; todo lo que deberá hacer el operador es aceptar la opción de evacuar. De hecho, si el propio operador estuviera comprometido, podrá abandonar su puesto de trabajo sin inconvenientes y el sistema hará el resto.
- Liberará las puertas de emergencia de cada zona, presurizará las escaleras de emergencia, activará las indicaciones audio-luminosas siguiendo el plan de evacuación preestablecido, cerrará las zonas donde se sepa que no hay ocupación para evitar robos, activará los mensajes de voz pregrabados que llevarán a cada grupo de ocupantes a las zonas seguras y guiará el flujo de gente hasta las salidas de emergencia, evitando situaciones de pánico.
- Activará los sistemas de alarmas de las zonas aseguradas y permitirá que se obvien las situaciones de alarma en las zonas comunes y de evacuación. Deberá restringirse el acceso de más funcionarios o visitantes al edificio en evacuación.
- Deberá avisar al cuerpo de bomberos mediante los canales de comunicación remota, deberá avisar a la estación de monitoreo de alarma de los detalles de la situación, enviará imágenes de los acontecimientos importantes y activará el envío de la mayor cantidad de información posible para tener un respaldo en un sitio remoto, libre de peligro. En caso de existir un centro de control alternativo, se pasará el mando a este punto de manera automática.
- Ordenará al sistema de aire acondicionado que detenga el suministro de aire para evitar avivar el fuego, pero dejando activo la extracción para suprimir la mayor cantidad de humo.
- El sistema de control de equipos electromecánicos podrá enviar los ascensores al piso de evacuación y dejarlos allí, como establece la norma correspondiente.
- Desactivará las cargas eléctricas que puedan tener inconvenientes en caso de emergencia o incluso hasta agrandar el incendio.
- Supervisará de manera crítica y constante la activación de todo el sistema hidráulico de extinción manual y automática de incendio.
- Suspenderá el suministro de las redes de gas al predio y controlará eficientemente el de agua potable.

Y de acuerdo con cada sitio, activará, desactivará y ajustará según corresponda una inmensidad de variables que no podemos predecir en este artículo, porque dependen de cada caso. Estos ajustes y cambios deben hacerse simultáneamente en la menor cantidad de tiempo posible.

Imaginemos que todo esto no estuviera comunicado entre sí bajo el control de un sistema integrado, sino que cada equipo tuviera que manipularse y reajustarse mediante el operador de turno: las ventajas de protección que ofrece la integración de sistemas se hace evidente.

Desde el punto de vista técnico existen distintos niveles de integración: desde equipos que se comunican por contactos secos hasta los que lo hacen a través de protocolos aceptados universalmente por la industria.

NIVELES DE INTEGRACIÓN

Imaginemos que muchos proveedores de soluciones de seguridad nos dicen que un sistema es integrado, pero que en realidad no pueden hacer ni siquiera el 20% de las acciones enunciadas: esto es porque existen distintos niveles de integración. Conozcamos un poco sobre las prestaciones que nos puede ofrecer cada uno de ellos.

El más simple es cuando nos dicen que los sistemas están integrados en una misma consola de control. Es decir, los vemos todos en un mismo sitio, en el mismo cuarto e incluso en el mismo mueble. Sin embargo, cada uno actúa por su lado. Esto, obviamente, no es integración (y pasa en el 80% de los casos).

El siguiente nivel nos habla de una comunicación entre equipos mediante interfaces de hardware que usan contactos secos y replicación de señales de alarma o control. En este caso, muchas empresas que se dicen integradoras repiten señales de alarma o de control mediante tarjetas de expansión. Esto se usa mucho cuando queremos conectar de manera simple dos y sólo dos sistemas; si no, la cantidad de cables y de señales hace que el cuarto de control sea inmensamente complejo. En ocasiones, encontrar un problema puede ser muy difícil, sin contar con las altísimas posibilidades de desconexión accidental; adicionalmente el costo de los expansores es alto y su cantidad puede llegar a un límite muy rápido. Un inconveniente adicional es la demora (a veces desesperante) que presentan los sistemas al manipular información: se activa el sistema de alarma contra incendio pero los presets y el despliegue en la matriz se activan 5 segundos después. Es decir que el tiempo de latencia del sistema es muy lento, poco conveniente para ajustes inmediatos de última hora. He estado en centros de control en los que la información comenzó a verse desde otros sistemas solo después de 30 o 40 segundos, lo cual implica controladores sobrecargados, plataforma de cómputo casera, memoria de video pequeña y sistemas interconectados con contactos secos.

Un nivel de integración un poco más eficiente es mediante transmisión serial de datos. Se aplica, por ejemplo, entre el sistema de alarma y el de integración o entre el sistema de acceso y el de CCTV. En este caso, se usan mucho los puertos RS-232 o RS-485 y sus diferentes acoples, actualmente a un puerto USB. Son una manera más simple de interconectar. Sin embargo, al igual que en el nivel anterior, se usan para comunicar dos y sólo dos subsistemas. El pro-

blema de latencia sigue siendo importante y, en algunas ocasiones, más largo que usando simples contactos secos por la falta de jerarquía, manejo de DMA (Direct Memory Access), manejo de interrupciones al procesador (IRQ) o, en general, porque estamos tratando de integrar sistemas que no están diseñados para ello. Los ingenieros electrónicos somos muy dados a fallar en este punto y sólo lo entendemos cuando ya es muy tarde y los sistemas están comprados y programados.

Un nivel de integración mejorado, muy usado por marcas que tienen un portfolio amplio de subsistemas, es una comunicación serial, usando nuevamente los puertos conocidos, pero en este caso con un protocolo propietario que hace que la comunicación sea completa y rápida. Los tiempos de latencia son bajos y ofrece la ventaja de permitir que, mediante el sistema de integración, una señal se pueda usar para generar acciones en cualquier otro subsistema. Es decir, aquí no se comunican únicamente dos sistemas sino que se integran en una misma plataforma conocida por la marca común. El único inconveniente es la falta de una plataforma abierta que permita fácil integración con terceros. Esto significa que su protocolo es cerrado y que el usuario final debe comprometerse con esta marca.

El siguiente nivel, a veces obvio, es muy similar al anterior, pero emplea protocolos de comunicación ampliamente conocidos en la automatización (como por ejemplo BacNet, LonWorks, ModBus, OPC o OneWire, entre otros), que poco a poco se convierten en estándares de la industria. De esta manera, no se depende de una sola marca con un lenguaje cerrado, sino que se pueden integrar muchas marcas que usen el mismo protocolo. Aquí, el asunto de integración comienza a ser interesante y eficiente. En este punto, muchos fabricantes hablan de la convergencia sobre una misma red.

El futuro a nivel latinoamericano, nacido en Europa y Estados Unidos hace mucho tiempo, son los Sistemas de Administración o Automatización de Edificios (BMS o BAS por sus siglas en inglés).

Algunas fábricas en el mercado tienen traductores de protocolos y controladores especiales de comunicaciones, que permiten hablar con cualquier equipo normalizado en la industria e incluso hacer desarrollos basados en las librerías de un producto que permitan incorporarlo al protocolo base del sistema.

Finalmente están las marcas (quizás las mejores y más avanzadas) que migran fácilmente hacia una plataforma de cómputo conocida y muy utilizada, como es la red de datos tradicional (LAN/WAN) con protocolos TCP/IP, enviando los caracteres de control y mapeo tradicionales de cada protocolo de tipo industrial, pero sobre una interfaz de red de datos estable y conocida. Aquí, algunos fabricantes nuevamente deciden usar el término convergencia, al tratar la red de datos como la unidad de toda la información.

Debe tenerse especial cuidado al olvidar la mística de seguridad y comenzar a hablar de comunicaciones. Compartir información en un medio con acceso abierto, frágil e inestable como las redes de comunicación actuales no es lo mejor para los datos de seguridad. Es decir, no es viable diseñar un sistema de seguridad inseguro. Mi sugerencia es construir una red de comunicaciones exclusivas para seguridad (no sólo para video) y compartir los canales existentes y el ancho de banda con el resto de la compañía, si y sólo si no encontramos otra opción posible.

Con el auge de las redes inalámbricas, algunas marcas se comunican mediante 802.11x, e incluso algunas más especializadas, mediante protocolos inalámbricos de control tipo Zigbee o similar. Nuevamente hay que tener cuidado con el tema de seguridad de la información: recordemos que hoy es difícil interceptar datos inalámbricos por los niveles de encriptación usados, pero todavía sigue siendo relativamente fácil interferirla. Hacer que las ondas transmitidas no lleguen a su destino es algo relativamente fácil, ya que el medio de transmisión es el aire. Este no es un tema menor y siempre debe ser tenido en cuenta.

CONCLUSIONES

En todas las integraciones de alto nivel, los retardos son mínimos y el tiempo de latencia es muy pequeño. Aun así, no hay que esperar milagros. Es importante aclarar que estas integraciones de alto nivel dependen casi siempre de un software de integración adecuado que pueda manejar una base de datos común sólida y flexible. Opera como administrador de la red de datos y permite que cada dispositivo guarde y controle su información con sus propios medios, mientras centraliza la información en un mismo sitio. Es lo más seguro, lo más eficiente y lo más rápido.

Debemos decir también que algunas marcas del mercado sólo se dedican a la integración de seguridad (acceso y CCTV o acceso e incendio), pero nunca tienen la opción de comunicarse con un sistema de control y automatización, o viceversa. Otras sólo pueden integrar uno o dos subsistemas, pero no el resto. Otras exclusivamente si son de la misma marca o holding empresarial y otras integran con protocolos propietarios que dicen ser abiertos pero que en la realidad nadie lo usa. En fin, el mercado está lleno de opciones; al analizar con detenimiento cada proyecto puede tomarse una decisión acertada.

También debemos advertir que esto no es sólo para los grandes proyectos: a nivel pequeño existen soluciones muy completas de costos moderados y, sobre todo, modulares, que permiten comenzar por lo básico e ir creciendo a medida que las necesidades se presenten.

Por último, el futuro a nivel latinoamericano, nacido en Europa y Estados Unidos hace mucho tiempo, son los Sistemas de Administración o Automatización de Edificios (BMS o BAS por sus siglas en inglés). Estos son sistemas totalmente integrados que debemos tener como punto de guía en el horizonte para evitar hacer compras o ventas erradas, que el día de mañana sean declaradas obsoletas. De todas maneras, siguiendo todas las posibilidades que hemos visto en este artículo, siempre es importante indagar a fondo sobre las ofertas de "integración" o "convergencia" para tomar la decisión acertada. ■