UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CAMPUS
A R A G Ó N

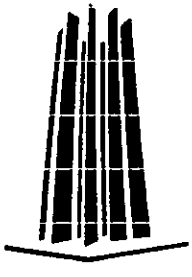
"SISTEMAS ELECTRÓNICOS DE SEGURIDAD"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

P R E S E N T A :

GUSTAVO MAURICIO MARTÍNEZ JAIMES



ENEP ARAGÓN

MÉXICO, D.F. 1998.

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

SISTEMAS ELECTRÓNICOS DE SEGURIDAD.

ÍNDICE

CAPÍTULO II. SISTEMAS LOCALES DE ALARMA Y VIGILANCIA.

CAPÍTULO III. SISTEMAS CENTRALES DE TELESUPERVISIÓN.

CAPÍTULO IV. APLICACIÓN DE LOS SISTEMAS ELECTRÓNICOS DE SEGURIDAD.

SISTEMAS ELECTRÓNICOS DE SEGURIDAD.

Objetivo:

Dar un panorama más amplio de los alcances de la electrónica en el área de alarmas de seguridad, y control, así como sus ventajas y desventajas.

INTRODUCCION.

Las alarmas electrónicas están cada día más extendidas debido a que se necesita una seguridad mayor. Antes los sistemas de seguridad sólo se disponían en lugares en los que se necesitaba preservar del robo, el atraco o el incendio, valores importantes de dinero o efectos.

Hoy en día se aplican en pequeños negocios, fábricas y hogares, además de las entidades bancarias y de ahorro. En los procesos industriales también se aplican para detectar cualquier fallo en los distintos procesos industriales, en las centrales nucleares, en los centros de investigación, etc. Pero esta exposición se centrará en las alarmas pensadas para la detección de los «amigos de lo ajeno y los incendios.

CAPITULO I.SISTEMAS DE SEGURIDAD.

Objetivo:

Describir los fundamentos de los sistemas de seguridad, así como algunas posibles soluciones.

CAPITULO I. SISTEMAS DE SEGURIDAD.

I.1. SISTEMAS ELECTRONICOS DE SEGURIDAD.

Los sistemas de alarma se utilizan en muchos casos como protección contra el robo, los incendios, inundaciones, escapes de gas, atracos o como simple aviso de emergencia.

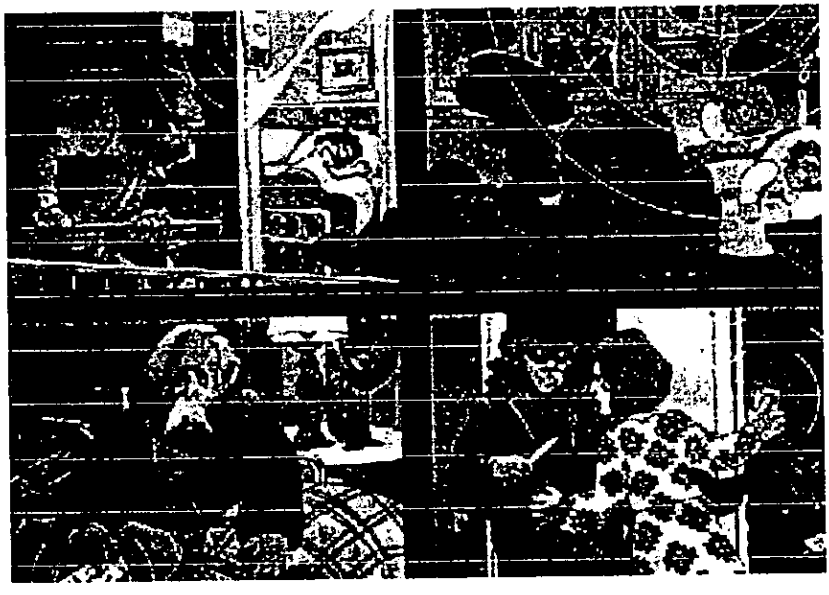


Figura 1. Los sistemas de alarma se utilizan en muchos casos como protección contra el robo, los incendios o como simple aviso de emergencia.

El propósito, de todos conocido, de un sistema de alarma es detectar cualquier anomalía debida a la entrada de un intruso o a un incendio. Cuando se trata de la detección de un indeseable, su mejor

efecto es el de alertar al propio intruso antes de que su entrada sea efectiva, es decir, actúa como sistema disuasivo.

El ladrón puede no estar enterado de la existencia del sistema de alarma, pero se asustará por el sonido del mismo antes de robar o causar otro daño mayor que el de forzar la puerta de entrada o cualquier otro acceso.

Todo sistema de alarma debe ser ante todo fiable. Un fallo en el momento oportuno anularía completamente el fin para el que se instala. Un sistema que es susceptible de dar falsas alarmas es realmente tan malo como el que puede romperse completamente. Un sistema que es propenso a dar falsas alarmas no es seguro y tenderá a ser ignorado. Una trampa utilizada por algunos ladrones es provocar una alarma deliberadamente y esperar en las cercanías. El propietario aparece y supone que es un defecto y para no ser molestado la desconecta. Luego, el ladrón entra sin el menor riesgo. Lo adecuado es buscar el defecto que ha provocado la alarma y luego volverla a conectar. Un sistema de alarma debe estar a prueba de desconexión por parte de intrusos. Por ello la desconexión debe estar en una parte protegida. Además debe estar diseñado para que, si la entrada ya se ha efectuado, la alarma no pueda silenciarse rápidamente por el intruso; para ello se deben ocultar las partes vulnerables del sistema, como son la unidad de control, la fuente de alimentación y la instalación de las alarmas sonoras.

Estas son por sí mismas vulnerables, ya que a menudo están instaladas dentro de cajas de acero a la intemperie. Esto hace que pueda ser saboteada si no se dispone en el lugar adecuado, lo suficientemente alto e inaccesible desde el exterior. Los cables que van a la sirena o cable pueden cortarse, por ello deben estar protegidos.

El coste del sistema es otro dato a considerar. Cuando se expone mucho valor, el coste inicial de la instalación de un sistema adecuado y efectivo no debería ser un impedimento para su consecución. Sólo debe escogerse el de menor coste siempre que no aminore la seguridad respecto al de mayor desembolso. El coste de funcionamiento, dadas las actuales tecnologías de circuitos integrados de bajo consumo, es prácticamente despreciable, a no ser que se trate de sistemas muy complejos.

Determinados cuerpos oficiales han expuesto algunas recomendaciones con miras a la construcción, instalación y servicio de sistemas de alarma para intrusos e incendios. La mayoría de las recomendaciones están basadas en el British Standard BS 4737 y similares IEC.

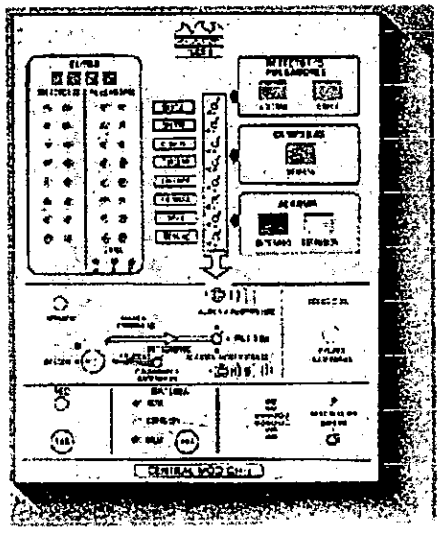


Fig. 2. Unidad de control contra incendios. También se denomina central de alarmas de incendios.

Las principales recomendaciones quedan resumidas seguidamente. Se recomienda que las llaves de conexión del sistema sean de seguridad o codificadas. El sistema deberá responder a señales de alarma mayores de 800 milisegundos, pero no a aquellas que sean menores de 200 milisegundos. Con esto se evitarán falsas alarmas debidas a transitorios externos. El abastecimiento de potencia autónoma deberá hacer funcionar el sistema en reposo como mínimo durante 8 horas, cuando la energía del fluido eléctrico del lugar desaparezca por alguna avería.

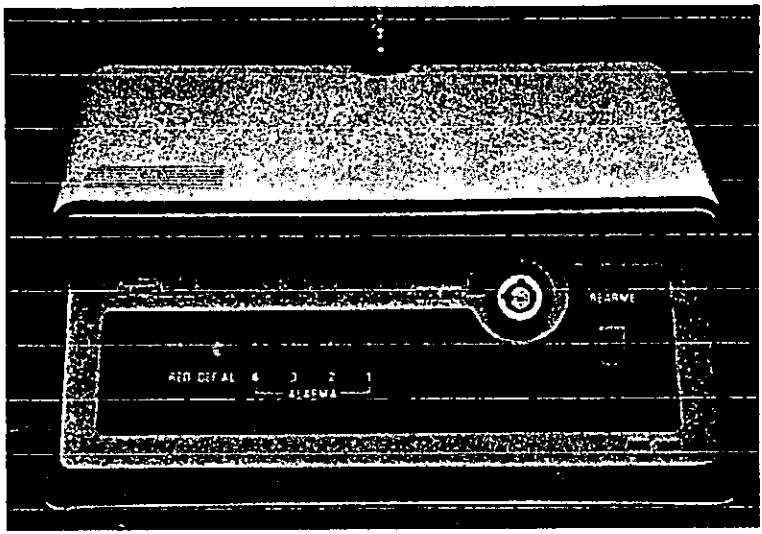


Fig. 3. Central de alarma que aprovecha la posibilidad de enviar señales vía radiofrecuencia.

También debe ser suficiente para 2 horas de alarma sonora. La batería, en caso de ser hermética, es conveniente cambiarla como mínimo cada 5 años, aunque no dé muestras de estar deteriorada. El nivel sonoro de la alarma no podrá bajar de 70 DB en todas las direcciones a 3 metros. El cableado tendrá que ser en bucle cerrado, disparándose la alarma si son cortados los cables. Otros organismos aconsejan que una vez disparada se fije una interrupción de la alarma después de 20 minutos. Hay sistemas sencillos que no cumplen todas las especificaciones pero los más profesionales sí lo hacen.

I.2. APLICACION DE LOS SISTEMAS DE SEGURIDAD.

En plan general se deben distinguir dos tipos de sistemas de alarma: Los sistemas locales de alarma y vigilancia y los sistemas centralizados de telesupervisión.

Los citados en primer lugar, como ya se sabe, son pequeños dispositivos electrónicos (en comparación con los demás) encargados de la vigilancia de fenómenos muy concretos que se desarrollan en espacios relativamente limitados, tales como protección de viviendas frente a intrusos, incendios, fugas de gas, detección y notificación de averías o deficiencias en el funcionamiento de máquinas aisladas en la industria, etc. En cuanto a los citados en segundo lugar, es decir, los sistemas centralizados de telesupervisión, el campo de aplicación es mucho más amplio, no sólo en lo que concierne al elevado número de procesos a los que son aplicables, sino en cuanto a la diversidad de funciones a realizar y en el número de puntos de vigilancia a los que se pueden. adaptar ya que estos sistemas son prácticamente universales, por ello se excluye en ellos la etapa transductora y es posteriormente el usuario el que se encarga en cada aplicación de introducir los sensores necesarios para convertir las variables a vigilar a unas unidades y márgenes normalizados que sean asequibles al sistema.

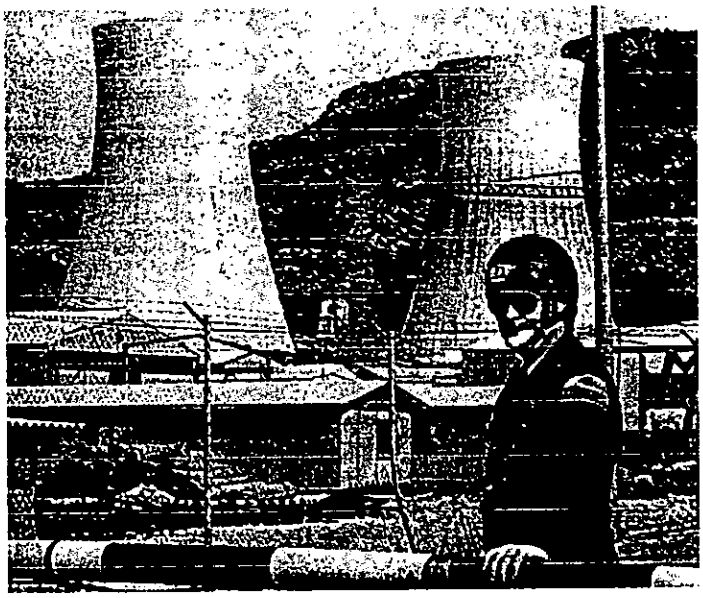


Fig. 4. Las alarmas se aplican con profusión en las instalaciones más sofisticadas y complejas, como son las centrales nucleares.

Como resumen no exhaustivo se expone una relación de procesos susceptibles de ser vigilados o supervisados por estos sistemas: vigilancia de temperaturas en grandes edificios, detección de incendios y fugas de gas en las viviendas, protección de propiedades frente a intrusos, vigilancia del correcto funcionamiento de máquinas, protección de los operarios de máquinas con partes móviles, supervisión de centrales hidroeléctricas, térmicas o nucleares; supervisión de gasoductos y oleoductos, supervisión de redes de captación y distribución de aguas, control fluvial, control de tráfico, supervisión de procesos de fabricación, centralización de datos referentes a la contaminación atmosférica de zonas extensas,

automatización de bancos, centralización de datos meteorológicos, señalización ferroviaria, vigilancia de unidades médicas, supervisión de redes eléctricas de distribución, centralización de datos en plantas siderometalúrgicas y petroquímicas, vigilancia forestal, sistemas antirrobo en bancos y entidades, vigilancia de centrales de calefacción, monitorización de procesos, sistemas de alarma para detección de objetos metálicos, sistemas de protección antichoque para objetos móviles, etc.

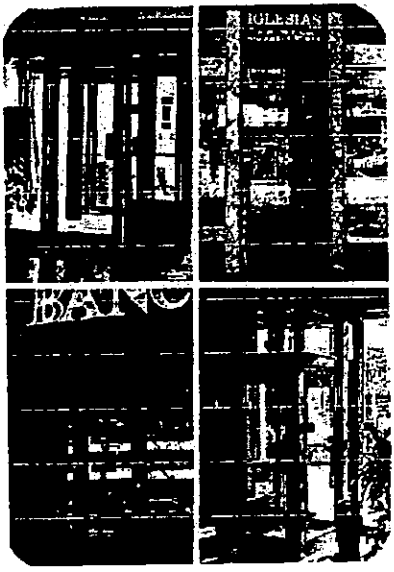


Fig. 5. La aplicación de los arcos detectores de metales y cabinas especiales, permiten tener un control de accesos para evitar atracos.

La aplicación de los arcos detectores de metales y cabinas especiales, permiten tener un control de accesos para evitar atracos.

Siendo de mucha utilidad en entidades bancarias, joyerías, aeropuertos y edificios públicos sujetos a atentados.

De esta lista de posibles aplicaciones, debido a la exposición resumida que de las alarmas electrónicas se quiere dar, las que conciernen a los sistemas antirrobo, antiatraco y anti-incendio serán las más detalladas.

En las alarmas antirrobo el modo para detectar la entrada del intruso se puede llevar a cabo de distintas formas: mediante la apertura de puertas o ventanas con contactos magnéticos de proximidad, mediante la detección del movimiento con sensores de ultrasonidos o microondas, por la rotura de cristales con detectores de vibración de cinta conductora, por la intercepción de barreras fotoeléctricas de luz o infrarrojos, por la detección de una variación brusca de temperatura al entrar una persona con detectores pasivos de infrarrojos.

Otros métodos para advertir del robo son los detectores sísmicos dispuestos en cajas fuertes, la vigilancia mediante circuito cerrado de televisión, etc. el atraco se puede paliar con pulsadores escondidos que dan la alarma, en cuanto son presionados, en comisarías de policía o centrales de seguridad, o limitando el acceso mediante controles electrónicos de identificación. La detección de incendios se lleva a cabo con sensores de humo y temperatura excesiva. Algunos de éstos son complicados mientras que otros pueden ser tan simples como un par

de contactos eléctricos bajo tensión de un resorte, separados por una sustancia química que se funde a una temperatura alta y permite que se unan activando la alarma.

En muchos casos, las firmas de protección a las propiedades proporcionan un servicio de alarma de estación central. Cuando los sensores detectan una anomalía, la unidad de control ordena a un dispositivo especializado que marque el número de esta estación o central de seguridad dando el mensaje dispuesto en una cinta y detallando la dirección del lugar siniestrado o robado.

Mediante este sistema se puede proteger e identificar individualmente un gran número de propiedades, ya que el personal de la estación central puede localizar el origen de la llamada y telefonear a la policía o a los bomberos, solicitando el adecuado auxilio.

En algunos países la comunicación con la estación se lleva a cabo con cables de televisión (TV por cable). Un sistema de alarma de estación central puede vigilar continuamente todas las propiedades protegidas, dando una mayor seguridad en comparación con la simple sirena exterior que puede no oír nadie o bien, si se oye, se ignora pensando que ya llamarán otros a la policía o bomberos.

I.3. SISTEMAS DE CONTROL DE ACCESO.

Existen diversas técnicas automatizadas de control de acceso. Los sistemas automáticos controlan el acceso a un edificio sin la ayuda de un guardia; pueden permitir el acceso basándose en el reconocimiento de un código en memoria, el reconocimiento de huellas digitales, el reconocimiento de un patrón de voz, etc. que se da por medio de equipo detector o lector.

Un número importante de factores son considerados al seleccionar un sistema de control de acceso. El más importante es la resistencia a la falsificación. El grado de resistencia requerido está en función de la importancia y de que tan crítica es el área que se esta controlando. La resistencia a la falsificación es una medida de la dificultad para duplicar el código de acceso. Los sistemas de reconocimiento del habla, la retina y la firma son considerados los más resistentes debido a la interacción dinámica necesaria para la identificación personal.

Los sistemas de reconocimiento de geometría de la mano y huella digitales se consideran como de medios a alto, mientras que cuando el acceso es dado por tarjetas, códigos en memoria y teclado ofrecen baja resistencia a la falsificación.

Otro factor importante a considerar en el control de acceso es el tiempo que tarda una persona normal en entrar, ya que mientras la puerta permanezca abierta otra podría introducirse.

Algunos sistemas dan una señal de alarma cuando la puerta permanece demasiado tiempo abierta. Además, es necesario considerar el tipo de cerradura.

I.4. SISTEMAS AUTOMATIZADOS DE CONTROL DE ACCESO.

Existen diferentes dispositivos par controlar el acceso a un área, la selección de este dispositivo está en función del nivel de seguridad deseado y del costo. A continuación se describen algunos de los sistemas más comunes.

I.4.1. TECLADO Y CÓDIGO EN MEMORIA.

En ellos se debe dar un código que se encuentra en memoria con la secuencia adecuada usando un teclado. Cuando el código es correcto se otorga el acceso activando inmediatamente la cerradura que abre la puerta.

Un punto vulnerable que presenta este sistema, es que, una vez que se ha abierto la puerta, más de una persona puede entrar pudiendo

ser alguna no autorizada. Algunas, ofrecen seguridad adicional, activando una alarma cuando la puerta permanece demasiado tiempo abierta.

Los sistemas con teclado y código en memoria proveen relativamente un nivel bajo de seguridad por lo que es importante darle una aplicación adecuada dependiendo de la necesidad que se requiera cubrir.

I.4.2. TARJETAS CODIFICADAS.

La mayoría de los sistemas de control de acceso usan tarjetas codificadas con sus respectivas lectoras. Para lograr el acceso la persona introduce o presenta su tarjeta a la lectora.

Dicha tarjeta en tamaño y apariencia se parece a una tarjeta de crédito. Aunque las técnicas de grabación del código varían en cada fabricante, se puede almacenar millones de combinaciones. La codificación puede ser magnética o electrónicamente con los datos necesarios para la completa identificación de la persona. Algunos, proporcionan una fotografía y las características propias del portador para una posible revisión complementaria.

Su aplicación requiere tener un procesador central con los datos de cada usuario, conectando a este, las lectoras de tarjetas remotas.

Puede controlar el acceso y la salida de cientos de usuarios usando lectoras en varios lugares. Cuando una tarjeta se presenta a la lectora, esta sensa la información codificada y la transmite al procesador, el cual recibe la información y la compara con los datos en memoria y en unos milisegundos decide si negar o acceder la entrada. Cuando el acceso es concebido el controlador manda una señal que abre inmediatamente la puerta.

La unidad central de control permite al operador realizar muchas funciones, una de las cuales es cancelar tarjetas perdidas o robada. Es necesario que la cancelación de tarjetas sea tan rápido y fácil como sea posible.

Una de las funciones adicionales en algunos sistemas es que no se permite el uso de la tarjeta para entrar hasta que ésta haya sido usada para salir del área de control. Con lo que se evita que la tarjeta pase de una persona que se encuentra adentro a otra que quiere entrar.

Las lectoras de tarjeta identifican a la tarjeta no al portador. La vulnerabilidad más común es la pérdida y que su propietario no se percate. Una combinación teclado y código en memoria robustece al sistema.

Las tarjetas pueden ser codificadas para dar información adicional, por ejemplo, el puesto del usuario, cuando y a que hora esta permitido el acceso.

A continuación se describen algunas formas más populares de control de acceso por tarjetas codificadas:

1. Tarjeta de identificación por foto. Este tipo puede ser la credencial de empleado con la fotografía del propietario, la cual puede ser inspeccionada por un guardia. Es difícil cuantificar la efectividad de este tipo de control de acceso, debido a que entra en juego el criterio del guardia cuando examina la credencial. Otro factor que interviene es el número de personas que estén entrando al mismo tiempo, además de que la credencial es fácil de falsificar.

2. Tarjetas con código magnético. Las tarjetas con código magnético tiene una hoja flexible de material magnético, entre dos hojas de material plástico, en la que graba un arreglo de marcas magnetizadas permanentemente. El código es determinado por la polaridad de las marcas.

Las desventajas que presentan estas tarjetas es que el código se puede borrar si es expuesta a una fuente campo magnético. Es posible falsificarlas, pero en general no presentan problemas.

3. Tarjetas con tira magnética. Una tarjeta de este tipo presenta una tira magnética a lo largo de uno de sus lados. La cual se codifica con los datos del portador. Algunos sistemas utilizan codificación alfanumérica permitiendo el nombre y datos adicionales.

Los sistemas que usan tarjetas con tira magnética tienen actualmente un amplio uso; pueden ser falsificadas y también existe el riesgo de un borrado accidental.

4. Tarjetas de código de barra. Estas tarjetas son codificadas por un arreglo geométrico grabado en cintas, los espacios representan dos codificados. La ventaja de estos códigos es que no requiere un lector sofisticado. Puede ser leído pasando un detector óptico sobre la tarjeta.

La desventaja es que el código es visible y puede ser fácilmente duplicado, aunque en las versiones recientes solo puede ser leído usando luz ultravioleta o infrarroja.

5. Tarjetas de proximidad. Las tarjetas de proximidad se codifican eléctricamente, un campo electromagnético es transmitido por una unidad estacionaria de interrogación ubicada junto a la entrada de acceso. Cuando la tarjeta esta expuesta al campo electromagnético se induce un voltaje en la tarjeta que activa un circuito eléctrico pasivo, entonces la unidad interrogadora sensa la información y la

envía a la unidad de control, si el dato es válido se abre la puerta. La ventana de estos sistemas es que no es necesario insertar la tarjeta en la lectora.

I.4.3. COMPARACIÓN POR VÍDEO.

En la comparación por vídeo, se utiliza un circuito cerrado de televisión y en combinación con el personal de seguridad se realiza el control de acceso. Dicho control es manual, ello implica que sea más lento y además depende de la dedicación y concentración del operador para el buen desempeño del sistema.

Las áreas que requieren de alta seguridad, el sistema controlador de acceso, verifica la identidad del solicitante a través del reconocimiento de huellas digitales, geometría de la mano, patrón de voz y algunas otras características que hacen única a una persona.

Para esto, se requiere digitalizar previamente los datos que identifican al usuario. Es muy común, que la persona que desea el acceso se identifique con una tarjeta codificada, posteriormente, para confrontar sus datos se procede a la verificación.

La verificación de entrada es digitalizada y comparada a alta velocidad con los datos de referencia para que en pocos segundos el

acceso pueda ser concebido dependiendo del resultado de la comparación.

Desafortunadamente, las características físicas de la gente cambian en tiempos relativamente cortos. Por ejemplo, las huellas digitales pueden verse afectadas por una herida, por el desgaste y por estar en contacto con superficies abrasivas dependiendo de la actividad que el usuario realice. El patrón de voz y la firma pueden ser afectados por stress la fatiga. Por estas razones el sistema debe tolerar un porcentaje de errores.

A continuación se describen algunos de los sistemas más comunes de verificación.

I.4.4. RECONOCIMIENTO DE HUELLA DIGITAL.

En estos sistemas, la huella que se desea reconocer se encuentra entintada en una superficie determinada. El área de la huella digital es explorada por métodos ópticos, digitalizada y transmitida a la unidad de control, la cual guarda esta información junto con los datos de la persona que posteriormente solicitará el acceso.

La identificación se lleva a cabo por comparación, es decir, la unidad de control compara la huella leída con el patrón guardado en memoria. Se comparan con los datos de las pequeñas interrupciones,

la terminación de arrugas y ramificaciones de un número de aproximadamente cien marcas impresas en una huella.

La terminal de este sistema cuenta con un "display", un teclado o lector de tarjeta, un dispositivo sobre el cual se pone el dedo del solicitante y un explorador óptico (scaner) para obtener la información de la imagen de la huella digital. El teclado o la lectora de tarjeta, son utilizados para identificar a la persona, ya sea que introduzca su tarjeta o teclee un número asignado previamente. En el display se indican los pasos a seguir para lograr el acceso.

Es muy común, que el sistema guarde información de más de un dedo, debido a que pueden producirse heridas o daños que causarían un error en la comparación de huellas, si esto ocurre se tiene la opción de cambio de dedo.

I.4.5. RECONOCIMIENTO DE LA FIRMA.

El sistema de reconocimiento de la firma, se basa en la comparación de las características dinámicas del firmante. Estas características son la precisión ejercida al ejecutar la firma y la velocidad con que se realiza. Dos son las técnicas utilizadas para identificar la firma. Una usa un sensor de presión especial puesto sobre el escritorio, el cual sensa la fuerza aplicada al escritorio por el firmante. Con ésta técnica no se requiere de una especial. La segunda técnica, utiliza una

pluma especial que sensa el movimiento de la punta y además la presión aplicada por el firmante.

El patrón de presión y movimiento de la pluma son diferentes en cada firmante lo que da un alto grado de certidumbre sobre la autenticidad de la firma. La falsificación de la firma original es muy difícil, debido a que la velocidad de escritura y la presión no están directamente relacionadas con la apariencia.

I.4.6. RECONOCIMIENTO DE LA GEOMETRÍA DE LA MANO.

Debido a que desde el momento en que se nace hasta que se muere, las manos cambian y aun así permanecen características en ellas como son: las dimensiones comparativas, la forma de los dedos, la posición exacta de las articulaciones, en fin, innumerables cianotipos complejos que hacen de la mano un elemento único para garantizar una identificación infalible.

El sistema cuenta con una cámara electrónica digital integrada, la cual toma una foto en tercera dimensión de la mano y un microprocesador extrae el patrón único de identidad de la persona en cuestión.

I.4.7. RECONOCIMIENTO DEL PATRÓN DE VOZ.

La persona que desea el acceso al área controlada, entra primero a una cabina para prueba de voz, en donde se identifica a través de un teclado o tarjeta codificada. Debe previamente recordar el mensaje individual que debe repetir frente a un micrófono, dicho mensaje generalmente está formado por cuatro palabras de dieciséis monosílabos aproximadamente. Estas frases tiene una duración de alrededor de dos segundos. La repetición de la frase en el micrófono es procesada y comparada con los datos en memoria. El sistema compara la amplitud de la onda de voz, además de la frecuencia y el tiempo.

I.4.8. RECONOCIMIENTO DE LA RETINA.

Para un control individual de acceso, en estos sistemas, se analiza el patrón arterial de la retina del ojo. El ojo es expuesto a una cámara que explora el área circular de la retina con un haz de luz infrarrojo de extremadamente baja intensidad. La luz reflejada por el fondo del ojo, es enfocada a un fotosensor que mide la magnitud de la luz en varios puntos distintos a lo largo de 420°. El resultado describe una forma por los datos de los puntos.

CAPITULO II. SISTEMAS LOCALES DE ALARMA Y VIGILANCIA.

Objetivo:

Describir los diferentes tipos de alarmas y sistemas de vigilancia que existen en el mercado, así como sus ventajas y desventajas.

CAPITULO II. SISTEMAS LOCALES DE ALARMA Y VIGILANCIA.

II.1. CIRCUITOS BASICOS.

En un sistema de alarma hay básicamente cuatro partes: los sensores, las sirenas o timbres, la fuente de alimentación que puede ser una batería cargada a través de la red, y la unidad de control.

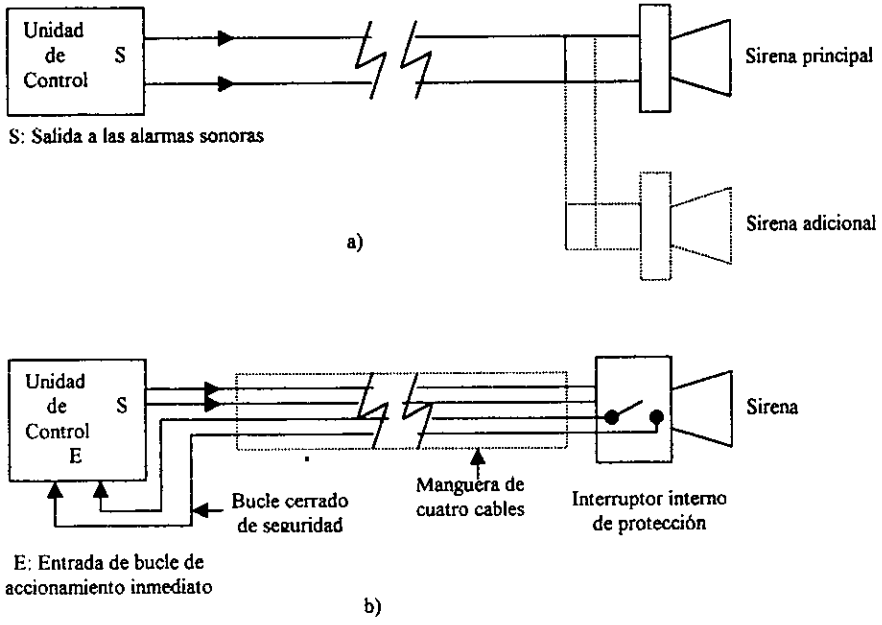


Figura 6. Conexiones realizadas entre la unidad de control y las sirenas.

La interconexión de los sensores y las sirenas o timbres con la unidad de control pueden llevarse a cabo de varias formas. La parte

más sencilla es la conexión de las sirenas. En la figura anterior se muestran dos sistemas de conexionado.

El primero es el más sencillo, pero requiere que los cables estén asegurados contra todo posible sabotaje desde el exterior del recinto de seguridad mediante un tubo de acero o disponiéndolos de forma que no sean accesibles, pasando desde el interior a la sirena directamente a través de un agujero en la pared en la que esté sujeta la sirena.

El segundo circuito es más seguro al llevar en la misma manguera un bucle cerrado, que protege los cables y la propia sirena. En este caso da igual que los cables y la sirena estén al alcance de cualquiera en el exterior, ya que si son saboteados sonará la alarma. Es aconsejable instalar siempre dos sirenas para que suene una al sabotear la otra.

En cuanto al circuito de detección, la figura 7. muestra los más usuales. El primero dispone los sensores normalmente abiertos y en paralelo. En él al darse una anomalía se cierra el contacto y la unidad de control actúa en consecuencia.

El del segundo es el más usado debido a sus claras ventajas respecto al anterior. Aquí los sensores están normalmente cerrados y conectados en serie.

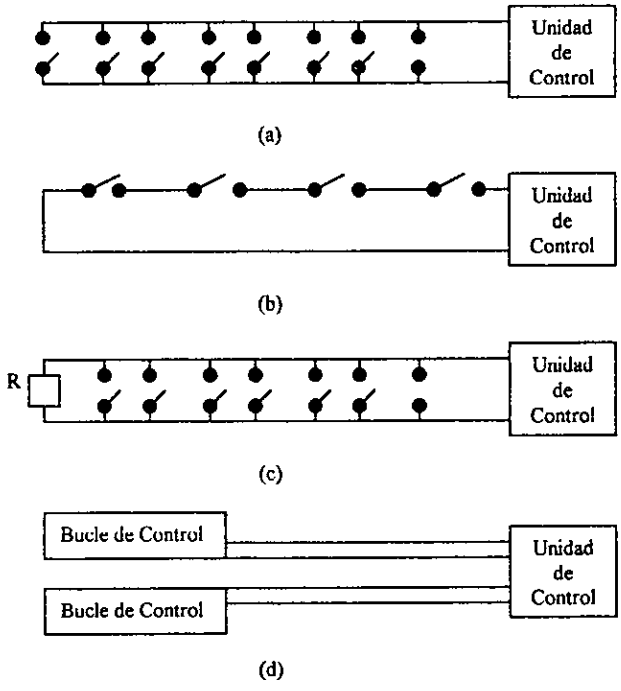


Figura 7. Conexiones de los sensores con la unidad de control
a) En paralelo, b) En serie, c) Serie-paralelo con resistencioa de final de línea, para sensores antiincendio, d) La mayoría de las unidades de control de tipo medio incluyen dos bucles, uno inmediato y uno retardado.

Si se activa cualquiera de los sensores el circuito se abre y la unidad de control da la alarma. El hecho de que la alarma no suene cuando el circuito está conectado demuestra que éste es continuo y que la intensidad pasa a través de él. Por consiguiente, ninguna parte de la instalación ha sido cortada o desconectada accidentalmente y ningún sensor ha sido activado. De este modo los sensores y la

instalación son comprobados para que ninguna parte de ella sea manipulada indebidamente.

Algunos sensores, como las alfombras de presión, están normalmente abiertos y actúan al cerrarlos; éstos requieren otro circuito independiente.

Para evitar que de todas formas pueda ser saboteado el cable del circuito abierto de las alfombras se puede disponer de un cable de cuatro conductores, en el que los dos sobrantes formen un bucle cerrado de protección contra cortes, disparando la alarma al ser cortado éste.

El tercer circuito es muy utilizado en los sistemas anti-incendio para conectar todos los sensores de humo y temperatura. En él los sensores están dispuestos en paralelo y en reposo quedan abiertos. La resistencia R cierra el circuito dejando pasar una débil intensidad. Si se activa cualquiera de los sensores la unidad de control da la alarma, pero si se corta el circuito da una señal de avería sin activar las sirenas.

Este caso no supone el sabotaje de los cables sino que la apertura del circuito será siempre una avería.

Algunas unidades de control, al dar la señal de avería también accionan un pequeño zumbador de aviso.

En prácticamente todas las unidades de control se prevén como mínimo dos circuitos (normalmente cerrados) cuya única diferencia es su tiempo de accionamiento de la alarma una vez detectada alguna anomalía.

El circuito retardado suele ir en las puertas de acceso hasta llegar a la unidad de control para desactivarla antes de que suene la alarma. El circuito inmediato servirá para el resto de los detectores en los que no es necesario este retardo.

II.2. SENSORES PASIVOS.

Esta denominación se aplica a aquellos sensores que no necesitan una alimentación auxiliar para desempeñar su función.

Todos se basan simplemente en un contacto eléctrico, sea abierto o cerrado. El de la figura 8. es un detector de vibración que está compuesto por dos partes, teniendo cada una sus funciones diferentes y reunidas bajo la forma de un apilamiento compacto que luego queda protegido en una carcasa.

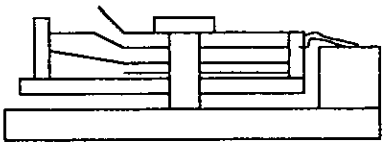


Figura 8. Sensor de vibración de láminas. Se utiliza en cristales de escaparates, joyerías, etc.

La parte activa se halla situada en la posición baja y está constituida por dos láminas superpuestas, una de ellas rígida de material magnético, la otra en acero especialmente tratado y sobrecargada por una pequeña masa calibrada que es el elemento de detección.

La parte pasiva se encuentra situada encima, está constituida también por dos láminas flexibles superpuestas que incluyen cada una un contacto autolimpiador. Cuando la carcasa de protección del detector está puesta, estos dos contactos aseguran la continuidad eléctrica del circuito de guardia: es el elemento de auto-protección. Una lámina rígida y una contra-lámina flexible, las dos de metal, situadas entre las partes activas y pasivas, permiten regular la sensibilidad del detector mediante un tornillo micrométrico. Como se ha dicho, está autoprotegido contra sabotaje con lo cual cualquier intento de apertura de la tapa de protección provoca la alarma.

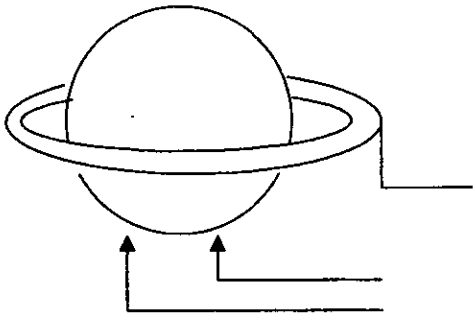


Figura 9. Sensor inercial de bola.

Otra forma de detectar vibraciones consiste en aprovechar otra característica del detector de inercia de la figura anterior, este detector es sensible a los movimientos y a las vibraciones a un mismo tiempo. Se utiliza en cristales, paredes, puertas, cercas etc. Está constituido por una esfera de plata dorada asentada en un par de contactos, formando de este modo un interruptor normalmente cerrado; cualquier movimiento rompe el contacto.

La versión de la figura tiene además un arco alrededor de la esfera que sirve como contacto normalmente abierto; una conmoción produce un contacto entre la esfera y el aro. De esta forma, el sensor tiene ambos tipos de contactos y puede formar un sistema de tres o cuatro conductores. En el caso de tener vibraciones altas de ruido de fondo, se utilizan unos sensores magnéticamente amortiguados para evitar falsas alarmas.

Si la intensidad es alta en el circuito puede tener lugar una deformación de los puntos de contacto. Esto es debido a que la superficie de contacto de la esfera es muy pequeña y también a que el efecto de calentamiento causado por una chispa está concentrado en esta superficie.

Cualquier picadura o protuberancia resultante haría empeorar la futura actuación del dispositivo. En algunos detectores de inercia la intensidad máxima está fijada en 0,2 amperios con una tensión aplicada máxima de 2 voltios. En comparación un detector de vibración puede dejar pasar 1 amperio a 250 voltios.

Otro método para la protección de cristales es la cinta adhesiva conductora de la figura 10. Esta se engancha al cristal de forma adecuada para que cuando se rompa el mismo también se rompa la cinta.

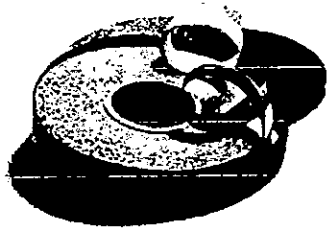


Fig. 10. Cinta adhesiva conductora para la protección de cristales.

La figura 11. presenta detectores magnéticos que superan las limitaciones de los microrruptores normales. Idealmente, un sensor no debería tener partes externas móviles y debería estar completamente protegido por sus contornos. Estos requisitos se cumplen con los captadores magnéticos que tienen en su interior un relé reed accionado por un imán externo Por proximidad. Al separar el imán del relé reed, éste abre el circuito.

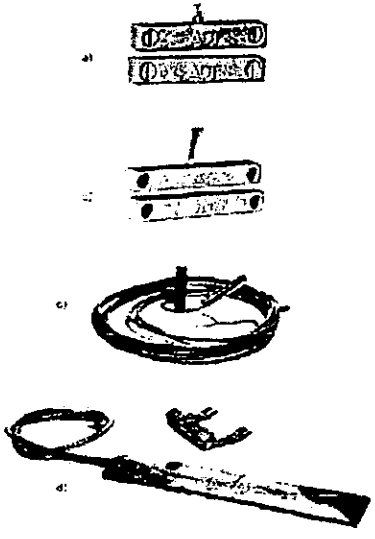


Fig. 11.a) Sensor magnético que detecta la apertura de puertas; b) sensor que permite una mayor separación que el anterior; c) y d) Sensor magnético para portalones, garajes y puertas grandes.

Los hay en diversas configuraciones para hacerlos lo más adaptadas posible a cada aplicación.

Existen almohadillas de presión, flexibles y rectangulares que presentan diversidad de tamaños con contactos en reposo abiertos. También hay alfombras de presión con un gran número de contactos abiertos extendidos en toda su superficie, de forma que cualquier presión en ella cierra algún contacto.

Hay interruptores llamados de onda de aire que son capaces de solucionar muchos problemas relacionados con la sensibilidad mecánica. El cuerpo del interruptor está dividido en dos cámaras mediante un diafragma de alta sensibilidad por el que se detectan los ligeros cambios habidos en la presión del aire. La sensibilidad es tan alta que el interruptor puede activarse por la acción del aliento aplicado a él. Un par de contactos de plata, con separación regulable, pueden actuar normalmente abiertos o unirlos para tener un circuito cerrado. Una onda de presión en una de las cámaras o el vacío en la opuesta, activará el dispositivo. Entre sus aplicaciones están las puertas de cierre automático.

La figura 12 muestra algunos dispositivos especialmente diseñados para impedir el atraco. En ellos el contacto propiamente dicho se realiza con relés reed en baño de mercurio debido a la ausencia de ruido al accionar éstos. Están sobre todo pensados para bancos y joyerías.

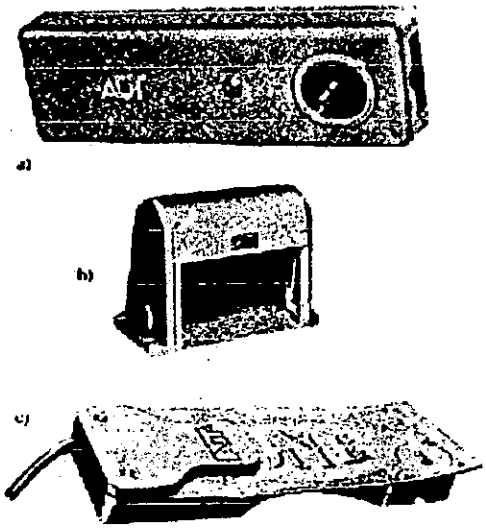


Fig. 12. Dispositivos antiatraco: a)Pulsador antiatraco con enclavamiento; b) pedal antiatraco con ausencia total de ruido al operar por medio de un conmutador con relés de mercurio; c) clip para billetes; su actuación se produce al retirar los billetes introducidos en él.

También existen interruptores de actuación manual por flexión que dispuestos convenientemente, también pueden ayudar a avisar en caso de atraco.

II.3. SENSORES INFRARROJOS.

Veamos ahora los sensores activos (necesitan alimentación auxiliar). Los sensores que se basan en la luz infrarroja son los detectores fotoeléctricos más utilizados hoy en día.

La luz visible casi ya no se usa debido al inconveniente de ser detectada por parte del intruso, con la posibilidad de que pueda esquivar las barreras que se interpongan en su camino.

Su consumo es relativamente bajo, no superando casi nunca los 20 mA con una tensión casi normalizada de 12 voltios. La figura 13 muestra unos detectores de este tipo que están pensados para efectuar su cometido en forma de barrera.

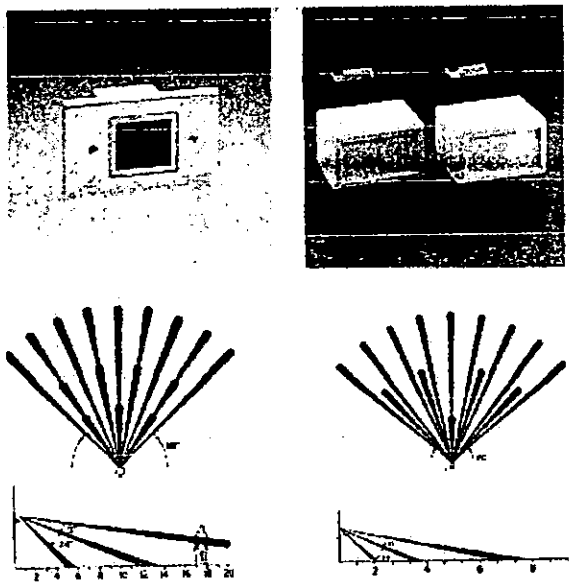


Fig. 13. Detectores volumétricos de radiación infrarroja. En el centro se observa el diagrama de radiación, visto en planta para cada modelo, mientras que en la parte inferior se detalla el alcance en metros de la zona sensible, y márgenes angulares.

La radiación infrarroja es una emisión electromagnética que se extiende por debajo de la parte de la luz visible en el espectro, pero mucho más alta que las bandas de radiofrecuencia usuales.

El margen de la frecuencia es mucho más ancho que la luz visible, (10^{12} hasta 10^{14} Hz) pudiéndose radiar fácilmente mediante un diodo semiconductor emisor de infrarrojos. La recepción tampoco tiene problema mediante diodos adecuados.

Si el rayo es interceptado, el receptor dispara la alarma. Para tener una protección eficaz es necesario disponer adecuadamente los emisores y sus receptores utilizando si es necesario espejos, como muestra la figura 14.

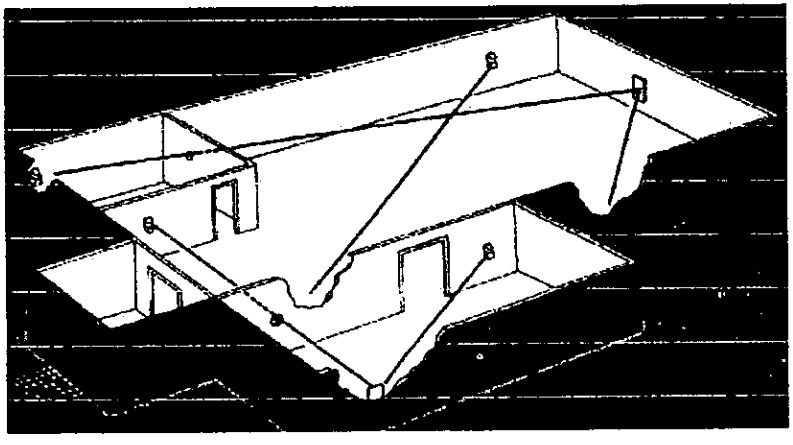


Fig. 14. Barrera infrarroja siguiendo la disposición mediante espejos.

La radiación infrarroja está generada también por fuentes que producen calor. El cuerpo humano o el de cualquier animal, una linterna, una estufa, etc., son generadores de infrarrojos.

Cualquiera de estos generadores podría interferir al receptor de la barrera y un intruso podría engañarlo encendiendo una linterna dirigida hacia él. Para evitar esto se modula la emisión de infrarrojos. La modulación se realiza en amplitud, de forma que el receptor sólo acepta la señal modulada. Si las señales cesan o incluso si se recibe radiación constante se da la alarma. El margen de longitud en las barreras usuales va desde un máximo de 10 metros para unidades muy pequeñas hasta llegar a 300 metros en las más grandes.

Cuando se refleja en un espejo el rayo es atenuado y por ello cada reflexión acorta la distancia a que se puede instalar la barrera.

En una reflexión la longitud se reduce a un 75%, dos reflexiones a un 60% y con tres desciende hasta un 43%. Los rayos también pueden atravesar cristales transparentes reduciendo la longitud eficaz, siendo menor la reducción que en el caso de la reflexión. En el paso de un cristal usual se pierde aproximadamente un 17% quedando un 83%. En dos queda un 70% en tres un 60% y en cuatro un 50%.

Existen otros sistemas que en forma de barrera utilizan los rayos láser, los cuales pueden ser rayos de luz infrarroja de una única frecuencia, no como en los casos anteriores en que eran un conjunto de frecuencias. Estas unidades pueden alcanzar hasta 15 kilómetros con niebla o nieve. El transmisor utiliza un diodo láser de arseniuro de galio (AsGa) con una potencia de aproximadamente un vatio (figura 15).

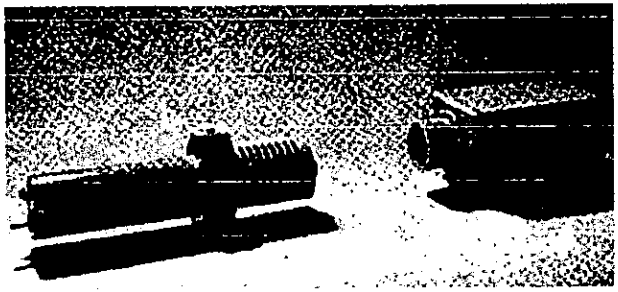


Fig. 15. Barrera protectora que emplea la moderna técnica del rayo láser.

II.4. SENSORES ULTRASONICOS.

Estos sensores utilizan los ultrasonidos, que son señales con frecuencia superior a 20 kHz. Por tanto no son audibles por las personas. Normalmente se utilizan las frecuencias comprendidas entre 23 y 40 kHz. El principio se basa en que un oscilador electrónico genera una frecuencia ultrasónica que alimenta a uno o más transductores ultrasónicos. Los sonidos de alta frecuencia se producen en el espacio protegido y se reciben después por un micrófono alojado en la misma unidad que el transductor. El receptor capta el sonido del emisor y

también el reflejado procedente del objeto en movimiento experimentará un cambio de frecuencia debido al efecto Doppler-Fízeau (figura 16).

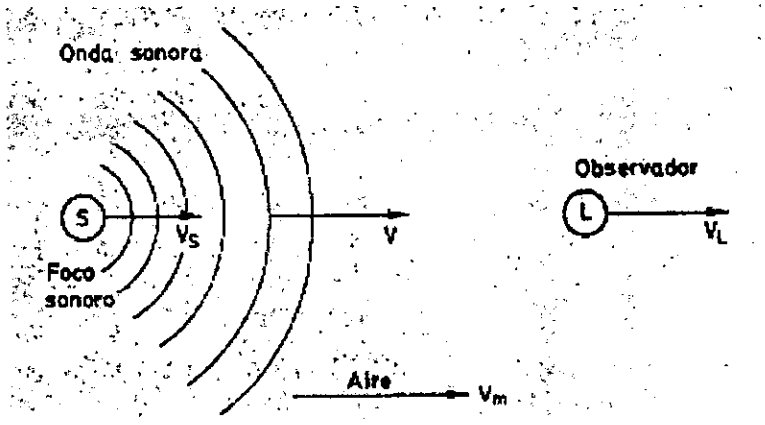


Fig 16. Representación esquemática del efecto Doppler.

Por ello, el micrófono captará frecuencias diferentes, la directa procedente del transductor, la reflejada procedente de los objetos estáticos y la frecuencia reflejada y cambiada procedente del objeto en movimiento. Si se mezclan dos frecuencias cercanas se producirá una tercera frecuencia que es la diferencia entre las anteriores, hecho que se conoce con el nombre de nota de batido.

En este caso, si la frecuencia directa es de 23 kHz y la reflejada Doppler de 22,7 kHz, a frecuencia de batido que aparecerá es de 0,3 kHz (23 kHz-22,7 kHz=0,3 kHz=300 Hz). También se genera la suma de las dos, pero se desecha por ser muy alta para las aplicaciones concretas en que se aplica este sistema. La frecuencia de la «nota de

batido depende de la velocidad del móvil relativa a la unidad detectora, pero siempre será mucho más baja que las frecuencias ultrasónicas que se producen.

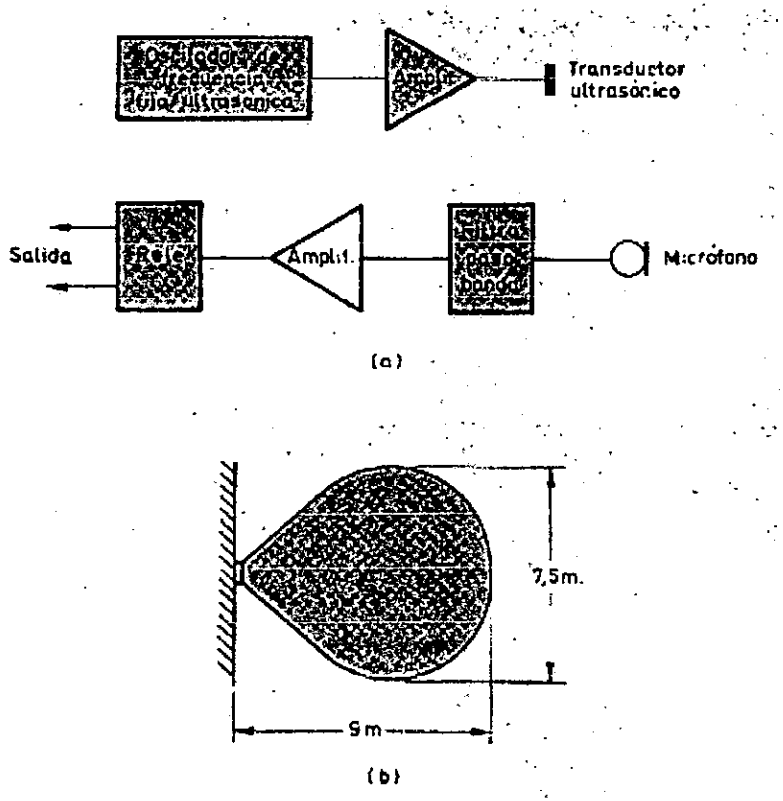


Fig. 17.a) Diagrama a bloques de un sensor volumétrico ultrasónico por efecto Doppler-Fizeau; b) Posible área de protección de un sensor untrasónico

La figura 17 presenta el diagrama de bloques de un detector usual y su zona de protección.

II.5. EFECTO DOPPLER.

Cuando un foco sonoro, un observador o ambos, están en movimiento respecto al aire, el tono (frecuencia) percibido por el observador no es en general el mismo que cuando el foco y el observador están en reposo. El ejemplo más conocido es quizá el descenso brusco de tono que se observa en el sonido emitido por la bocina de un automóvil y que se produce justamente cuando se encuentra y se pasa un automóvil que avanza en sentido opuesto. El fenómeno se conoce con el nombre de efecto Doppler o DopplerFizeau.

En la figura 16, S representa un foco sonoro que se mueve hacia la derecha con una velocidad V_S y emite ondas sonoras de frecuencia f_0. El observador, que se mueve hacia la derecha con una velocidad V_L, está representado por *L*.

Para mayor generalidad se supone que el medio (aire) se mueve también hacia la derecha con una velocidad V_m. Las velocidades V_S, V_L y V_m son todas velocidades relativas respecto a tierra.

Una onda sonora emitida por el foco S en el instante t=0 avanza respecto al medio con una velocidad de propagación V.

La velocidad de propagación de las ondas sonoras en/o respecto al medio es una propiedad que sólo depende del medio y es

independiente de la velocidad del foco (las ondas se olvidan del foco tan pronto como lo abandonan).

Puesto que el medio está moviéndose hacia la derecha con una velocidad V_m, la velocidad de las ondas emitidas hacia la derecha, respecto a tierra es la suma de su velocidad V respecto al medio y de la velocidad del medio respecto a tierra, o sea, $V+ V_m$.

Por consiguiente, en un tiempo t una onda avanza hacia la derecha una distancia $(V+V_m)t$. Durante el mismo tiempo, el foco ha avanzado una distancia V_St y ha emitido f_0t ondas.

Por tanto, f_0t ondas ocupan la distancia comprendida entre el foco y la onda emitida en el instante t= 0, ósea, una distancia $(V+ V_m)t-V_St=(V+V_m-V_S)t$.

La distancia entre dos ondas cualesquiera consecutivas, es decir, la longitud de onda, será por tanto:

$$\lambda = \frac{(V+V_m-V_S)t}{f_0t} = \frac{V+V_m-V_S}{f_0}$$

Consideremos ahora el observador. Las ondas sonoras que pasan por él tienen una velocidad $V+ V_m$, pero su propia velocidad es V_L y la velocidad de las ondas respecto al observador es $V+ V_m-V_L$. El

número de ondas que pasan por el observador por unidad de tiempo, o sea, la frecuencia aparente f, es la razón de la velocidad relativa a la longitud de piedad que sólo onda, esto es:

$$f = \frac{V+V_m-V_L}{(V+V_m-V_S)\,|\,f_0} = \frac{f}{f_0} = \frac{V+V_m-V_L}{V+V_m-V_S}$$

Siendo $f\,|\,f_0$ la razón de la frecuencia aparente a la verdadera.

Cuando se aplica esta ecuación debe prestarse especial atención a la construcción del esquema de partida y a los signos algebraicos. Si en algún caso algunas de las velocidades son opuestas a la de la figura debe invertirse su signo en la última ecuación.

La velocidad de propagación V se considera siempre positiva. El efecto Doppler no queda limitado a las ondas sonoras. La luz de una estrella que se aproxima a la Tierra tiene su frecuencia un poco más elevada o longitud de onda más corta que si las dos estuvieran en reposo relativo. Con microondas también se puede aplicar este efecto, por lo que se pueden construir radares basados en él.

Las desventajas de estos detectores es que tienen propensión a las falsas alarmas. Una frecuencia Doppler filtrada puede ser producida por el aire, a través del cual viaja el sonido, moviéndose de la misma forma que lo hace la superficie reflectora. Debido a esto, los sensores

ultrasónicos no se utilizan en el exterior porque la más ligera brisa podría dar la alarma.

En el interior se deben evitar las corrientes de aire, el movimiento de cortinas y el movimiento de animales. Otra causa posible de falsas alarmas es que los sonidos de tono muy alto originan otros cercanos. Estos pueden tener armónicos que se extiendan en el margen de frecuencias de los ultrasonidos y, debido a esto, pueden producir notas de batido en el sensor.

Otras fuentes de fallos son los frenazos de los vehículos en las calles adyacentes, el silbido de la base de tiempo de líneas procedente de un televisor cercano, fugas en las canalizaciones de aire comprimido, de agua y de gas.

Existen otros sensores que tienen el emisor y el receptor separados y montados en distintas cajas. Se trata de un sensor de ultrasonidos volumétrico que al tener el emisor y el receptor separados proporciona una gran flexibilidad en su distribución. El sistema puede estar compuesto por uno o varios pares emisores y receptores. Las ondas ultrasónicas generadas por el emisor principal recorren todo el volumen a proteger, se reflejan en los distintos objetos situados en el local y finalmente son captadas por el receptor.

Cualquier movimiento registrado en el área vigilada es captado, activando la alarma. El emisor principal suministra la alimentación a los emisores secundarios y los receptores, y vigila las líneas de conexión. El emisor principal recoge las señales procedentes de los receptores y las transmite a la central. Pueden conectarse al emisor principal un máximo de 4 emisores secundarios y 5 receptores, de forma que puedan disponerse de 5 conjuntos emisor/receptor.

Para minimizar los efectos secundarios, la evaluación de las señales se efectúa en una banda estrecha de 25 a 75 Hz.

Aunque no sean ultrasónicos, al tratar con el sonido es conveniente presentar otros sensores que se basan en el sonido para detectar cualquier irregularidad. Uno muy significativo es el mostrado en la figura 18.

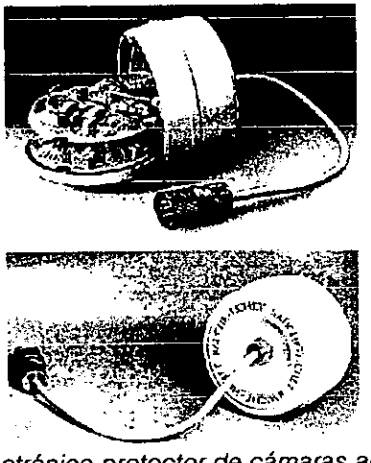


Fig. 18. Sensor electrónico protector de cámaras acorazadas, cajas fuertes y paredes de compartimentos bancarios.

Especialmente estudiado para la protección de cámaras acorazadas, vigila las paredes, las cajas fuertes y los compartimentos bancarios, teniendo como fin detectar vibraciones mecánicas características que se propagan dentro de la estructura de los materiales cuando se produce un ataque con la utilización de las herramientas conocidas hasta hoy (dispositivos de percusión, muelas de diamantes, sopletes, etc.).

El ataque a una caja fuerte, a una cámara acorazada, a compartimentos bancarios, provoca vibraciones mecánicas internas cuyas características varían según las herramientas utilizadas. El principio de la detección de este sensor se basa en la medida de la amplitud y de la frecuencia de estas vibraciones, las cuales se propagan en los materiales en caso de ataque. Cuando su nivel alcanza un punto de referencia en un espectro de frecuencia determinado, se produce una reacción en el detector y las señales registradas son analizadas y puestas en memoria.

Un proceso electrónico permite la discriminación de los efectos de la mayoría de las fuentes parásitas de vibraciones de aquellas que caracterizan un ataque. Si las señales se mantienen o se vuelven a producir durante un tiempo predeterminado, o bien si la amplitud instantánea de las vibraciones es muy importante (caso de ataque con explosivos), la alarma se dispara.

El principio mencionado también está adaptado para la detección de medios de ataque que generan un bajo nivel de vibraciones internas y en particular para las vibraciones consecutivas a la utilización de una lanza térmica. Situado en una pared monolítica de cemento armado, su detección cubre un radio de 5 metros (es decir una superficie aproximada de 80 m^2).

Existen dos versiones: una para vigilancia de paredes de cámaras acorazadas y otra para las cajas fuertes y compartimentos bancarios.

II.6. SENSORES DE MICROONDAS.

Los sistemas de alarma por microondas se utilizan para proteger áreas similares a las regularmente protegidas por los sistemas basados en el método ultrasónico, pero se pueden instalar en el exterior.

La mayoría de los sistemas corrientes emplean dispositivos que se basan en el efecto Doppler, empleando frecuencias portadoras de radio frecuencia en la banda de UHF (ultra hígh frequency) o microondas. El sistema ofrece una total cobertura de pared a pared y de techo a suelo y está dotado para la protección de áreas superiores a 850 metros cúbicos por unidad. La frecuencia utilizada está situada usualmente entre 800 M Hz y 15 GHz.

Estas oscilaciones se proyectan en forma de ondas de radio desde un radiador como un haz. La potencia radiada varía, aunque generalmente es de unos 10 mW. Como en el caso de los de uitrasonidos, al detectar cualquier movimiento dan la alarma. Lo más notable de las microondas es que pueden atravesar la madera, el cristal, el yeso e incluso, con una extensión limitada, los ladrillos.

Esto puede tener tantas alarmas el haz no deberá ser mayor que el recinto que tiene que ser protegido. La mayoría de los sensores tienen posibilidad de ajuste de la potencia emitida.

Las microondas están atenuadas por la lluvia y la niebla. Otro riesgo, en las instalaciones exteriores, son los pequeños objetos, pájaros y papeles arrastrados por el viento, que pueden interceptar el rayo y causar una falsa alarma. La solución adoptada por algunos fabricantes es establecer un tamaño mínimo para los objetos interceptores de haces que podrían producir una alarma.

Lo mismo que con los sensores ultrasónicos, es virtualmente imposible anular un sistema de microondas que esté trabajando, siendo detectada cualquier aproximación a los sensores.

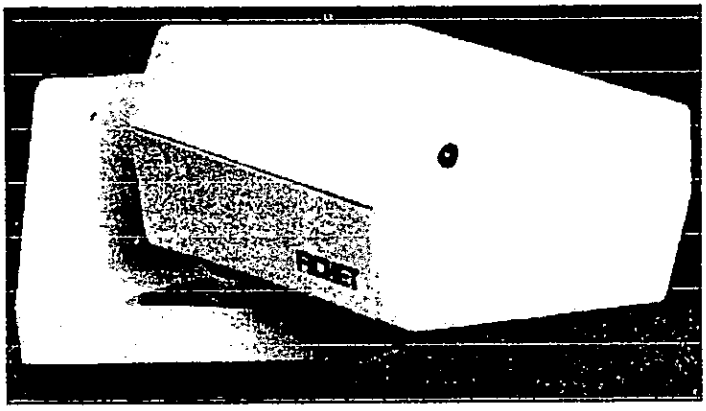


Fig. 19. Sensor volumétrico de microondas fijado en la zona alta de la pared.

Estos sensores tienen varias configuraciones. Una de ellas es la mostrada en la figura 19, parecida a la de los ultrasónicos. Otras están diseñadas para su trabajo como barreras exteriores de protección, semejantes a las puestas en la instalación presentada en la figura 20. Esta puede tener en cada enlace una longitud de 15 a 150 metros y una anchura de 2 a 6 metros, sin estar afectada por fuego, nieve o niebla. Hay otros modelos con radiación radial para ser montados en el techo y así hacer que los objetos de metal, como grandes máquinas, no puedan ocultar a un intruso. Otros no utilizan el efecto Doppler, sino que transmiten un haz estrecho al receptor situado en un punto remoto (parecido a la barrera mencionada antes).

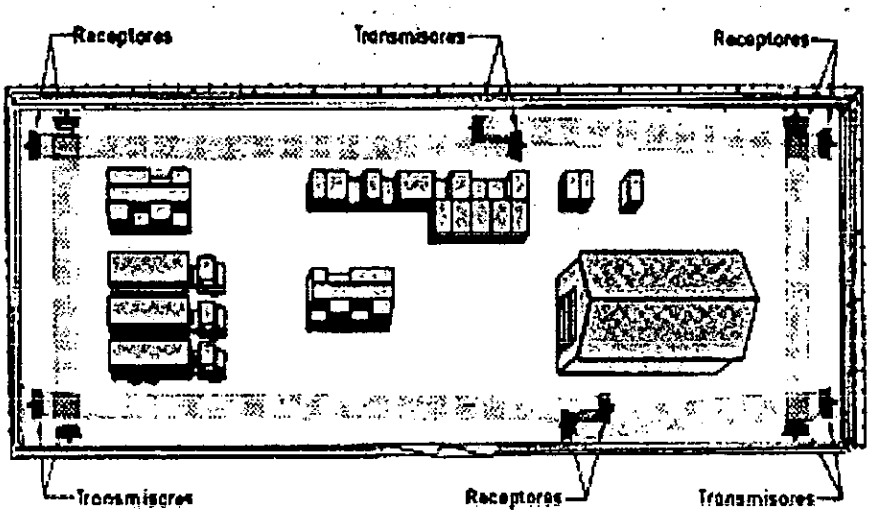


Fig. 20. Sistema protector de tipo perimétrico que emplea las microondas como medio protector.

Existen sistemas que utilizan microondas para proteger perímetros. Estos sistemas utilizan cables especiales enterrados en los que actúan las microondas enviadas por un emisor. Como se ilustra en la siguiente figura, el transmisor se conecta a un cable transductor y un receptor se conecta al otro cable. Unos impulsos cortos de VHF (very high frequency) provocan una onda de superficie que se propaga a lo largo y fuera del cable del transmisor. Una parte de esta onda de superficie se acopla en el cable receptor y éste la envía al receptor. La variación de la amplitud de esta onda en función del tiempo es

demodulada y, si no hay ningún intruso, la forma de onda demodulada permanece estacionaria.

Cuando un intruso entra en el campo de acoplamiento entre los cables causa una modificación en la forma de onda demodulada, la cual puede ser detectada mediante un sistema digital. La forma de onda S_1, se pasa a digital y memoriza mediante un procesador (S_2).

Este procesador puede realizar la diferencia entre señales (S_3) detectando la presencia de un intruso cuando esta diferencia supera un umbral preestablecido. La localización mencionada se determina por el tiempo de retardo entre el comienzo del impulso emitido y la recepción de la perturbación en la forma de onda demodulada. El resultado se lleva a una señal acústica y a otra visual. (visualizador o display de LEDS).

II.7. SENSORES DE INCENDIO.

La figura 21 muestra varios de los sensores que se (utilizan en la detección de incendios. En función del tipo de fuego a detectar y de la futura situación del detector se determinará el tipo a utilizar. Dentro del campo de la detección el tipo más perfeccionado y eficaz en la mayoría de los casos es el detector iónico.

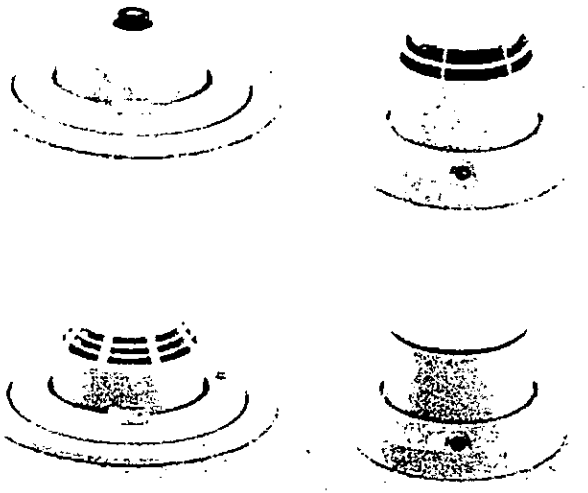


Fig. 21. Distintos tipos de sensores detectores de incendios. Se fijan en paredes y techos.

Cuando se inicia la combustión normalmente se desprenden gases y humo no visibles al ojo humano, pero que sí alteran las condiciones ambientales del lugar donde ocurre la combustión. Esto provoca la alarma.

El sensor iónico se compone básicamente de dos cámaras separadas entre sí, ambas están constantemente ionizadas por una fuente de material radioactiva (americio 241) situado en la cámara interior o de referencia.

Esta atmósfera ionizada, al serle aplicada una tensión entre las cámaras, crea una débil corriente de iones que en condiciones normales

es idéntica en ambas cámaras, manteniendo el potencial medio constante.

Cuando se produce un desprendimiento de gases o humos por la combustión y éstos llegan al detector penetrando en la cámara exterior, chocan con la corriente de iones, impidiendo así su movimiento al hacer que las partículas ionizadas sean más pesadas, con lo que se produce un desequilibrio entre las dos cámaras, aumentando el potencial y disparándose el circuito electrónico que transmite la señal de alarma a la central.

La radiación del material de la fuente radioactiva es en forma de rayos alfa y gamma blandos. El campo de los rayos alfa es muy corto, aproximadamente de unos 4 cm, por lo que no pueden pasar de la cámara exterior y solamente son emitidos por el sensor los rayos gamma blandos, cuya radiación se controla para que no sobrepase el valor de 1,5 microcuries por hora a una distancia de 5 cm desde la superficie del sensor, este valor es inofensivo por estar por debajo de la radiación normal del ambiente admitida y que está estimada en 5 microcuries por hora.

Los sensores termovelocimétricos también se utilizan en la detección de incendios. Estos se basan en el principio del aumento de la presión del aire por el aumento de la temperatura. Están pensados de forma que mientras el aumento de temperatura es menor de 2º

centígrados por minuto, la diferencia de presión es compensada por la cámara interior en comunicación con el aire exterior, pero en cuanto dicha temperatura aumenta a una velocidad superior, la presión aumenta poniendo en situación de alerta al detector hasta que se dispara la alarma a la temperatura prefijada, que normalmente suele ser de 70ºC, cubriendo normalmente un área de 80 m^2.

Otro sistema de detección termovelocimétrica utiliza termistancias como elementos detectores de la variación de la temperatura. Usualmente se combinan estos sensores con sensores estáticos de temperatura, a base también de termistancias.

Los detectores ópticos de humos se componen de una cámara que estanca en el interior a la luz exterior, en la que va montado un diodo emisor de luz con una célula fotoeléctrica o un fototransistor, de forma que la luz emitida por el diodo no llegue a la célula si no es por refracción de la luz sobre las partículas de humo que penetran en el detector, en cuyo momento la luz reflejada alcanza al fototransistor activando el circuito de alarma.

Son muy adecuados para materiales que pueden arder sin llama pero que desprenden humo en mucha cantidad como el PVC, por ejemplo. Este efecto de dispersión de la luz se llama efecto Tyndall. Las corrientes de reposo no superan los 200 μA, y activados los 100 mA.

Los sensores ópticos de llamas funcionan a base de una célula fotosensible situada en el exterior del mismo para captar las radiaciones de los rayos infrarrojos que emite el fuego. Para evitar falsas alarmas producidas por emisores de puntos caloríficos normales, como la calefacción o el alumbrado, la señal que da la célula es analizada por un circuito electrónico que rechaza las que no son emitidas por una llama oscilante de 5 a 1 0 Hz, en cuyo caso da la alarma.

Todos estos detectores llevan incorporado un indicador luminoso que señala exteriormente su activación.

II.8. INDICADORES DE ALARMA.

Un indicador de alarma puede ser una lámpara, un zumbador, una sirena, un timbre, etc. Estos deben tener un sonido fuerte para que pueda ser oído en una gran extensión. Puesto que el sistema de alarma completo culmina en el dispositivo indicador y tiene un gran riesgo para los intrusos, pero si se sabotea toda la instalación queda inútil. Por ello es conveniente instalar más de una sirena o timbre como sistema redundante también es aconsejable disponer de un marcador automático telefónico que nos avise a nosotros y a la policía o bomberos. Para una seguridad óptima, el sistema debe estar diseñado para trabajar satisfactoriamente a partir de baterías de reserva y esto significa la limitación de la intensidad del dispositivo de alarma en un

valor que pueda ser sostenido por las baterías hasta una media hora antes de que se agoten.

El nivel de sonido en decibelios (dB) generado por un dispositivo acústico de alarma necesita ser alto. El oído humano no responde linealmente al nivel de sonido, lo hace de una forma logarítmica. Esta característica permite al oído contener, con un amplio margen, sonidos muy altos de nivel y escuchar perfectamente sonidos muy tenues. Cualquier ruido por encima de 80 dB se considera usualmente alto. El umbral de dolor se alcanza a 130 dB. Una cuestión importante es que la presión sonora decrece con la distancia.

Si una fuente de ruido da a tres metros de distancia un nivel de 90 dB, este nivel habrá decrecido a 70 dB a 30 metros. La sonoridad de la señal de alarma implica una intensidad alta ya que se requiere mucha potencia para producirla.

El dispositivo de alarma más común es el timbre, de todos conocido. Es conveniente, en el caso de alarmas antirrobo, encerrar el timbre en una caja metálica antisabotaje. Cuando se requieran fuentes de sonido extraordinariamente fuertes o que deban ser oídas a distancias muy grandes se deberán utilizar sirenas.

CAPITULO III. SISTEMAS CENTRALES DE TELESUPERVISION.

Objetivo:

Mencionar las principales consideraciones que se deben tomar en cuenta para la instalación de centrales de control y vigilancia.

CAPITULO III. SISTEMAS CENTRALES DE TELESUPERVISIÓN.

III.1. UNIDADES DE CONTROL O CENTRALES.

La unidad de control es el corazón de todo el sistema de alarma, determinando la flexibilidad, la facilidad, la eficacia, la fiabilidad y la explotación del sistema. Su primera función es procurar el enclavamiento del circuito, de forma que la alarma continúe sonando después de haber sido disparada por el sensor que haya activado el intruso, el fuego o el mismo propietario de la alarma como consecuencia de un atraco.

Es esencial disponer de medios para verificar el sistema a fin de detectar cualquier anomalía en la seguridad, debiendo ser éste silencioso. En la unidad de control se encuentra también la fuente de alimentación de ella misma, de todos los sensores y de los indicadores de alarma. Las centrales antirrobo pueden tener también circuitos para antiatraco. Las más usuales disponen de un circuito retardado y uno inmediato como mínimo. El retardado puede llegar a tener un tiempo de retardo ajustable de 0 a 120 segundos.

El circuito de atraco es normalmente abierto y los de robo cerrados. Los circuitos inmediatos pueden ser más de uno para poder discriminar entre distintas zonas protegidas, permitiendo la conexión o desconexión de cada zona por separado y la indicación luminosa

independiente de su activación, sabotaje o avería, al tener posibilidad de conectar los sensores por zonas es fácil detectar falsas alarmas, si las hay, y saber qué sensor o conjunto de sensores conectados a una zona las ha provocado, debido a que cada zona tiene una memoria. Esta memoria actúa en todo momento, pero se puede decidir si se quiere activar el indicador de alarma o no. Esta característica permite la puesta a prueba de las instalaciones recién terminadas sin necesidad de molestar a nadie dando la alarma externa innecesariamente. Este factor es importante ya que, de lo contrario, podrían acostumbrarse a las falsas alarmas y no dar la debida importancia en un caso real de robo o incendio.

La salida de las unidades de control es, en la mayoría de los casos, un relé con varios circuitos de salida, a los cuales se pueden conectar las sirenas, timbres o marcadores telefónicos necesarios. Cuando se da una señal de alarma y desaparece, el relé conecta los indicadores de alarma durante 2 ó 5 minutos. Si la señal de alarma no desaparece, el relé mantiene conectados los indicadores hasta que se agota la fuente de energía o se desconecta la unidad de control mediante la típica llave de seguridad.

La unidad de control deberá estar en un lugar protegido y disponer de llave de seguridad o de codificación secreta. Las operaciones a realizar son: conectar la central y abandonar el local con el cierre de todas las puertas protegidas. Si la central pasara a funcionar

totalmente desde un primer momento, al abrir cualquier puerta se dispararía la alarma; para evitar esto, se recurre a colocar todas las puertas que debe recorrer quién conecte la alarma en el circuito de retardo mencionado anteriormente o bien, si están en el circuito inmediato, instalar una central que retarde todos los circuitos (inmediatos más retardados) al conectarla durante unos minutos (2 a 5) (tiempo de salida) independientemente del tiempo que se haya determinado para el tiempo de entrada (circuito retardado). Es decir que en la central se tendrán tres tiempos de retardo a tener en cuenta: tiempo de entrada, tiempo de salida y tiempo de alarma.

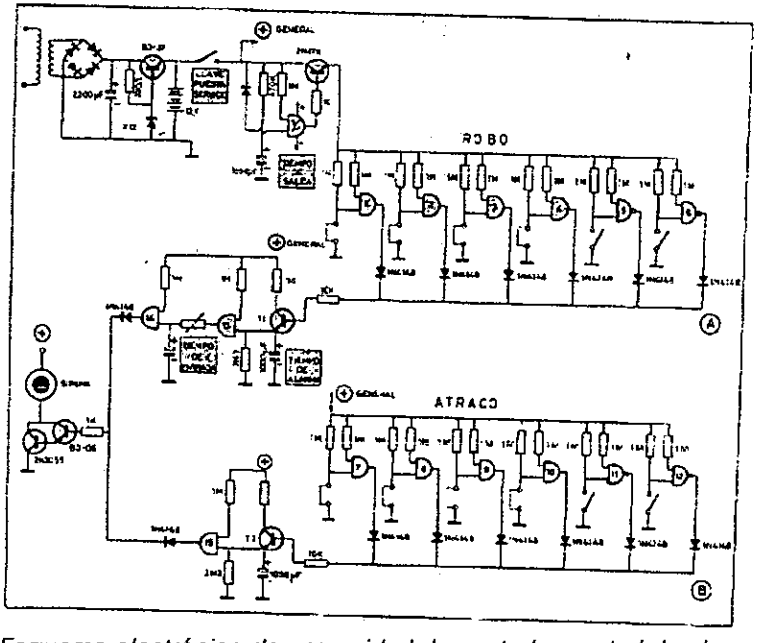


Fig. 22. Esquema electrónico de una unidad de control o central de alarma.

La figura 22 presenta un esquema práctico de una unidad de control con las siguientes características: 4 bucles o circuitos cerrados de robo, 2 bucles abiertos de robo, 4 bucles cerrados de atraco, 2 bucles abiertos de atraco, tiempo de entrada regulable entre 0 y 2 minutos, tiempo de 1 salida regulable entre 0 y 2 minutos y tiempo de alarma de 3 minutos más el tiempo que tarde en desaparecer la causa de la alarma. Su consumo en reposo no supera 20 mA. Al colocar la llave de puesta en marcha en ON, aparece inmediatamente la tensión de 12 V para los circuitos correspondientes al atraco, pero se debe esperar un tiempo mínimo (tiempo de salida) para que esta tensión aparezca en los circuitos correspondientes a robo.

En este intervalo, cualquier apertura o cierre de un lazo de robo no repercutirá en la señal de alarma. A partir de ese momento la central comienza a funcionar en su estado operativo normal. Una apertura de cualquiera de los lazos correspondientes a atraco proporciona un nivel alto en B, suficiente para saturar el transistor Tr_2 que carga al condensador que va unido al emisor.

Mientras persista este nivel alto se mantendrá la alarma y en el momento en que desaparezca la causa de alarma el nivel en B pasa a bajo, con lo que Tr_2 se bloquea y es la célula RC la que determina el tiempo de permanencia de alarma (minutos). La apertura de un bucle (o cirre) correspondiente a la zona de robo origina el nivel alto en A, lo que satura Tr_1 cargando el condensador C_i, el cual origina un nivel alto en la

salida de la puerta Y nº 13 que ataca a la célula RC de constante de tiempo variable, la cual determina el tiempo de entrada.

Como se puede observar, el diseño de las unidades de control admite muchas variantes y por ello el futuro instalador debe conocer las posibilidades de las unidades de control que potencialmente debe instalar para asegurar un proyecto de seguridad óptimo.

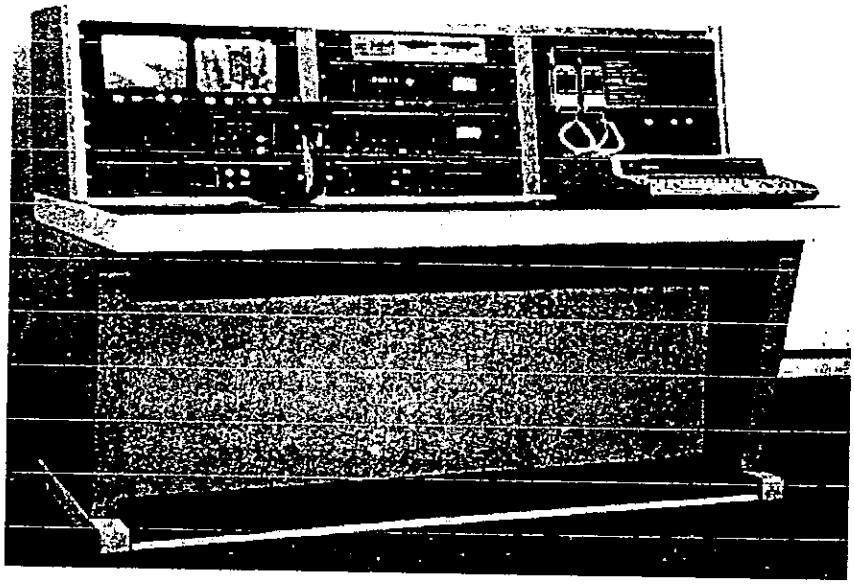


Fig. 23. Sistema centralizado de alarmas de radio. En una amplia consola puede tenerse información visual o sonora de los diversos puntos a proteger.

En las instalaciones muy complicadas de alta seguridad y dado el actual dominio de la microelectrónica, se disponen unidades de control

de gestión informática de las alarmas por grado de urgencia con un tratamiento mediante consignas de seguridad figura 24.

La detección de las alarmas se realiza de la misma forma, repartida en zonas. En estos casos la seguridad es integral y agrupa también los sensores de incendio e incluso los actuadores necesarios para apagar el fuego en el lugar en que ocurra.

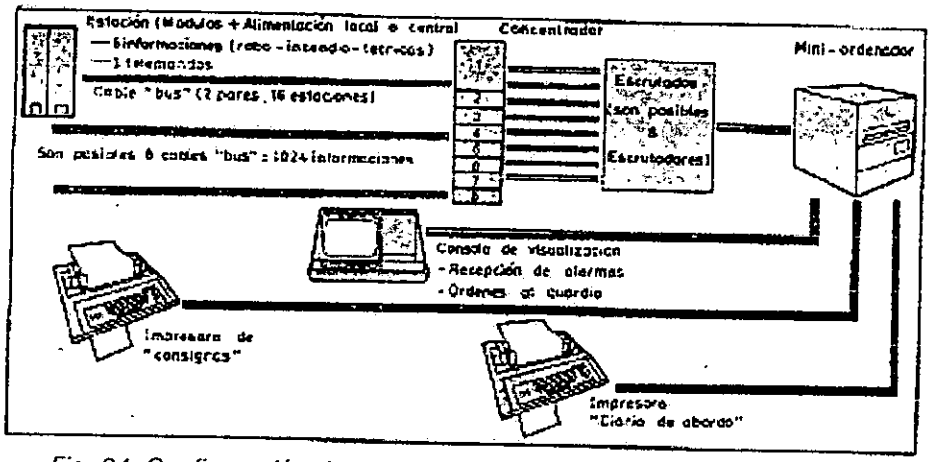


Fig. 24. Configuración de un sistema informático de control de alarmas.

Pero además, se pueden procesar informaciones provenientes de detectores de presión, nivel, humedad, etc. para dar distintas alarmas en función de la causa. Además de estas alarmas se puede poner en marcha el circuito cerrado de TV de vigilancia, el aviso de incendio a los bomberos, así como dar la alerta de los responsables de la seguridad, el cierre de las puertas corta-fuego, la apertura de las puertas de ventilación. Todas estas disposiciones se hacen funcionar desde unos

circuitos de mando específicos para cada una de ellas. Los detectores y dispositivos de alarma o de telemando se unen con una unidad de gestión a través de un sistema de colección y distribución que constituye la red de transmisión.

La transmisión o enlace con la unidad de control o gestión se realiza mediante estaciones modulares, cables interfaces y dispositivos de seguridad de línea. Las estaciones modulares se componen de dos módulos acoplables. Uno es el encargado de la recepción y memorización de las informaciones que le dan los sensores. El otro transmite estas informaciones a la unidad de gestión y de esta unidad recibe las órdenes de telemando, distribuyéndose a los distintos órganos en cuestión. Cada una de las estaciones posee una dirección distinta y se le interroga permanentemente. El cable BUS asegura el enlace entre las estaciones y la unidad de gestión. Un solo cable telefónico estándar de dos pares, apantallado, es suficiente para hacer el servicio de 16 estaciones. Una unidad de gestión admite en base 8 cables BUS, o sea, una capacidad para 128 estaciones, pudiendo reunir 1.024 informaciones y distribuyendo 384 telemandos de dos situaciones. Por simple extensión es posible conectar varias decenas de cables BUS a la unidad de gestión y proporcionar así 2.048, 3.072 etc. informaciones al igual que 768, 1.1 52 etc. telemandos.

La unidad central de gestión consta de un minicomputador y de una unidad de discos flexibles o en cartucho. El minicomputador

programado en tiempo real rige la explotación de toda la instalación de seguridad. El conjunto de procedimientos se pone en memoria y un importante número de operaciones se efectúa automáticamente en función de programas determinados con antelación. Cuando se trata de una alarma de robo, por ejemplo, dará la alarma a los empleados de seguridad con los medios adecuados. No se prevé el acceso directo del empleado a los programas, con el objeto de salvaguardar la integridad de la instalación. La modificación de los programas siempre la efectúa la empresa instaladora.

El usuario sólo tiene acceso a la modificación de los datos. El conjunto de datos relacionados con la gestión de las informaciones aparece en la pantalla y se retiene en memoria tratándose éstos en función de los acontecimientos. La gestión de las alarmas se realiza en función del grado de urgencia preestablecido: puede controlar la reacción de los guardianes, editar automáticamente las consignas en lenguaje claro, gestionar automáticamente la puesta en marcha y fuera de servicio de las zonas de los sensores e identificar completamente una alarma incluyendo su fecha y hora.

Ciertos programas aseguran la gestión automática de varias tareas con el objeto de facilitar un poco los servicios de seguridad: el pasar al estado de alarma o la vuelta a la situación normal da lugar a un mensaje claro acerca de cada acontecimiento, pudiendo ser consecutivo a la puesta en marcha o al fuera de servicio de una zona.

Se prevén varios programas de ronda y cada uno de ellos da lugar a un control durante su transcurso. Cuando la pantalla está saturada las alarmas que han de llegar y son de prioridad inferior son almacenadas en una cola de espera y van apareciendo después, a medida que van siendo registradas. La presentación de las alarmas también se realiza opcionalmente mediante impresora.

Centrando la exposición en las unidades de control contra-incendio diremos que éstas tienen un comportamiento semejante a las de robo y atraco, pero con algunas variantes. Incluso entre ellas hay muchas peculiaridades en función de la marca, la complicación del local a cubrir, el sistema de extinción, etc. Normalmente, a diferencia de las de robo/atraco, funcionan con una tensión de corriente continua de 24 V (las otras a 12 V). Dan la indicación de alarma de forma visual y acústica, disponiendo también de indicadores de avería en los sensores, fallo de tensión, corte acústico, indicador de servicio, pulsador para la comprobación general de los bucles y los indicadores de alarma. Desde las mismas se pueden enviar señales de acción o de alarma a toda clase de sistemas como sirenas, válvulas, sistemasautomáticos de extinción de incendios, etc.

La figura 25 da un esquema de posibles actuaciones de una unidad de control de incendios. Como se ve, pueden disponer de un circuito especial para pulsadores manuales de alarma.

Las líneas de campanas, una por zona, son medidas continuamente, produciéndose la alarma cuando la línea se encuentra abierta. Para evitar que al producirse una alarma ésta suene inmediatamente, lo cual puede ser peligroso en particular si es falsa, las alarmas son retardadas un cierto tiempo programable, permitiendo de este modo realizar una comprobación de la alarma producida. Si en el momento en que se produce la alarma el encargado de servicio de seguridad está atento y acciona el pulsador luminoso de enterado; el retardo en la actuación de las campanas es ampliado. Pueden instalarse pulsadores para la detección de la alarma en caso de que ésta sea falsa, encendiéndose el indicador de detención.

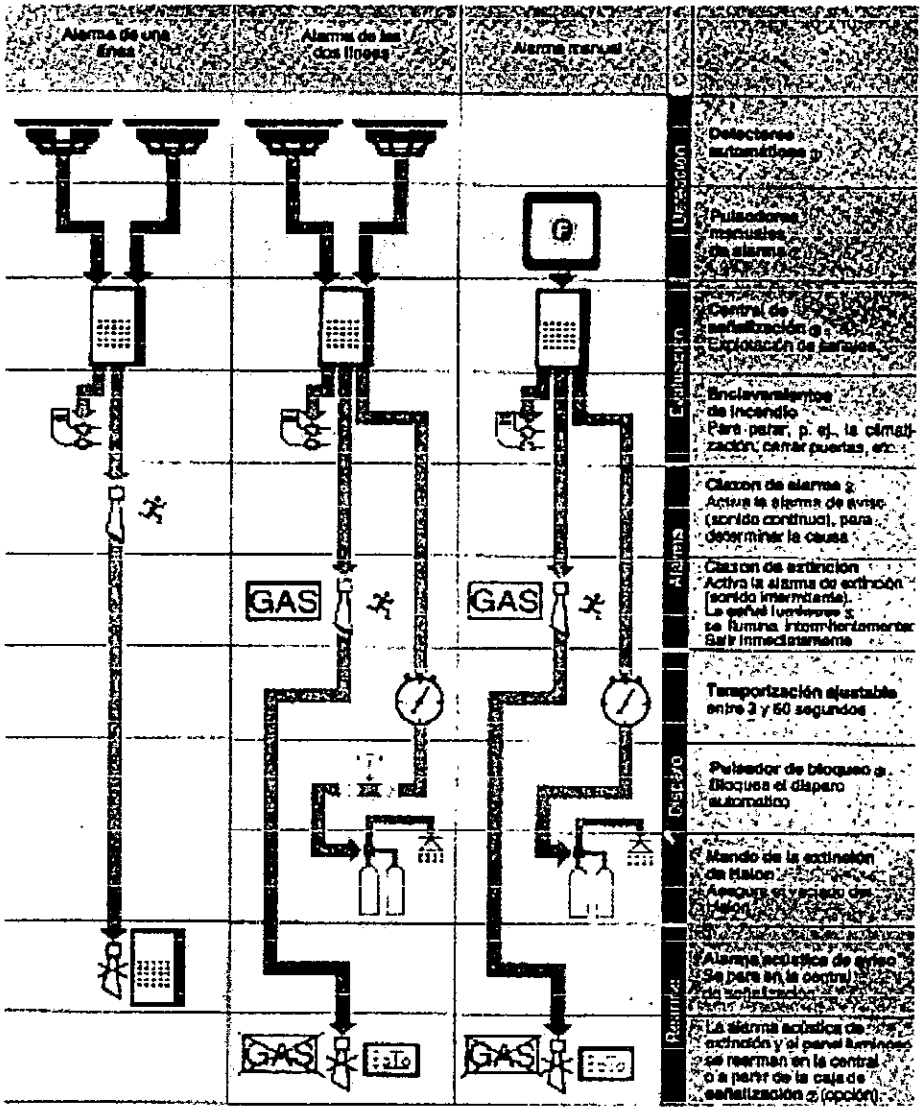


Fig. 25. Diferentes posibles actuaciones de una unidad de control.

Las fuentes de alimentación de todo el sistema se incluyen usualmente en las propias unidades de control. También existen

sistemas en que hay sensores autoalimentados o indicadores de alarma también autoalimentados. Las fuentes de alimentación constan de una batería de tipo hermético sin mantenimiento y de una fuente de alimentación propiamente dicha estabilizada para la carga de la batería y el suministro de energía a todo el sistema cuando hay energía de la red. De esta forma la batería no se descarga en funcionamiento normal y sólo entra cuando falla la red eléctrica. En ese momento las baterías alimentan todo el sistema durante un tiempo máximo que varía según la instalación y la propia batería, pero que usualmente se calcula de unas ocho o diez horas si no se disparan las alarmas. Si ello ocurre y la instalación es pequeña, ya se ha dicho que el tiempo máximo de actuación se prevé para unos 20 ó 30 minutos, cuando la causa que ha provocado la alarma no cesa. En las instalaciones mayores, en las que se quiere mayor seguridad, se recurre a los sensores e indicadores de alarmas autoalimentados. En este caso las baterías dispuestas en el interior de los sensores e indicadores se cargan también a través de la fuente de alimentación estabilizado de la unidad de control.

III.2. INSTALACION DEL SISTEMA DE SEGURIDAD.

La protección que ofrece un sistema de seguridad depende de la forma en que éste se instala y de la fiabilidad de sus componentes; si éstos se conectan con alambres fácilmente accesibles para los intrusos y las interconexiones se realizan con empalmes de alambres descubiertos, el nivel de seguridad será bajo. Los dispositivos eléctricos

y electrónicos se clasifican en términos de TMAF (tiempo medio antes de fallar), expresados en horas y con unas condiciones específicas.

Un elemento que ha sido diseñado para funcionar dentro de un local no es fiable si se usa en el exterior. En el caso de los relés, muy usados en este tipo de instalaciones, están afectados por el tiempo y el número de veces que operan, así como el medio donde se usan. Serán más fiables los relés reed que los convencionales. Al instalar un sistema se puede caer en el error de adquirir componentes baratos, lo que puede llevar a tener problemas de falsas alarmas y costos elevados de mantenimiento.

Para planificar un sistema de seguridad se deberá emplear la técnica de ponerse en el lugar del ladrón o saber los máximos riesgos de incendio de cada zona. Se deben proteger todos los accesos externos o bien los accesos internos que sean necesarios para detectar con seguridad el paso de un intruso. La unidad de control deberá situarse en un lugar disimulado, de forma que su visión por parte de un intruso no sea casual ni fácil. También se debe disimular el cableado. El cableado del indicador de alarma, sobre todo si éste es único, merecerá una atención especial dado que es el más vulnerable. Si se sabotea este cableado, la totalidad del sistema estará fuera de servicio. No se pueden dar normas generales de instalación ya que cada caso es independiente y necesita soluciones distintas. Lo único a tener en cuenta siempre es

pensar lo que podría hacer un intruso o dónde se podría declarar un incendio más fácilmente.

CAPITULO IV. APLICACION DE LOS SISTEMAS ELECTRONICOS DE SEGURIDAD.

Objetivo:

Describir las características de los principales usos de los sistemas electrónicos de seguridad.

CAPITULO IV. APLICACIÓN DE LOS SISTEMAS ELECTRONICOS DE SEGURIDAD.

IV.1. APLICACIONES ESPECIALES.

Además de todos los sistemas mencionados siempre surgen nuevos problemas que no se pueden resolver con los procedimientos usuales. Es entonces cuando se aplican otros medios no tan normales. En el caso de elementos antiatraco se emplean placas de alarma para rodilla, pulsadores montados en pedales accionados con los pies, cámaras fotográficas de vídeo o cinematográficas.

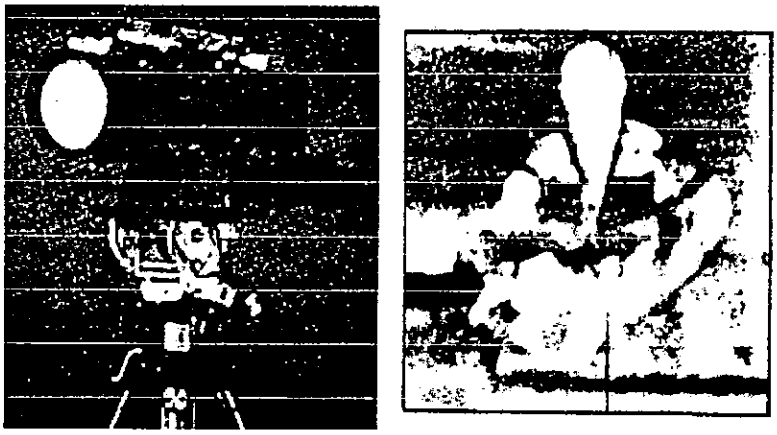


Fig. 26. Sistema de observación nocturna, basado en la utilización de los rayos infrarrojos. A la derecha de la cámara se observa una imagen obtenida en la obscuridad.

Las cámaras fotográficas son elementos de seguridad antíatraco, estando previstas para actuar en caso de sospecha o agresión real de forma remota, proporcionando fotografías claras del sospechoso o agresor, incluso en condiciones de poca luminosidad sobre película de 35 mm. Las cámaras garantizan la identificación del delincuente, por lo que su instalación ejerce una acción disuasoria sobre él. La cámara se activa partiendo de una señal eléctrica producida por cualquier elemento de detección conectado al sistema.

Para evitar el sabotaje, estas cámaras están alojadas en cajas de acero y todos los circuitos electrónicos y cables pasan por el interior del soporte, quedando el objetivo protegido contra el polvo y las manipulaciones involuntarias y mal intencionadas por medio de un cristal. Las cámaras cinematográficas, en lugar de realizar fotografías filman las secuencias del posible o real atraco en cuanto se les da la orden de forma eléctrica con una velocidad de dos fotogramas por segundo.

La película de uno u otro modo (fotos o cine) está depositada en una caja autónoma parecida a un cassette de fácil cambio.

Siguiendo con los elementos antiatraco cabe mencionar los sistemas de control de accesos, estos sistemas confieren un mayor grado de seguridad y se recomiendan particularmente en los locales de alto riesgo (figura 27).

Cada usuario compone la misma clave numérica de grupo, la apertura numérica del acceso controlado se obtiene o no, mediante la introducción de la tarjeta en el lector y la composición de una clave numérica de grupo sobre el teclado. Los diferentes programas posibles están registrados en una unidad de programación y ofrecen una selección muy variada de modos de funcionamiento: lectura de tarjeta únicamente, codificación numérica únicamente y las dos funciones a la vez. Toda búsqueda de la combinación de la clave se señala después de uno, dos o tres errores de manipulación en el teclado.

Fig. 27. Accesos de seguridad colocados a la entrada de una empresa.

Todo usuario de este control de acceso puede señalar discretamente las presiones morales o físicas de las cuales él puede ser objeto. Es suficiente con poner en el lugar de la última cifra de la

combinación, otra cifra determinada con antelación. Esta codificación dará la apertura deseada, pero a la vez liberará un contacto especial en la unidad de programación con el que resulta posible una alerta secreta y discreta. Hay otros lectores en que cada usuario posee una tarjeta y una clave numérica personalizada, funcionando por lo demás como las anteriores.

Fig. 28. Arco detector de metales aplicado a la detección de armas.

Otro sistema que se utiliza como un control de accesos son los arcos detectores de metales para la detección de armas como protección contra atraco, robo o sabotaje (figura 28), están

especialmente diseñados para indicar la presencia del metal, al paso de una persona, bolso de mano, equipaje o cualquier otro contenedor no metálico. Estos lectores en que cada sistemas son totalmente transportables, aunque algunos tipos se instalan de forma fija. Permiten el registro de 50 a 60 personas por minuto, evitando aglomeraciones dando la alarma en cuanto captan metal. Algunos se basan en medir las perturbaciones causadas en el campo magnético al pasar por el arco y otros en la desviación de la frecuencia de un oscilador.

Fig. 29. Etiqueta antirrobo edosada a una prenda de vestir.

También se utilizan captadores de proximidad que podrían tanto ser capacitivos como inductivos, los cuales se pueden aplicar como

control de niveles de fluidos, polvos, granos, contaje de piezas metálicas o no, para tacómetros, y control de posicionamientos. Se utilizan sobre todo en el control de procesos en fábricas, pero pueden tener su aplicación en la seguridad en casos muy especiales. La distancia a que detectan la proximidad de un objeto depende de éste y de la captación del propio detector, pero nunca llega a ser muy grande (máx. 25 mm).

En los lugares en que se requiere alta seguridad, incluso en la oscuridad, el sistema de seguimiento y vigilancia por imagen térmica es un elemento acorde. Está destinado a la observación nocturna o bajo condiciones ambientales difíciles. Su alta capacidad se basa en una técnica de visualización derivada de especificaciones militares. Su capacidad está basada en un mecanismo de exploración que opera en la región infrarrojo de la luz. Los detectores de antimoniuro de indio (Insb) se refrigeran hasta 77°K con un minirrefrigerador Jouie-Thomson a base de gas nitrógeno a presión. Normalmente se montan en conjunto con sistemas perimetrales de protección. Realmente constituye un complemento a cualquier sistema de 5 mm).

Existen alarmas antirrobo especialmente diseñadas para vehículos, las cuales son activadas por consumos eléctricos específicos de la batería del automóvil o camión, a través de un interruptor que protege el compartimento del motor de los vehículos no equipados con luz de capó. Este sistema elimina la necesidad de numerosos interruptores que requerirían el taladro de orificios a través de los que

introducir el cableado correspondiente. Cualquier intento para levantar el capó, hacer funcionar el interruptor de ignición, activar las luces internas abriendo las puertas, o conectar las luces de posición, etc. disparará inmediatamente la sirena de aviso o el propio claxon del automóvil. Otros sistemas emplean un interruptor oculto en el interior del vehículo o bien la cerradura de la llave de contacto. También se puede utilizar sistemas inerciales, pero tienen el inconveniente de que cualquiera que sin querer toque el vehículo moviéndolo podría activar la alarma, no obstante, si se ajusta convenientemente la sensibilidad del sensor inercial, se puede emplear perfectamente.

Los marcadores telefónicos anteriormente mencionados constituyen una salida muy importante de las unidades de control para dar aviso a quien se haya programado anteriormente, pudiendo avisar a varios números de teléfono. Estos cambios se pueden accionar mediante un botón oculto o un pulsador de pie o incluso con un transmisor minúsculo de radio. Cuando se hacen funcionar, el marcador marca los números de emergencia y cuando después de marcar cada número responde el teléfono marcado, éste transmite el mensaje grabado en una cinta. El marcador telefónico se conecta a la línea de teléfono a través de un clavijero de teléfono montado en la pared, de la misma manera que una extensión telefónica, o alambrando permanentemente la conexión a la línea de teléfono.

IV.2. CONSIDERACIONES PARA UNA RED DE CONTROL DE ACCESOS.

Plan de instalación: para la instalación de una red de control de accesos, se deberán de tomar en cuenta ciertas consideraciones para una óptima instalación y una efectiva confiabilidad del sistema.

La protección que ofrece un sistema de seguridad, depende de la forma en que se instala, y de la confiabilidad del sistema.

La protección que ofrece un sistema de seguridad, depende de la forma en que se instala, y de la confiabilidad de sus componentes; si estos se conectan con alambres fácilmente accesibles para los intrusos y las interconexiones se realizan con empalmes de alambres descubiertos, el nivel de seguridad será bajo. Un elemento que se ha diseñado para funcionar en un local, no es seguro si se utiliza en el exterior. Al instalar un sistema, se puede caer en el error de comprar componentes baratos, lo que puede llegar a tener problemas de falsas alarmas y costos elevados de mantenimiento. Así mismo, se deben considerar los lugares ideales donde estarán situados los cables de conexión; esto es, la canalización debe localizarse en un lugar donde sea susceptible a movimientos bruscos, a su vez debe ser sencillo su manejo en caso de mantenimiento. Los equipos controladores estarán situados en áreas restringidas, dentro del edificio inteligente, esto para brindarle una mayor confiabilidad al sistema. Todos estos aspectos,

deben ser tomados en cuenta por el arquitecto y el ingeniero encargado del diseño e instalación de todos los sistemas de control del edificio.

Plan de operación: Dentro de este plan deberá tomarse en cuenta que cada controlador deberá ser capaz de ejercer control y monitorear sus variables independientemente de otro controlador en la red, y deberá contar con un procesador de control digital con contador de tiempo real, para así ejecutar lazos de control (loops).

Los equipos detectores y sensores operarán recibiendo información (codificada o sin codificar) y posteriormente transmitiéndola por la red (control de accesos) hasta el equipo controlador, el cual procesará y almacenará la información que servirá para poder determinar si se dará o no el acceso.

Para el sistema de control de accesos se definirán 5 niveles de accesos de seguridad, los cuales serán asignados de acuerdo a la actividad que realice cada empleado del edificio.

1. Nivel general (personal en general y visitantes).
2. Nivel de servicio (personal capacitado para trabajo en áreas críticas dentro del edificio).
3. Nivel de mantenimiento (personal de mantenimiento o equipos, personal de limpieza).
4. Nivel ejecutivo (personal ejecutivo).

5. Nivel de control y de seguridad (personal de seguridad y monitoreo del edificio).

Así, el personal que labora en el nivel 1, solo tendrá acceso al nivel 2 u superior, por medio de un permiso el cual será habilitado en el nivel 5, ya que estos son los encargados de monitorear la red de control de accesos. Este permiso, se brindará, si existe alguna persona como responsable del acceso al área en cuestión. Esta metodología se realizará cada vez que personal de cierto nivel, quiera acceder a otro superior. No teniendo que efectuar estos pasos si se requiere acceder a niveles inferiores al que se tiene.

Plan de administración; En este plan se deberán se basar los otros planes, además se tomarán en cuenta aspectos relacionados con la supervisión y control de las instalaciones y equipos que integren los servicios básicos del edificio, los cuales se llevaran acabo por medio de un centro de control, cuya localización se determinará de acuerdo al diseño del edificio.

En el cuarto de control central se instalarán los tableros del sistema de alarma, detección, voceo y protección contra incendio, además de conectividad entre la computadora central con el sistema de control de accesos y controles del sistema de circuito cerrado de televisión, debiendo de existir una comunicación bidireccional entre estos y la computadora central. Para el registro de eventos, el apoyo en

acciones de emergencia y la corrección de situaciones de funcionamiento anormales.

La computadora central deberá contar con programas suficientes para llevar a cabo automáticamente las funciones de control, respaldo de información, registro en las bases de datos y notificación impresa y visual de eventos al operador, a quien también le deberá permitir el acceso en tiempo real al conocimiento de estado de los parámetros de operación por medio de gráficos desplegados en pantalla. Así mismo, deberán incluirse programas para llevar a cabo protocolos de pruebas de los sistemas de seguridad y emergencia.

Plan de mantenimiento: Se desarrollarán gráficos para el desplegado de información y para la interacción del operador por pantalla, el nivel de detalle que lo exija cada instalación, permitiendo ubicar fácilmente donde sucedió el evento.

El software contendrá como mínimo las siguientes características:

- Algoritmos de control.
- Horarios para el funcionamiento de los equipos.
- Protección de los equipos de control en caso de falla de energía.

Todos los programas deberán ser efectuados automáticamente sin necesidad de la intervención del operador y deberán ser flexibles

para permitir hacer modificaciones y ajustes. Así también ejecutará el manejo de alarmas, estas deberán ser monitoreadas, almacenadas y enviadas para generar reportes directos a la computadora de control de accesos, sin importar la topología existente en nuestra red.

La red general se configurará en una topología que permita la total conectividad a lo largo de todo el edificio, y a su vez posibilitando una conectividad de máxima flexibilidad y eficacia con otros edificios o áreas colindantes si ello fuese necesario.

El papel que desempeñara nuestra red en un edificio es brindar seguridad y control en el acceso de personal tanto a áreas restringidas, como a las que no lo son. En la fig. 30 se muestra una distribución simple de una red de control de accesos.

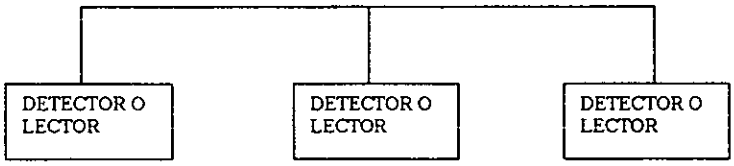


Fig. 30 Distribución de una red de control de accesos simple.

En la figura 31 se muestra la distribución que se propone, para el diseño de una red de control de accesos. El controlador general del edificio se refiere al CPU que servirá de controlador (administrador) de todos los servicios automatizados que tenga el inmueble. El controlador

de la subred de control de accesos, será un equipo CPU de menor potencia y velocidad que el controlador general, esto con la finalidad de evitar el desperdicio de recursos. Y los equipos detectores podrán ser cualquiera de los mencionados en el capítulo anterior, el cual se decidirá de acuerdo a las necesidades específicas del edificio.

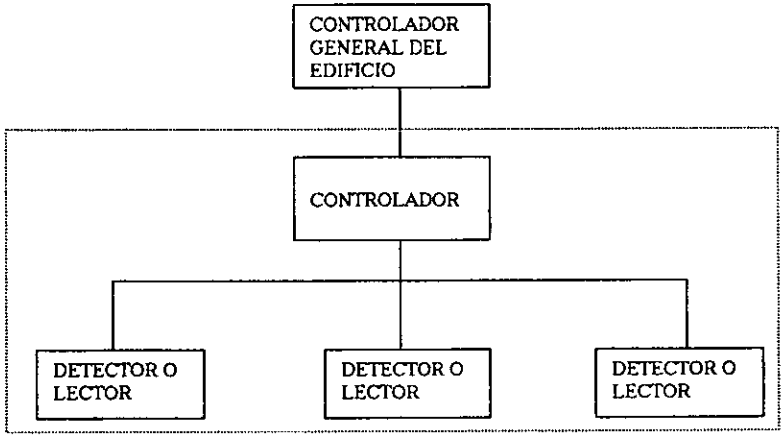


Fig. 31 Red de control de accesos.

A continuación se mencionarán características y consideraciones que deben de tomarse en cuenta para la realización de un sistema de control de accesos, tomando en cuenta los avances tecnológicos en el mercado en cuanto a hardware y software.

IV.2.1. RED.

El diseño de una red de control de accesos, es brindar la mayor seguridad posible en cuanto al manejo del tráfico de personal en áreas restringidas, también el obtener un control instantáneo de la hora de

entrada de usuarios en ciertas zonas. Este sistema puede utilizarse como reloj verificador localizándolo en las zonas de entrada del inmueble. Con esto se ahorran costos a mediano plazo, ya que al implementar un equipo de detección biométrica se excluye el uso de consumibles como en el caso de los lectores de tarjeta; en los cuales después de determinado tiempo es necesario reemplazar las tarjetas por el desgaste que sufren por el uso continuo, así mismo cuando se pierde esta por descuido.

Al implementar un detector de parámetros biométricos se inhibe la posibilidad de falsificación del medio de acceso, ya que las características fisiológicas de cada individuo son únicas y permanecen constantes, como es el caso de la huella digital, el iris del ojo y la forma y dimensiones de la mano. Por lo que la detección se basará en dispositivos biométricos capaces de reconocer la forma y dimensiones de la palma de la mano.

La red que soportará el servicio de control de accesos, manejará un tráfico bajo, debido a que la información transmitida por los detectores no será constante, además el tamaño de la palabra es pequeño, por lo que no necesita un gran ancho de banda. Esta red debe tener una alta confiabilidad en cuanto a la calidad de información, con lo que la presencia de errores se reducirá a un nivel casi nulo, también existirán procedimientos para evaluar la calidad de transmisión

en cuanto a la detección de errores, debido a ello el sistema de transmisión se basará en la transmisión asíncrona.

El diseño de nuestra red se dividirá en tres áreas, las cuales se explican a continuación.

1) Detección de personas que acceden a cierta área. Esta sección involucra a los dispositivos de detección que cumplen con la función de accesar la información al sistema, la cual será comparada y procesada para obtener o no el acceso a cierta área. La conexión de estos con el (las) computador(as) se hará por medio de equipos MODEM cuando así lo requiera, esto será; si sobrepase la distancia recomendada por la norma de transmisión que este siendo utilizada, a su vez estos equipos MODEM así como los detectores se conectarán a través de un canal, que podrá ser alámbrico o inalámbrico, esto dependerá de los equipos que se vayan a implementar, así como de los recursos con los que se cuenten para la implementación del sistemas, ya que los equipos con transmisión inalámbrica son más costosos en su mayoría que los alámbricos. Debido a que la información transmitida es escasa y aleatoria, un cableado de par trenzado satisfacerá ampliamente nuestros requerimientos de ancho de banda, velocidad y costo, ya que este tipo de cableado tiene un rango de velocidades de hasta 10Mbps y con una atenuación aceptable, esta área se muestra en la fig. 31.

2) Computador(as) de control: Son los equipos que controlan todos los dispositivos de detección que al conectarse a un CPU (computadora personal) lo hacen a través de sus puertos o tarjetas multipuertos, logrando una topología individual para cada computador en estrella; estas computadoras compartirán información y recursos entre si, por lo que al interconectarse logran una topología de bus a través de un cable coaxial delgado con velocidad de transmisión de 10 a 100 Mbps. Como se muestra en la fig. 31. Debido a que el tráfico en esta área es más abundante que en la primera, es por lo cual se penso en este medio de transmisión.

3) Backbone. Esta sección tiene el objetivo de conectar las redes locales ubicadas en los diferentes pisos, con lo cual establece un sistema de transmisión común reduciendo costos por concepto de interconexión como son los puentes.

Este sistema de transmisión logra una topología en bus de alta velocidad, los requerimientos del cableado son baja tasa de errores, alta inmunidad a interferencias electromagnéticas, tramos con longitudes elevadas sin la utilización de repetidores, un rango de velocidades de 100Mbps en adelante, un gran ancho de banda y una alta inmunidad al robo o interferencia de las señales.

IV.2.2. TELECOMUNICACIONES.

El edificio inteligente debe contar con infraestructura necesaria para brindar servicios de telecomunicaciones, esto con el fin de que el control general del edificio pueda ser monitoreado desde el mismo inmueble o de otro que se encuentre a cientos de kilómetros de forma confiable, para este caso es necesario la utilización de líneas de comunicación que pueden ser:

- Líneas telefónicas.
- Enlaces de microondas.
- Enlaces satélitales.

Esto nos brinda eficiencia en cuanto a los servicios que se ejercen en el edificio inteligente. En el caso de la red de control de accesos existirá una interconexión con el controlador general del edificio. Esta interconectividad nos permitirá realizar envíos de mensajes o correo electrónico entre terminales de supervisión de la red.

Para la interconexión de la red de control de accesos con el controlador general del edificio, se llevará a cabo un proceso de conversión de protocolos, debido a que una red transmite en forma asíncrona y la otra forma síncrona.

IV.2.3. SERVICIOS DE ADMINISTRACIÓN.

El control de esta red será distribuido con el fin de no saturar o bloquear los procesos que se llevan a cabo en el controlador de la red, brindándole con esto autonomía a cada uno de los puntos de detección, pudiendo realizar procesos específicos en cada uno de ellos. Esto nos permitirá que en caso de que falle el controlador de la red, no se afectarán los puntos de detección, ya que estos trabajarán independientemente.

Se asignarán claves por grupos o individuales para tener acceso a ciertas áreas.

Se tomarán en cuenta parámetros para futuras expansiones de la red, con la implementación de concentradores, repetidores, convertidores, multiplexores y tarjetas multipuertos de acuerdo a las necesidades requeridas, también se podrán realizar cambios en los medios de transmisión para mejorar los anchos de banda y la velocidad de transmisión.

IV.2.4. MANTENIMIENTO Y OPERACIÓN.

Los dispositivos de la red de control de accesos serán supervisados por medio de software el cual monitorea constantemente con el fin de registrar los cambios de estado que se presenten llevando

un registro contínuo de la operación del sistema, con lo que se tiene la posibilidad de identificar fallas o intentos fallidos de acceso, por lo que deberá de contener rutinas para diagnóstico, para corrección de errores, así como envíos de parámetros de control.

Es necesario tener un registro estadístico de los cambios de los dispositivos de la red para detectar los horarios en los que son más necesarios los dispositivos lectores, ya que la posibilidad de presentarse una falla en estos es mayor que en un equipo que no tienen un uso muy frecuente.

El desarrollo de este software se obtendrá directamente de la compañía fabricante de los equipos detectores o en su defecto será realizado por un ingeniero de sistemas.

A continuación se mencionarán los requerimientos de transmisión por partes de la red de control de accesos propuesta.

IV.2.5. REQUERIMIENTOS DE TRANSMISIÓN.

Para la implementación de un sistema de transmisión en la red de control de accesos deben de tomarse en cuenta ciertos aspectos para un funcionamiento óptimo, ya que si no existe un cableado que sea flexible para ser utilizado en cualquier tipo de transmisión (voz, datos y vídeo) demeritará en el funcionamiento a futuro de la misma, ya que es

posible que en determinado tiempo se cambien los equipos que se utilizan en esta red por otros con una tecnología superior a la actual.

Debido a esto, es necesario utilizar el concepto de cableado estructurado, el cual se forma por medio de transmisión y puntos de conexión, que pueden ser utilizados indistintamente por redes de transmisión de datos, voz y vídeo, que funcionen con equipos de distintos proveedores. De esta forma se pueden tener los cableados para una red aún sin conocer el tipo de red o tecnología a utilizar.

La descripción de estos requerimientos se hará por partes para brindar una información más detallada.

La conexión entre los equipos detectores y el equipo controlador, como mencionamos anteriormente, se realizará por medio de par trenzado. Para esto, nuestro equipo detector contará con un puerto serial de comunicaciones RS-232. Así mismo nuestro equipo controlador contará con una o más tarjetas multipuertos en la(s) que se conectarán los detectores. Dependiendo de la distancia entre estos, se considerará la utilización de equipos MODEM. La transmisión en este punto será asíncrona por lo cual la velocidad de transmisión es baja y no sobrepasará los 96000bps. La detección y corrección de errores en esta parte de nuestra red se dará por medio del código Hamming. Debido a que en la transmisión asíncrona no existe protocolo se utiliza únicamente el medio Start-Stop.

La conexión entre los equipos controladores de la subred (en el caso de existir más de uno) , como con el controlador general del edificio, se hará por medio de tarjetas de comunicaciones , que funcionarán bajo el protocolo de comunicaciones Ethernet (CSMA/CD) y el medio de transmisión será cable coaxial delgado con conectores BNC. La velocidad de transmisión en esta sección rondará los 10Mbps, brindando con esto un perfecto intercambio de información entre las bases de datos, además de ofrecer información en tiempo real del estado de todos los equipos de nuestra red de control de accesos. La corrección y detección de errores en esta sección de la red se hará por medio del código Manchester.

El controlador general del edificio podrá conectarse al backbone por medio de otra tarjeta de comunicaciones, esta dependerá del protocolo de comunicaciones (sistema operativo) bajo el que este funcionando. El medio de conexión dependerá del diseño del Backbone. Es decir del tipo de medio que se este utilizando como tal (cable coaxial grueso o fibra óptica), teniendo que utilizarse un transceiver para esto.

IV.3. ALTERNATIVAS TECNOLÓGICAS.

IV.3.1. HARDWARE.

Algunos dispositivos que se pueden implementar en el diseño de la red, son listados a continuación:

Equipos detectores o lectores para control de accesos.

- Tarjetas codificadas con fotografía.
- Tarjetas codificadas con código magnético.
- Tarjetas codificadas con código de barras.
- Tarjetas codificadas de proximidad.
- Teclado con código en memoria.
- Comparación de vídeo.
- Reconocimiento de firma.
- Reconocimiento de patrón de voz.
- Reconocimiento biométrico de huella dactilar.
- Reconocimiento biométrico de la retina.
- Reconocimiento biométrico de la mano.

Cableado

- Par trenzado.
- Par trenzado blindado.
- Cable coaxial delgado.
- Cable coaxial grueso.
- Fibra óptica.

Equipos de computo

- Con microprocesador 80486

- Con microprocesador PENTIUM.
- BOCA FDV241.
- BOCA FDV24E.
- BOCA SE1440.

IV.3.2. SOFTWARE DE PROPÓSITO GENERAL.

A continuación se mencionarán los sistemas operativos bajo los cuales podrá trabajar la red de control de accesos, así como el software con el que puede ser monitoreada la misma.

SISTEMAS OPERATIVOS PARA REDES.

El sistema operativo de una red, es el conjunto de programas que regulan y distribuyen el funcionamiento de la misma, proporciona elementos para establecer la interfase con el usuario, controla y define los grupos y niveles de seguridad, es el encargado de la integridad y seguridad de la información contenida en ella; además controla la compartición de recursos. En general, optimiza los recursos del sistema para un mejor rendimiento y aprovechamiento de los mismos.

Algunas de las tareas que realiza el sistema operativo, para satisfacer las necesidades de los usuarios, y para administrar los recursos de las redes son:

- Manejadores de dispositivos de entrada y salida.
- Un sistema de archivos.
- Interprete de comandos.
- Utilerías.

NOVELL NETWARE.

El Advanced Netware es un sistema operativo de red independiente del hardware, por lo cual puede correr en una gran variedad de redes. Ha estado en el mercado desde 1983 y es el sistema operativo más ampliamente usado en redes de área local.

Novell desarrolló originalmente el NETWARE como el sistema operativo para el equipo NOVELL-S NET. Una red que utiliza una topología estrella y un servidor propietario basado en el microprocesador MOTOROLA 68000. Debido a que este microprocesador no tenia ningún sistema operativo estándar NOVELL decidió desarrollar el suyo partiendo de cero y lo optimizó para redes, diseñando de paso todas sus características alrededor de la funcionalidad de la red.

Cuando comenzó el éxito de las PC (computadoras personales), los autores de NETWARE vieron que, este software esta escrito en lenguaje C, podría fácilmente convertirse a la arquitectura de la familia

INTEL 8088 y que podría soportar virtualmente cualquier red en el mercado.

Debido a que el ROM BIOS de la IBM PC XT fue diseñado para un sistema operativo (DOS) de un solo usuario, y como NETWARE es particularmente multiusuario, los programadores de NETWARE decidieron ignorar el ROM BIOS y así comunicarse directamente con el hardware, para eliminar efectivamente cualquier limitación. Lograron con ello, permitir a NETWARE procesar requerimientos de otra estación de trabajo. La única desventaja de esta forma de operar, es la imposibilidad de utilizar las interfaces (drivers) del DOS para disco duro. NOVELL surte estas interfaces para discos compatibles con IBM y muchos fabricantes surten sus propios drivers para NETWARE.

A continuación se presenta una lista resumida de las principales características del NOVELL NETWARE en el cual se resaltan sus principales ventajas y desventajas.

VENTAJAS.

A) Rendimiento muy superior a los demás sistemas operativos para redes cuando se utilizan de 20 a 100 nodos.

B) Facilidades de conectividad para establecer comunicación hacia otros ambientes ya sea remotos o locales mediante PUENTES o RUTEADORES.

C) Sistema de seguridad completo y eficiente el cual asigna derechos a diferentes tipos de usuarios para la utilización de recursos.

D) Posibilidad de definición de menús mediante una utilería en el NETWARE para accesar a programas en la red o comandos de esta.

DESVENTAJAS.

A) Sistema de mensajes entre usuarios, deja mucho que desear.

B) Requiere de una mayor preparación técnica por parte de los usuarios, principalmente del supervisor de la red, lo cual implica conocimientos de controladores de disco, protocolos de comunicación, direcciones de nodos, etc.

C) Instalación tardada, ya que una adecuada instalación y configuración requiere de varias horas, esto dependiendo de la capacidad del servidor, tiempo en el cual NETWARE sólo esta verificando partes del disco duro; este problema es posible aminorarlo, ya que el NETWARE solicita al usuario el intervalo de chequeo de pistas del disco duro, lo cual permite calcular el tiempo de formateo.

D) El costo de NETWARE es elevado, lo cual se justifica si la red es grande y/o se requiere alta seguridad en la información

contenida. Esta desventaja la elimina NETWARE con su versión ELS diseñada para redes de 4 a 8 nodos.

UNIX.

UNIX, es un sistema operativo que ha evolucionado durante los últimos veinte años hasta convertirse en un entorno e influyente en el mundo. Entre sus características fundamentales se pueden enumerar que:

- Es una poderosa herramienta de software. UNIX introdujo una nueva idea en la computación; la creación de programas de aplicación y la resolución de problemas concernientes a comunicación, programación, etc. pueden ser resueltos mediante la interconexión de programas y procesos simples. Estos programas son diseñados para realizar bien una única tarea, con lo cual, pueden contribuirse grandes aplicaciones a partir de secuencias de orden simples, debido a esto, resulta ser muy productivo al elaborar aplicaciones complicadas con programas simples.

- Facilidad de ser transportado a otras computadoras. UNIX ha sido transportado a casi cualquier computadora construida, de trama; o moderado o grande. Solo unos cuantos cambios o adaptaciones mínimas han sido necesarios para hacer a UNIX utilizable sobre nuevas computadoras.

- Las versiones modernas de UNIX están organizadas para funcionar en un ambiente de red. Las herramientas de comunicación internas del sistema, la fácil aceptación de rutinas de dispositivos adicionales bajo nivel y la organización flexible del sistema de archivos, son naturales para el entorno de red. Usar computadoras en grupos de trabajo es posible gracias a las capacidades de conexión a recursos dispuestos en red que ofrece UNIX.

UNIX ofrece productos para construir redes y las características son las siguientes:

- Permite la ejecución de programas en forma asíncrona.
- Es portable por estar escrito en lenguaje de alto nivel.
- Es modular. Se compone de un conjunto de herramientas básicas que integradas forman estructuras complejas.
- Permite el procesamiento por lotes.
- Presentan una estructura de archivos jerarquía, que ha sido fundamento de muchos sistemas operativos, incluyendo DOS y OS/2.
- Permite la comunicación entre procesos, tienen entrada y salida compatibles, todos los dispositivos y archivos son vistos como archivos.
- Tiene un conjunto de utilerías, entre ellas las que permiten crear, modificar, escribir y desarrollar programas y archivos de texto.

Todas estas razones ayudan a la popularidad que UNIX ha gozado en años recientes, sus bondades están ligadas estrechamente a las del lenguaje C, por haber sido desarrollado con este.

IV.3.3. SOFTWARE PARA CONTROL DE ACCESOS.

Existen diversas compañías dedicadas a la fabricación y a la implementación de dispositivos para el control de accesos, los cuales a su vez desarrollan el software necesario para el funcionamiento de los mismos. Como los que a continuación se mencionan.

HAND NET

Este software es utilizado para el control de los lectores biométricos, fue realizado en lenguaje C, sin embargo este se ofrece al cliente bajo la característica de programa ejecutable, ya que es un software de explotación y uso general. Las fuentes de este sistema, son propiedad de Recognition Systems, por lo cual podrá ser modificada la información contenida en los archivos de transacciones.

Algunas de sus características son:

- Soporta una red local de hasta 31 dispositivos biométricos lectores de la mano, basado en un sistema de control de accesos con base de datos distribuidos.
- Capacidad para enrolar usuarios.

- Definición de la clave de usuarios (hasta 10 dígitos).
- 62 tiempos de trabajo diferentes (horarios).
- 64 niveles de acceso (por tiempo y lugar).
- Definición de días festivos.
- Monitoreo de la red.
- Control de toda la red desde el concentrador (controlador) para actuar sobre indicaciones específicas (bloquear lectores, accionar puertas, alarmas, etc.).
- Emisión de reportes por:

- Usuario
- Fecha
- Hora
- Lector
- General
- Y combinaciones de los anteriores
- Horarios
- Días festivos

Niveles de acceso.

- Fijar la fecha y la hora de arranque de cada lector.
- Generación de archivos con la información de todas las transacciones en código ASCII. Esto hace que los archivos

generados por el software sean 100% transportables a cualquier sistema para su explotación.

Además el software HAND NET brinda la alternativa de manejarlo por medio de menús, los cuales despliegan la siguiente información:

Actividad: Despliega en pantalla todas las transacciones o situaciones del sistema en tiempo real.

Log: Identificación y clave de acceso del operador.

Override: Operación remota de los dispositivos controlados por los handkeys.

Reportes: Emisión de reportes de transacciones, generación de archivos tipo ASCII y listado de los archivos de trabajo.

Uso: Mantenimiento al archivo de usuarios (altas, bajas y cambios).

Configuración: Mantenimiento a los archivos de programación, horarios, niveles de acceso y días festivos.

Download: Envío de parámetros de control de información de usuarios a los HANDKEYS de la red (selectivo o general).

SISTEMA DSX-1030

El software DSX-1030 de DSX Access System, Inc.; es líder mundial en el control de accesos, basado en una computadora personal. Este software cuenta con las siguientes características:

Debido a su gran flexibilidad, es posible controlar diferentes tecnologías, como lectoras de tarjetas, lectores biométricos, así como combinaciones de estos. El sistema DSX-1030 es eficiente ya que cuenta con un sistema lector único simple. La transición de un sistema lector único simple a uno con muchas locaciones a través de cientos de kilómetros y conteniendo cientos de lectores de tarjetas, está logrando con el mismo software y añadiendo más modelos del mismo hardware. El DSX-1030 no depende del hardware, no hay módulos adicionales al software.

En DSX- 1030 los reportes están diseñados para apuntar a la dirección exacta que usted desea, se pueden especificar los rangos por fechas, tiempos, combinaciones de puertas, de división o de compañías, posesión individual de tarjeta o por tipo de evento o combinaciones de ambas. DSX también tiene la utilería de base de datos que permite 16 campos definidos por el usuario de hasta 50 caracteres cada uno por tarjeta. Los títulos de cada campo pueden estar por departamentos, antecedentes escolares, género, tipo de sangre, color de pelo, modelo de carro, o cualquier otro campo definido

por el usuario. La búsqueda puede ser generada no solamente en cualquier campo definido por el usuario, sino por la combinación de uno a 16 campos.

La interfase de operador del DSX es fácil de usar, al abrir manualmente una puerta establece una conexión controlada por módem, cada paso es conducido por un menú. El operador cuenta también con una ayuda de contexto sensible. La tecla F1 de cualquier teclado de datos presenta una ayuda en pantalla, con información específica para ese punto en concreto. La seguridad del sistema es brindada por una contraseña única por cada operador, cada operador puede tener acceso a la porción del programa que esta autorizado únicamente.

El sistema DSX-1030 provee 1000 diferentes niveles de acceso, cada nivel describe un grupo separado de puertos, que con la tarjeta pueden entrar. Los niveles de acceso de puertas pueden también programarse con la hora y la fecha del día o días festivos. Este número de nivel de acceso le permite al sistema mejorar a las necesidades que se requieren.

Este sistema puede monitorear hasta 30,000 puntos separados, cada punto puede tener un mensaje único de definición y de acción. Los puntos de alarma pueden ser programados, armados y desarmados por ellos mismos en planes individuales que pueden variar con la hora, los

días de la semana y días festivos. Si la alarma es activada, el operador es avisado con una alerta audible. Una descripción del punto de alarma y un mensaje de alerta se despliega, mediante el teclado el operador obtiene el lugar exacto de alarma en la pantalla, así como un alejamiento o acercamiento de ella. Sobre la decisión de la alarma, el operador mediante el teclado especifica la acción tomada y cualquier otro comentario que pueda aclarar el evento. El DSX acomoda hasta 10,000 pantallas gráficas individuales, ambos controles de alarma de entrada y salida son exhibidos en el momento mismo que se requieren, son monitoreados automáticamente tanto local como remota.

Además este sistema cuenta con control de elevadores, para casos locales y de control con módem.

SLM.

SLM es el primer programa de administración de tiempo y asistencia, desarrollando en ambiente Windows para las necesidades de las empresas mexicanas. El sistema le permite al usuario interactuar con su nómina, realizar un análisis de las causas que provocan las horas no trabajadas y elaborar la prenómina de manera automática.

SLM le permite identificar de manera inmediata, en un ambiente de ventajas y en forma amigable, las excepciones que se presentaron en cada día de trabajo o por un periodo de tiempo específico.

SLM hace interfase con su programa de nómina y prácticamente con cualquier equipo de control de accesos, lo que le da a las empresas un nivel superior de administración de personal y evita el tradicional verificador de tarjetas. Así mismo, permite fuera de línea, obtener estadísticas sobre la información de las transacciones generadas por los dispositivos de control de accesos. Los principales reportes son:

- Número de eventos por día (por tipo de evento o general).
- Número de eventos por persona.
- Número de eventos por fecha.
- Reporte de ausentismos.
- Integrador de horas trabajadas.
- Número de alarmas por tipo.
- Horas extras autorizadas.
- Permisos, comisiones u otros.
- Vacaciones y/o incapacidades.

El SLM incorpora catálogos de personal que hacen interfase con la nómina, de esta forma no es necesario actualizar dos bases de datos para la administración del sistema.

Gracias a la flexibilidad del sistema y su facilidad de manejo, es posible diseñar reportes de acuerdo a las necesidades específicas de cada empresa, estos pueden ser, reportes diarios de la asistencia del personal, o del rango de fechas solicitado por el usuario. De la misma

manera se pueden elaborar reportes por cada una de las excepciones que se presentaran en el periodo de tiempo que seleccione el usuario. Los reportes son tabulares o gráficos y pueden ser presentados en pantalla o impresos. Después de haber hecho un estudio a fondo sobre las diferentes alternativas en el diseño de una red de control de accesos, se llegó a la conclusión de que un sistema basado en lectores biométricos Handkey, es el más conveniente para la seguridad y el control de un edificio.

CONCLUSIONES

Debido a la creciente inseguridad de nuestra ciudad, se ha tenido que recurrir a la tecnología para crear dispositivos que nos permitan desarrollar nuestras actividades cotidianas.

Los sistemas de alarma se utilizan en muchos casos como protección contra el robo, los incendios, inundaciones, escapes de gas, atracos o como simple aviso de emergencia.

El propósito, de todos conocido, de un sistema de alarma es detectar cualquier anomalía debida a la entrada de un intruso o a un incendio. Cuando se trata de la detección de un indeseable, su mejor efecto es el de alertar al propio intruso antes de que su entrada sea efectiva, es decir, actúa como sistema disuasivo.

Uno de los resultados más fascinantes y notables obtenidos a partir de los avances tecnológicos, en el área de seguridad son los apartados de identificación biométrica; los cuales brindan un alto grado de inmunidad a falsificaciones, ya que esta tecnología se basa en el reconocimiento de un rasgo corporal único, por lo que reconoce a las personas y no a objetos. La llegada de estos dispositivos al mercado electrónico, permite integrarlos en diseños que brinden un alto grado de seguridad.

BIBLIOGRAFIA

Andrew S. Tanenbaum
Redes de ordenadores
Prentice-Hall Hispanoamérica, S.A.
México, 1991

AT&T
Manual del SYSTEMAX PDS
México, Marzo, 1994.

BESCO Sistemas de seguridad
Control de accesos
México, 1994.

Recognition System, Inc.
ID3D-R Handkey Han Reader Operating and Installation Manual.
Cabell, U.S.A.,1990.

IMC Networks
Repeaters: What are they? And Why do I need them?
Invine CA, U.S.A., 1993.

ERICSSON S.A. DE C.V.
Redes inteligentes
Sistema de gestión de voz y datos Manual
México, 1990.

Northern computer, Inc. (Atapco Security and comunications group)
Acceses Control Solution Manual
Milwakee, WI. U.S.A., 1991
Northem Telecom (Cala) Corp.
Red de distribución integrada para edificio Manual
Miami Lakes, FI. U.S.A 1993

Jhonson Controls Inc.
Metasys netware sales resource Manual
Inteligent Access Control
Milwakee, WI. U.S.A., 1992

Black Box Catalogue
The source for connectivity
LAN, WAN Y DATACOMM
México, 1994

IMEI
Productos y soluciones
México, 1993

Sistemas electrónicos de seguridad
Edit. Marcombo