(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 511**

(51) Int. CI.:

G08B 13/196 (2006.01)
G07C 9/00 (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.01.2014 E 14152345 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2019 EP 2765564**

(54) Título: **Sistema y método para controlar sistemas de seguridad**

(30) Prioridad:

07.02.2013 US 201313761871

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2019

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road
Morris Plains, NJ 07950, US

(72) Inventor/es:

DZIADOSZ, JOHN A. y
QI, SHIYUAN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema y método para controlar sistemas de seguridad

Campo de la invención

El campo de la invención se refiere a sistemas de seguridad y, más particularmente, al control de dispositivos de seguridad en sistemas de seguridad.

Antecedentes de la invención

Los sistemas de seguridad son, en general, conocidos. Dichos sistemas normalmente se utilizan para proteger zonas protegidas frente a amenazas. Las amenazas pueden incluir intrusos que representen una amenaza para personas que estén autorizadas a estar dentro de la zona protegida o amenazas ambientales como incendios o humo.

Normalmente, el acceso a las zonas protegidas se impide mediante el uso de un cercado de muros que rodea la zona protegida. Puede proporcionarse una o más puertas para el acceso de personas autorizadas.

Puede proporcionarse un panel de control centralmente ubicado para monitorizar la zona protegida. Uno o más detectores y/o cámaras puede/n detectar la presencia de intrusos o de amenazas ambientales dentro de la zona protegida. Los detectores pueden incluir fines de carrera en las puertas para detectar la entrada de intrusos en la zona protegida. En las puertas pueden proporcionarse lectores de tarjetas para detectar la entrada de personas autorizadas.

En el documento de patente nº US2009/070477A1 se describe un sistema de seguridad integrado que integra un acceso y un control móviles de banda ancha con sistemas de seguridad convencionales y dispositivos en las instalaciones para proporcionar una red de seguridad trimodal con acceso y conectividad remotos. El sistema de seguridad integrado dota a la protección vigilada en las instalaciones convencional de una funcionalidad de vigilancia y control remotos en las instalaciones y sirve de complemento a los equipos de protección en las instalaciones existentes. El sistema de seguridad integrado se integra en la red en las instalaciones y se acopla inalámbricamente al panel de seguridad convencional, lo cual permite un acceso de banda ancha a los sistemas de seguridad en las instalaciones. Pueden añadirse dispositivos de automatización que permitan a los usuarios ver remotamente vídeo o imágenes y controlar dispositivos domésticos a través de un portal web privado u otros dispositivos clientes. Las cámaras de la red en las instalaciones se pueden configurar y gestionar automáticamente mediante una gestión de cámaras. La gestión de cámaras abarca el control y la vigilancia remotos desde fuera del cortafuegos de la red en las instalaciones para incluir el encaminamiento de imágenes o de vídeo desde un dispositivo de fuente de retransmisión hasta un dispositivo cliente solicitante.

Cheshire S. y otros describen como pueden nombrarse y estructurarse registros de recursos DNS para facilitar el descubrimiento de servicios [CHESHIRE M KROCHMAL APPLE INC S, “DNS-Based Service Discovery; draft-cheshire-dnsext-dns-sd-11.txt”, DESCUBRIMIENTO DE SERVICIOS BASADO EN DNS; BORRADOR-CHESHIRE-DNSEXT-DNS-SD-11.TXT, GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET, IETF; PROYECTO DE TRABAJO ESTÁNDAR, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH-1205 GINEBRA, SUIZA, (20111210), págs. 1-54, XP015079709 [Y] 1-15 * pág. 3, línea 1 - pág. 4, línea I * * pág. 8, línea 7 - línea 16].

Guttman E. y otros describen un protocolo de seguimiento de normas de Internet para la comunidad de Internet y solicita un debate e ideas de mejora [GUTTMAN C PERKINS SUN MICROSYSTEMS J VEIZADES @HOME NETWORK M DAY VINCA CORPORATION E, “Service Location Protocol, Version 2; rfc2608.txt,” 5. REUNIÓN JCT-VC; 96. REUNIÓN MPEG; 16-3-2011 - 23-3-2011; GINEBRA; (EQUIPO DE COLABORACIÓN CONJUNTA SOBRE CODIFICACIÓN DE VÍDEO DE ISO/IEC JTC1/SC29/WG11 E ITU-T SG.16); URL: HTTP://WFTP3.ITU.INT/AV-ARCH/JCTVC-SITE/, GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET, IETF, CH, (199906), ISSN 0000-0003, XP015008391 [A] 1-15 * pág. 5, línea 1 - pág. 8, línea I*].

Si bien dichos sistemas funcionan bien, a menudo son difíciles de configurar y administrar. En el caso de instalaciones de gran tamaño, el número de puertas y de detectores puede ascender a varios centenares. Dichos sistemas son difíciles de configurar debido al gran número de puertas y detectores. Por consiguiente, es necesario dar con maneras rápidas de configurar dichos sistemas de seguridad.

Sumario de la invención

Los diversos aspectos de la presente invención se exponen en las reivindicaciones adjuntas.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques de un sistema de seguridad, mostrado de una manera que generalmente está de acuerdo con una forma de realización ilustrada; y

La figura 2 diagrama de bloques de un conjunto de pasos que pueden ejecutarse en el sistema de la figura 1.

Descripción detallada de una forma de realización ilustrada

Aunque las formas de realización pueden adoptar muchas formas diferentes, en los dibujos se muestran formas de realización específicas de la invención, que se describirán detalladamente en la presente memoria descriptiva. Se entenderá que la presente memoria descriptiva ha de considerarse una ejemplificación de la invención reivindicada así como la mejor manera de ponerla en práctica. No se pretende limitar la invención a la forma de realización específica que se ha ilustrado.

La figura 1 es un diagrama de bloques de un sistema de seguridad 10, mostrado de una manera que generalmente está de acuerdo con una forma de realización ilustrada. El sistema de seguridad puede incluir uno o más detectores 12, 14 que detecten amenazas dentro de una zona protegida 16. Las amenazas pueden deberse a la presencia de intrusos o deberse a amenazas ambientales. En el caso de los intrusos, los detectores pueden incluir fines de carrera conectados a entradas (p. ej., puertas, ventanas, etc.) 18 que permiten la entrada a o la salida de zona protegida 16. Alternativamente, los uno o más detectores pueden incluir un lector de tarjetas y una cerradura eléctricamente activada que permitan acceder a los usuarios autorizados a la zona 16 por una de las puertas 18.

En el caso de las amenazas ambientales, los uno o más detectores pueden fabricarse para detectar incendios. Pueden fabricarse otros detectores para detectar la presencia de gas natural.

La zona protegida también puede incluir una o más cámaras 20, 22. Las cámaras pueden ser monitorizadas por un guarda de seguridad o pueden tener capacidad de detección de movimiento.

Cada uno de los detectores y cámaras puede monitorizarse a través de un panel de control 22. Al detectarse una amenaza por medio de uno de los detectores o cámaras, el panel de control puede enviar un mensaje de alarma una central de vigilancia 24. La central de vigilancia puede responder enviando ayuda (p. ej., la policía, los bomberos, etc.).

El panel de control (y cada uno de los detectores y cámaras) puede incluir uno o más aparatos de procesamiento (procesadores) 26, 28 que trabajen bajo el control de uno o más programas informáticos 30, 32 que se carguen desde un soporte legible por ordenador no transitorio (memoria) 34. Tal y como se emplea en la presente memoria descriptiva, la referencia a un paso realizado por un programa informático del panel es también una referencia al procesador que ejecute ese paso.

A este respecto, un procesador de alarmas del panel puede monitorizar los detectores y las cámaras. Al detectar una amenaza para la seguridad, el procesador puede activar una alarma audiovisual local. El procesador también puede escribir un mensaje de alarma y enviarlo a la central de vigilancia. El mensaje puede incluir un identificador del sistema de seguridad (p. ej., su número de cuenta, la dirección de la zona protegida, etc.) y un identificador del tipo y de la ubicación del detector o cámara.

El panel y cada uno de los detectores pueden conectarse entre sí por medio de una conexión cableada o inalámbrica. Cuando se utilice una conexión inalámbrica, el panel y cada uno de los detectores también pueden incluir un transceptor inalámbrico 36. Los transceptores inalámbricos 36 pueden utilizarse para establecer un canal de conexión inalámbrica entre el panel de control y cada uno de los detectores y con las cámaras.

Según una forma de realización ilustrada, la conexión entre el panel y cada uno de los detectores y cámaras puede utilizar un protocolo de tipo DNS Multidifusión/Sin Configuración como el descrito por el Grupo de Trabajo Zeroconf de la IETF (p. ej., www.zeroconf.org). El uso de mensajería DNS Multidifusión/Sin Configuración permite establecer automáticamente una conexión respectiva y correspondiente entre el panel y cada uno de los detectores y cámaras con muy poca o sin ninguna intervención humana.

Para facilitar el establecimiento de la conexión entre el panel y cada uno de los detectores y cámaras, una o más pasarelas dentro del panel pueden intercambiar una serie de mensajes con uno o más procesadores aguas abajo (o asociados a) de cada uno de los detectores y cámaras. La pasarela dentro del panel se refiere a uno o más procesadores programados 26, 28 y a un transceptor 36 que funcionan juntos como pasarela. De manera similar, el término “procesador aguas abajo” se utiliza aquí para referirse genéricamente a una parte respectiva de uno de los detectores o cámaras, donde la parte aludida incluye uno o más procesadores programados 26, 28 y un transceptor 36 dentro del respectivo detector o procesador.

A este respecto, la pasarela puede dotarse de una o más listas de grupos de servicios. Tal y como se utiliza en la presente memoria descriptiva, un grupo de servicios se refiere a uno o más detectores y/o cámaras que proporcionan idéntica o similar funcionalidad. Por ejemplo, un detector puede ser un controlador de acceso (incluyendo un lector de tarjetas, una cerradura accionada eléctricamente, unos procesadores asociados y un transceptor) que esté incluido dentro de un tipo particular de grupo de servicios. Asimismo, una cámara puede incluir un detector de movimiento (incluyendo una cámara, un procesador de detección de movimiento y un transceptor) que esté incluida dentro de otro grupo de servicios. Según otra alternativa más, un detector podría incluir un módulo detector de apertura de ventana o de puerta (incluyendo un fin de carrera, un procesador y un transceptor) que esté incluido dentro de otro grupo de servicios.

Para cada grupo de servicios la pasarela podrá transmitir a los detectores y cámaras un mensaje de multidifusión que identifique cada vez a un grupo de servicios a fin de descubrir automáticamente a los respectivos miembros de cada grupo de servicios. El mensaje de multidifusión transmitido por la pasarela incluye al menos un identificador del grupo de servicios y un certificado de autenticación.

Los controladores aguas abajo sólo responden al mensaje de multidifusión que identifica al grupo de servicios al que pertenece los controladores. A este respecto, cualquier controlador aguas abajo que reciba el mensaje responderá con un mensaje de anuncio que anuncie el tipo de servicio prestado por ese detector o cámara. La pasarela autentica el controlador aguas abajo y establece un canal con el controlador aguas abajo.

A medida que se va descubriendo cada controlador aguas abajo, las características de identificación del controlador aguas abajo se guardan en una tabla de mapas de sistema y en una tabla de estados de servicio. En caso de que la pasarela se conecte con distintos tipos de grupos de servicios, las características de identificación de cada grupo pueden guardarse en una tabla diferente asociada a ese grupo.

No obstante, a veces puede perderse periódicamente la conexión con el controlador aguas abajo. Para tener en cuenta a esta posibilidad, el controlador de pasarela vuelve a entrar periódicamente en modo de descubrimiento (p. ej., cada 30 segundos) para redescubrir cada uno de los detectores y/o cámaras que esté dentro de la zona protegida que se encuentre dentro de su alcance. La pasarela puede entonces hojear las respuestas para actualizar la tabla de mapas del sistema.

En la figura 2 se muestra un flujograma simplificado 100 de un registro de los detectores y las cámaras en el sistema 10 a través de la pasarela. A este respecto, el controlador aguas abajo transmite 102 un mensaje de anuncio en respuesta al mensaje de descubrimiento de unidifusión procedente de la pasarela. El mensaje de anuncio 102 puede incluir una dirección MAC del controlador aguas abajo, la dirección IP y un certificado firmado. En este caso, el certificado puede haber sido firmado por el controlador aguas abajo con el fin de autenticar al controlador aguas abajo con el controlador de pasarela.

El mensaje de anuncio también puede incluir uno o más campos de datos adicionales. Dentro de los campos de datos adicionales puede incluirse un identificador del servicio prestado a través del controlador aguas abajo (p. ej., un identificador del controlador aguas abajo que lo identifique como controlador de acceso, una cámara, etc.). Los campos de datos también pueden incluir otros identificadores, incluyendo un número de revisión del software que se ejecute en el controlador aguas abajo, un modelo de lector de tarjetas, un modelo de cámara, etc.

La pasarela recibe el mensaje de anuncio y autentica 104 al controlador aguas abajo. La pasarela puede autenticar al controlador aguas abajo basándose en el conocimiento previo de las capacidades de procesamiento y firma de certificados utilizadas por el controlador aguas abajo para firmar el certificado de autenticación que fue proporcionado originalmente por la pasarela.

Una vez que se haya autenticado al controlador aguas abajo, el controlador aguas abajo es registrado 106 por un procesador de registro en la tabla de mapas de sistema y en la tabla de estados. Además de registrar al controlador aguas abajo en el mapa de sistema, el controlador de pasarela también puede dar de alta al controlador aguas abajo en un conjunto apropiado de aplicaciones de procesamiento de alarmas. Por ejemplo, un controlador aguas abajo que incluya una cámara puede darse de alta en una o más aplicaciones de grabación que graben el vídeo de la cámara, ya sea de forma continua o únicamente cuando se detecte movimiento dentro de un campo visual de la cámara.

El procesador de registro también puede reenviar un mensaje de registro completo a un procesador apropiado del controlador de pasarela. En respuesta, el controlador de pasarela toma medidas para establecer una conexión de capa 4 (L4) con el controlador aguas abajo autenticado. A este respecto, el procesador de pasarela puede enviar 110 un mensaje de conexión TCP al controlador aguas abajo. El controlador aguas abajo puede responder 112 con un mensaje de conexión aceptada.

La pasarela también toma medidas para establecer un canal de comunicación entre el controlador aguas abajo autenticado y la pasarela mediante una sesión de capa 5 (L5). Esta pasarela hace esto enviando 114 una petición de enlace al controlador aguas abajo. La petición de enlace incluye la dirección MAC de la pasarela y un certificado de seguridad. El controlador aguas abajo rechazará la solicitud de enlace si el controlador ya está enlazado a otra pasarela. Si no es así, el controlador aguas abajo puede completar el establecimiento del canal devolviendo 116 una respuesta de enlace a la pasarela.

El controlador aguas abajo también puede guardar datos relativos a la conexión en un archivo de estado de pasarela de la memoria del controlador aguas abajo. Los datos pueden incluir al menos un identificador de la pasarela y una dirección IP de la pasarela. Los datos de la pasarela de conexión se guardan en la memoria del controlador aguas abajo por si otra pasarela interroga al controlador aguas abajo. Si fuese así, el controlador aguas abajo rechazaría entonces la conexión de la otra pasarela.

La pasarela también puede establecer una conexión segura con el controlador aguas abajo mediante una sesión de capa 5 (L5). A este respecto, la pasarela puede enviar 118 un establecimiento de comunicación de seguridad que incluya una clave de seguridad y un método de cifrado (p. ej., AES). Si se utiliza AES, el cifrado puede realizarse mediante SSL/TLS.

El controlador aguas abajo puede devolver 120 un establecimiento de conexión de seguridad de aceptación que incluya un reconocimiento de un nivel de seguridad y un método y un nivel de cifrado. Los detalles de la conexión segura también pueden guardarse en el archivo de conexión.

Una vez que se haya establecido un canal seguro entre la pasarela y el controlador aguas abajo, pueden intercambiarse mensajes según sea necesario. A este respecto, pueden enviarse 122 comandos cifrados de la pasarela al controlador aguas abajo y pueden recibirse 124 respuestas cifradas.

También pueden enviarse y recibirse mensajes asíncronos. Por ejemplo, en caso de que el controlador aguas abajo sea un interruptor de puerta, la activación de ese interruptor puede dar lugar a que se envíe 126 un mensaje de alarma a la pasarela.

Una vez que se haya establecido un canal con cada controlador aguas abajo, un usuario puede acceder a los detectores y cámaras correspondientes a través de una interfaz de usuario 38. Se pueden mostrar una o más pasarelas en una pantalla 40 de la interfaz de usuario. El usuario puede hacer clic en la pasarela con un ratón o un teclado 42 para ver una lista de detectores y cámaras descubiertos por grupos de servicios. El usuario puede hacer clic en cada grupo de servicios y obtener una lista de dispositivos (p. ej., detectores, cámaras, etc.) descubiertos por la pasarela dentro de ese grupo de servicios.

Al hacer clic en uno de los dispositivos, un procesador de configuración del panel que funciona a través de la pasarela puede recuperar los ajustes de ese dispositivo. Si el dispositivo es una cámara, los ajustes pueden incluir una frecuencia de imagen de la cámara, independientemente de si la cámara tiene capacidad de detección de movimiento y de si la cámara tiene capacidad de movimiento de rotación en el plano horizontal, movimiento de rotación en el plano vertical y zoom (PTZ). El usuario puede regular los ajustes y asignar un procesador PTZ a la cámara a fin de controlar la capacidad PTZ de la cámara.

Del mismo modo, si el dispositivo es un controlador de acceso, el usuario puede ver el modelo del lector de tarjetas y ajustar sus capacidades. Además, el usuario puede descargar un conjunto de identificadores de usuarios autorizados o conectar lógicamente el lector de tarjetas a un procesador de autorizaciones independiente.

Una vez finalizada la configuración, el sistema puede funcionar de forma convencional. La activación de un detector por un intruso puede hacer que se envíe un mensaje al procesador de alarmas del panel por el canal establecido. El panel puede activar una alarma local y enviar un mensaje de alarma a la central de vigilancia 24.

El uso de la pasarela permite agregar una serie de controladores aguas abajo cableados y/o inalámbricos (i.e., detectores y/o cámaras) mediante una pasarela individual. Además, si una pasarela quedase inutilizada, los detectores y las cámaras pueden descubrirse automáticamente y las conexiones restablecerse a través de otra pasarela.

En un ejemplo, las pasarelas redescubren periódicamente (p. ej., cada 30 segundos) los controladores aguas abajo del/de los grupo/s de servicios asignados a esas pasarelas. Para cada dispositivo que responde la pasarela intenta encontrar la dirección MAC de ese controlador aguas abajo en su tabla de estados de servicio. Si la pasarela no encuentra la dirección MAC, este controlador aguas abajo es un dispositivo nuevo y se añadirá a la tabla de estados de servicio. Si encuentra la dirección MAC, la pasarela compara la dirección IP y el identificador (nombre del ordenador central) del controlador aguas abajo con el contenido actual del registro en la tabla de estados del servicio. Si se ha cambiado la dirección IP y/o el nombre del ordenador central, entonces se actualiza la entrada.

A este respecto, la disponibilidad de múltiples pasarelas permite a cada pasarela crear una agrupación diferenciada de controladores aguas abajo. Si hay varias pasarelas, cada pasarela puede servir como respaldo a uno o más controladores diferentes.

Según algunas formas de realización, la autenticación de controladores aguas abajo podría ser un proceso manual que requiriese la participación de un administrador. Esto podría ser útil cuando el administrador active manualmente un detector o una cámara de cada controlador aguas abajo descubierto para confirmar la ubicación del controlador descubierto.

Según otras formas de realización, la autenticación de controladores de pasarela por parte de los controladores aguas abajo puede involucrar opcionalmente a un tercero o a otra parte de confianza para que valide la autenticidad del certificado de pasarela. Esto puede lograrse conectando un procesador opcional a cada uno de los procesadores aguas abajo, donde los procesadores opcionales pueden tener capacidades adicionales para procesar y autenticar certificados.

Se observará gracias a lo expuesto anteriormente que pueden realizarse numerosas variaciones y modificaciones sin apartarse del alcance de la invención tal y como está definido en las reivindicaciones. Debe entenderse que ni se pretende ni debe inferirse que haya alguna limitación con respecto al aparato específico ilustrado en la presente memoria descriptiva. Naturalmente, está previsto que las reivindicaciones adjuntas cubran todas las modificaciones de este tipo que se encuentren dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Método que comprende:

la transmisión por parte de un controlador aguas abajo de un sistema de seguridad de un anuncio de un tipo de servicio del controlador aguas abajo en una subred;
la detección del anuncio y la autenticación por parte de un primer controlador de pasarela del sistema de seguridad del controlador aguas abajo como parte de un grupo de servicios correspondiente al tipo de servicio;
el envío por parte del primer controlador de pasarela de una petición de conexión al controlador aguas abajo;
el establecimiento por parte del primer controlador de pasarela y del controlador aguas abajo de una conexión L4 basada en la petición de conexión;
el establecimiento por parte del primer controlador de pasarela y del controlador aguas abajo de un canal de sesión L5 a través de la conexión L4;
el guardado por parte del primer controlador de pasarela de unas características identificativas del controlador aguas abajo contenidas en el anuncio en una tabla de mapas de sistema y una tabla de estados de servicio asociadas al grupo de servicios;
el guardado por parte del controlador aguas abajo de unos datos relativos a la conexión L4 en un archivo de estado de pasarela de una memoria del controlador aguas abajo, en el que los datos relativos a la conexión L4 incluyen al menos una primera dirección MAC del primer controlador de pasarela; y
el rechazo por parte del controlador aguas abajo de una segunda conexión de un segundo controlador de pasarela cuando una segunda dirección MAC del segundo controlador aguas abajo recibida por el controlador aguas abajo no coincida con la primera dirección MAC del primer controlador de pasarela almacenada en el archivo de estado de pasarela.

2. Método según la reivindicación 1, en el que el controlador aguas abajo incluye un lector de tarjetas que da acceso a una zona protegida del sistema de seguridad.

3. Método según la reivindicación 2, en el que el anuncio incluye un identificador de tipo de servicio del lector de tarjetas.

4. Método según la reivindicación 1, en el que el controlador aguas abajo incluye una cámara que capta imágenes de una zona protegida del sistema de seguridad.

5. Método según la reivindicación 4, en el que el anuncio incluye un identificador de tipo de servicio de la cámara.

6. Método según la reivindicación 1, que comprende además:

la multidifusión por parte del primer controlador de pasarela de un identificador de grupo de servicios del grupo de servicios del controlador aguas abajo; y
el anuncio por parte del controlador aguas abajo del tipo de servicio en respuesta a la multidifusión.

7. Método según la reivindicación 1, en el que el canal de sesión L5 está cifrado.

8. Método según la reivindicación 1, que comprende además el establecimiento por parte del controlador aguas abajo y del primer controlador de pasarela de una conexión DNS de multidifusión sin configuración tal y como ha sido definida por el Grupo de Trabajo Zeroconf.

9. Aparato que comprende:

un controlador aguas abajo de un sistema de seguridad, estando en controlador aguas abajo configurado para transmitir un anuncio de un tipo de servicio del controlador aguas abajo en una subred; y
un primer controlador de pasarela del sistema de seguridad, estando el primer controlador de pasarela configurado para detectar el anuncio y autenticar al controlador aguas abajo como parte de un grupo de servicios correspondiente al tipo de servicio,
en el que el primer controlador de pasarela además está configurado para enviar una petición de conexión al controlador aguas abajo,
en el que el primer controlador de pasarela y el controlador aguas abajo además están configurados para establecer una conexión L4 basada en la petición y un canal de sesión L5 a través de la conexión L4,
en el que el primer controlador de pasarela además está configurado para guardar unas características identificativas del controlador aguas abajo contenidas en el anuncio en una tabla de mapas de sistema y una tabla de estados de servicio asociadas al grupo de servicios,

en el que el controlador aguas abajo además está configurado para guardar unos datos relativos a la conexión L4 en un archivo de estado de pasarela de una memoria del controlador aguas abajo,
en el que los datos relativos a la conexión L4 incluyen al menos una primera dirección MAC del primer controlador de pasarela, y
en el que el controlador aguas abajo además está configurado para rechazar una segunda conexión de un segundo controlador de pasarela cuando una segunda dirección MAC del segundo controlador aguas abajo recibida por el controlador aguas abajo no coincida con la primera dirección MAC del primer controlador de pasarela almacenada en el archivo de estado de pasarela.

10. Aparato según la reivindicación 9, en el que el controlador aguas abajo incluye un controlador de acceso.

11. Aparato según la reivindicación 10, en el que el controlador de acceso incluye un lector de tarjetas que da acceso a una zona protegida del sistema de seguridad.

12. Aparato según la reivindicación 11, en el que el anuncio incluye un identificador de tipo de servicio del lector de tarjetas.

13. Aparato según la reivindicación 9, en el que el controlador aguas abajo incluye una cámara que está configurada para captar imágenes de una zona protegida del sistema de seguridad.

14. Aparato según la reivindicación 13, en el que el anuncio incluye un identificador de tipo de servicio de la cámara.

15. Aparato según la reivindicación 9, en el que un procesador del primer controlador de pasarela está configurado para multidifundir un identificador de grupo de servicios del grupo de servicios del controlador aguas abajo, y en el que el controlador aguas abajo está configurado para anunciar el tipo de servicio en respuesta a la multidifusión.

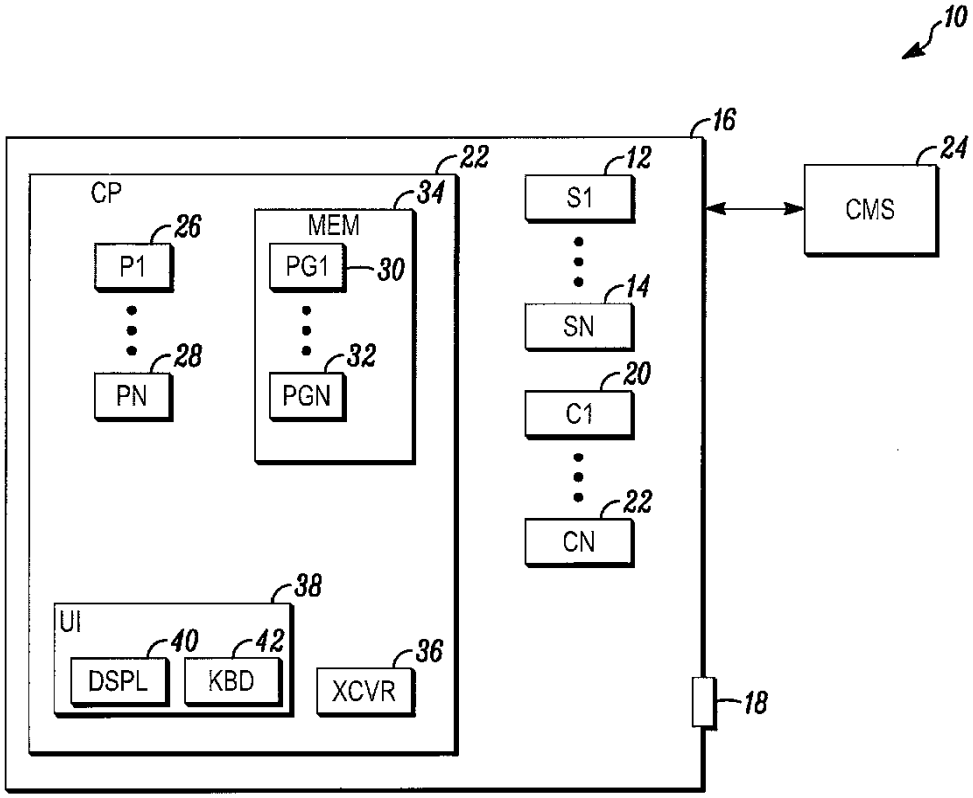
10
16
22
CP
34
MEM
26
P1
PG1
30
28
PN
32
PGN
12
S1
14
SN
20
C1
22
CN
24
CMS
38
UI
40
42
DSPL
KBD
36
XCVR
18

FIG. 1

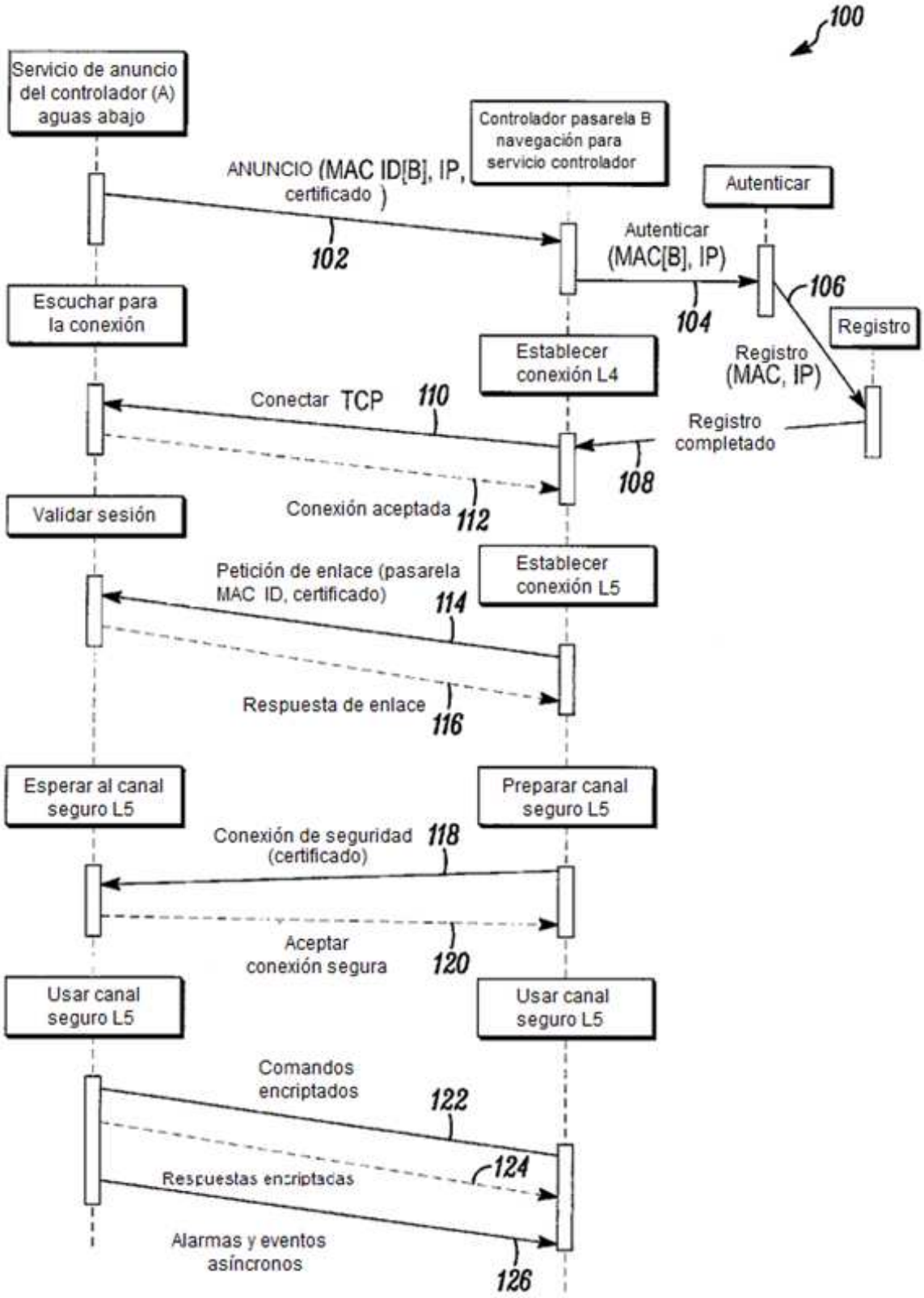
100
Servicio de anuncio del controlador (A) aguas abajo
Controlador pasarela B navegación para servicio controlador
Autenticar
ANUNCIO (MAC ID[B], IP, certificado)
102
Autenticar (MAC[B], IP)
104
106
Escuchar para la conexión
Registro
Establecer conexión L4
Registro (MAC, IP)
Conectar TCP
110
Registro completado
108
Validar sesión
Conexión aceptada
112
Petición de enlace (pasarela MAC ID, certificado)
Establecer conexión L5
114
Respuesta de enlace
116
Esperar al canal seguro L5
Preparar canal seguro L5
Conexión de seguridad (certificado)
118
Aceptar conexión segura
120
Usar canal seguro L5
Usar canal seguro L5
Comandos encriptados
122
124
Respuestas encriptadas
Alarmas y eventos asíncronos
126

FIG. 2