

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 372 329**

51 Int. Cl.:
H04L 29/06 (2006.01)
G08B 25/00 (2006.01)
H04N 7/18 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **08753757 .7**
96 Fecha de presentación: **07.05.2008**
97 Número de publicación de la solicitud: **2153614**
97 Fecha de publicación de la solicitud: **17.02.2010**

54 Título: **SISTEMA Y PROCEDIMIENTO PARA INTERCAMBIAR DATOS ENTRE UN PRIMER SISTEMA DE PROCESAMIENTO DE DATOS Y UN SEGUNDO SISTEMA DE PROCESAMIENTO DE DATOS MEDIANTE POR LO MENOS UNA RED DE COMUNICACIÓN PARCIALMENTE PÚBLICA.**

30 Prioridad:
07.05.2007 NL 2000632

45 Fecha de publicación de la mención BOPI:
18.01.2012

45 Fecha de la publicación del folleto de la patente:
18.01.2012

73 Titular/es:
SPECTATOR INTELLECTUAL PROPERTIES B.V.
VENESTRAAT 1-3
4931 BM GEERTRUIDENBERG, NL

72 Inventor/es:
KLOONEN, Marinus, Adrianus, Hendrikus;
VAN DEN HOEK, Rolf, Martijn;
ERMSTRANG, Gerrit, Gijsbert;
VAN DE WATER, Godefridus, Johannes y
HERMES, Hubertus, Franciscus, Maria

74 Agente: **Zea Checa, Bernabé**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

ES 2 372 329 T3

DESCRIPCIÓN

Sistema y procedimiento para intercambiar datos entre un primer sistema de procesamiento de datos y un segundo sistema de procesamiento de datos mediante por lo menos una red de comunicación parcialmente pública

5 **[0001]** La presente invención se refiere a un dispositivo y procedimiento para intercambiar datos entre un primer sistema de procesamiento de datos y un segundo sistema de procesamiento de datos mediante una red de comunicación por lo menos parcialmente accesible al público. La presente invención se refiere particularmente a un sistema para vigilancia de una primera ubicación desde una segunda ubicación, haciendo uso de tal dispositivo.

10 **[0002]** Cuando se transmiten datos desde una primer sistema de procesamiento de datos a un segundo sistema de procesamiento de datos mediante una red de comunicación por lo menos parcialmente accesible al público, tal como Internet, se utilizan protocolos de comunicación, normalmente el protocolo de Internet o un protocolo similar. Además de tener varias ventajas, estos protocolos presentan el inconveniente de que personas con intento malicioso, que tienen acceso a la red de comunicación relevante por lo menos parcialmente accesible al público, pueden tener acceso (también denominado "piratería informática") a los sistemas de procesamiento de datos conectados a la red de comunicación en una manera relativamente simple mediante tal protocolo de comunicación
15 cuando existe la posibilidad de presentarse a una parte confiable en algún lugar en la red de comunicación. Con frecuencia esto es posible ya que hacen uso inteligente de errores de software, errores de usuario y/o errores de ajuste de por ejemplo cortafuegos, enrutadores o aplicaciones conectadas a la red de comunicación por lo menos parcialmente accesible al público.

20 **[0003]** Las técnicas de seguridad conocidas tales como cortafuegos, las cuales generalmente se implementan como soluciones de software, aún pueden desviarse y de este modo formar un riesgo de seguridad. La función de los sistemas de procesamiento de datos conectados a la red de comunicación por lo menos parcialmente accesible al público, y otros sistemas conectados mediante estos sistemas pueden accederse de este modo. La seguridad de los datos por lo tanto no puede garantizarse.

25 **[0004]** Dos campos de aplicación en los que esto resulta particularmente problemático son los sistemas de seguridad y la atención médica para, entre otros fines, vigilancia remota de una ubicación u objeto o para comunicación con esa ubicación o ese objeto.

30 **[0005]** En el caso del sistema de seguridad, tales sistemas pueden obviar la necesidad de la presencia de una persona física en la ubicación para vigilancia, reducir el número de personal de seguridad presente, incrementar el sentido de seguridad del personal de seguridad presente, y crear la posibilidad de comprobar la seguridad existente al proporcionar medios que permiten la vigilancia remota de esta ubicación, con frecuencia locales (comerciales) tales como un banco o una tienda, por ejemplo de una joyería.

35 **[0006]** Un sistema de seguridad por ejemplo comprende un sensor tal como un contacto de puerta o un detector de movimiento en una primera ubicación con el fin de generar una señal de alarma la cual se transmite a una segunda ubicación. Esto generalmente tiene lugar mediante una infraestructura opcional y específicamente asignada, por ejemplo PSTN o ISDN.

40 **[0007]** En la segunda ubicación –un centro de información, centro de emergencia o sala de control- la señal se convierte en una señal discernible para un guardia de seguridad, tal como una señal visible, audible o táctil. El guardia de seguridad en la segunda ubicación entonces puede decidir qué medida de seguimiento debe tomar. En algunos casos, una señal de alarma también se pasa a los servicios de emergencia tal como la policía o una compañía de seguridad privada.

[0008] Un problema con un sistema como el descrito anteriormente sin embargo es que una gran parte de las señales de alarma generadas por estos sistemas no se activan por la presencia de un ladrón en la ubicación para vigilancia, sino por animales, condiciones climáticas (tal como una tormenta), equipo ajustado o activado erróneamente, mantenimiento técnico insuficiente u otras razones, por lo que se genera una falsa alarma.

45 **[0009]** El resultado de ello es que los servicios de emergencia ya no toman medidas basándose en la señal de una alarma, y que una compañía de seguridad privada debe aportar, o un propietario o gerente de la ubicación debe llevar a cabo por sí mismo una inspección.

50 **[0010]** Por lo tanto, cada vez es más usual proporcionar medios para verificar la señal de alarma, que permita a un operario, en el cuarto de control donde llega la señal de alarma, determinar la validez de la señal de alarma. También ha de ser el caso en que un guardia de seguridad en un cuarto de control debe llevar a cabo una inspección por su propia iniciativa –por ejemplo en momentos establecidos- independientemente de cualquier señal de alarma o, inversamente, ya está al tanto de la llegada de, por ejemplo, un proveedor en instante en el que la ubicación se encuentra inhabitada o no tiene protección. Para permitir la vigilancia de la ubicación en ese momento

se encuentran colocados, además de posibles sensores tales como contactos y detectores de movimiento, medios de grabación audiovisual tales como cámaras con las cuales un operario puede formar una imagen más detallada de la primera ubicación después de recibir una señal de alarma.

5 **[0011]** El medio de grabación audiovisual para verificar la señal de alarma puede formar parte de un sistema de circuito cerrado de televisión el cual normalmente se implemente utilizando un primer sistema de procesamiento de datos adaptado para comunicarse mediante un protocolo de comunicación, tal como el protocolo de Internet. Para intercambiar datos entre la primera ubicación y la segunda ubicación, y opcionalmente también ubicaciones de servicios de emergencia, el sistema de procesamiento de datos en la primera ubicación puede conectarse mediante una conexión de comunicación con un sistema de procesamiento de datos en la segunda ubicación, el cual también
10 está adaptado para comunicarse mediante el protocolo de comunicación en cuestión, tal como el protocolo de Internet. El primer sistema de procesamiento de datos y el segundo sistema de procesamiento de datos nuevamente se conectan mediante una red por lo menos parcialmente pública, en la cual un protocolo de comunicación, por ejemplo el protocolo de Internet, se opera por razones de simplicidad de la comunicación. Además, es normal que la señal de alarma se transmita por sí misma mediante una conexión diferente, tal como la conexión telefónica
15 dedicada antes mencionada.

[0012] Los datos, por ejemplo material visual grabado en una ubicación para vigilancia, se transmiten de este modo desde un primer sistema de procesamiento de datos en la ubicación para vigilancia hasta un segundo sistema de procesamiento de datos en el cuarto de control, y los datos de comando, por ejemplo para accionar medios de grabación para generar el material visual, se transmiten desde el segundo sistema de procesamiento de datos en el
20 cuarto de control hasta el primer sistema de procesamiento de datos en la primera ubicación. Sin embargo, el peligro de estos sistemas de procesamiento de datos que son pirateados hace uso de una red de comunicación por lo menos parcialmente accesible al público menos atractiva sin protección adicional contra esta piratería informática. En este caso la mejora del intercambio de datos puede tener lugar con el sistema de procesamiento de datos y otros sistemas conectados al sistema de procesamiento de datos.

25 **[0013]** Esto es debido a que una persona con intento malicioso puede tener acceso a todas las ubicaciones y dispositivos conectados a la red de comunicación tan pronto como haya podido tener acceso a una de las ubicaciones pirateando el sistema de procesamiento de datos asociado a esta ubicación. Entonces al presentarse como un usuario regular del sistema de procesamiento de datos de la red de comunicación que se ha pirateado, se considera que es una parte confiable en otras redes de comunicación conectadas al sistema de procesamiento de
30 datos, y que también puede tener acceso a la misma de una forma relativamente simple.

[0014] Con un sistema de procesamiento de datos es posible intercambiar no sólo datos tales como audio, vídeo e información de control, sino también virus informático, correo electrónico (*spam*) y datos de personas maliciosas que tratan de piratear la red de comunicación. Todos estos datos se transportan indiscriminadamente sobre la misma conexión de comunicación. En los sistemas de seguridad conocidos, la seguridad contra intercambio de datos
35 indeseable se gestiona, por ejemplo mediante un cortafuegos o encriptación de datos. Cuando tales soluciones se basan en software, la seguridad puede saltarse encontrando una contraseña, una clave de encriptación o haciendo uso de errores de software.

[0015] JEFFREY MENOHER, Owl Computing Technologies en "*Owl Products Help Manage Medical Information Security in Compliance with HIPAA Regulations*" describe transferencia segura de datos médicos en un sentido.

40 **[0016]** El prospecto de Tecton Limited "*High Performace IP solutions –Network Toolkit*" describe una combinación de dos redes RS232 conectadas a través de internet, una red de área local de una red de empresa. Los datos en las redes que se han de conectar se encuentran de este modo en formato RS232 mientras que la conexión entre las redes están en formato IP.

[0017] La Solicitud de patente americana US 2006/139162 describe en los párrafos [0024-0027] un "Eje" –de
45 transferencia continua, que convierte datos RS 422 en datos IP para transmitir estos datos. Se menciona, además, el uso de cámaras que pueden producir paquetes de protocolo de Ethernet. Sin embargo, no describe la conexión de dos redes IP mediante una conexión de datos inaccesible al tráfico de datos de acuerdo con el protocolo de Internet. Además, la protección de datos no se describe como propósito en absoluto.

[0018] Por lo tanto, un objetivo de la presente invención es disponer un procedimiento y un sistema para
50 intercambiar datos entre un primer sistema de procesamiento de datos y un segundo sistema de procesamiento de datos mediante una red de comunicación por lo menos parcialmente accesible al público con lo cual se evitan por lo menos parcialmente los inconvenientes indicados anteriormente.

[0019] Otro objetivo de la presente invención es disponer un sistema de vigilancia de una primera ubicación desde una segunda ubicación, en el que la primera y la segunda ubicación comprenden un sistema de procesamiento de

datos adaptado para comunicarse de acuerdo con un protocolo de comunicación haciendo uso del procedimiento indicado anteriormente.

[0020] Para este fin, la invención dispone un sistema de comunicación para intercambiar datos, mediante una red de comunicación por lo menos parcialmente accesible al público, entre una primera red de comunicación con al menos un sistema de procesamiento de datos, por ejemplo un ordenador o una cámara de seguridad, y una segunda red de comunicación con al menos un sistema de procesamiento de datos, donde ambos sistemas de procesamiento de datos están adaptados para comunicarse de acuerdo con el protocolo de comunicación, donde el primer sistema de procesamiento de datos se conecta mediante una primera conexión a la red de comunicación por lo menos parcialmente accesible al público y el segundo sistema de procesamiento de datos se conecta mediante una segunda conexión a la red de comunicación por lo menos parcialmente accesible al público, donde la invención se caracteriza por el hecho de que por lo menos una de las conexiones comprende una conexión de datos inaccesible al tráfico de datos de acuerdo con el protocolo de comunicación.

[0021] Una red de comunicación por lo menos parcialmente accesible al público de acuerdo con la presente invención también debe entenderse que se refiere a una red de comunicación privada o una conexión de comunicación privada que es públicamente accesible por cualquier razón o puede ser de cualquier manera susceptible de ser pirateada, tal como una red de comunicación fija basada en IP tal como la Internet, intranet, extranet, LAN, WAN, VPN, HFC, cable o X-DSL, una red de comunicación inalámbrica basada en IP, incluyendo GPRS, W-LAN, WIMAX, EDGE, UMTS o una red de satélites, GSM, GSMdata, HSCSD, ISDN o una red PSTN.

[0022] Un sistema de procesamiento de datos puede comprender un ordenador, pero también cámaras de seguridad digitales u otros sistemas que estén adaptados para generar datos que puedan transportarse mediante un protocolo de Internet o protocolo relacionado, o que estén adaptados para comunicarse mediante dicho protocolo. Tales sistemas pueden conectarse mediante una interfaz analógica o digital a la red de comunicación por lo menos parcialmente accesible al público, donde el protocolo de comunicación puede comprender un protocolo de comunicación de red, y en particular puede comprender un protocolo del grupo de protocolo de Internet (IP), V.110, o X.75.

[0023] Debido a la conexión que es inaccesible mediante el protocolo de comunicación utilizado, no es posible que personas maliciosas tengan acceso desde la red de comunicación, por lo menos parcialmente accesible al público, tal como una red de comunicación inalámbrica o fija basada en IP, una red de comunicación ISDN o PSTN, por medio del protocolo de comunicación utilizado al sistema de procesamiento de datos conectado a la conexión que es inaccesible a través del protocolo de comunicación aplicado.

[0024] Para permitir comunicación mediante la conexión inaccesible al protocolo de comunicación utilizado, los datos deben convertirse de acuerdo con el protocolo de comunicación utilizado en un formato de datos para que pueda accederse a la conexión. La conexión inaccesible al protocolo de comunicación utilizado se proporciona para este propósito en una realización de la presente invención con un conversor de protocolo para convertir datos de acuerdo con el protocolo de comunicación utilizado en datos adecuados para el transporte mediante la conexión inaccesible al protocolo de comunicación utilizado, cuya conexión por ejemplo puede comprender una conexión de vídeo, una conexión de audio, o una conexión de datos de acuerdo con el protocolo RS232. Estas conexiones pueden ser aquí de forma analógica y digital.

[0025] En una realización adicional, la presente invención dispone un sistema de comunicación para vigilancia de una primera ubicación, tal como un local (comercial), desde una segunda ubicación utilizando medios de grabación audiovisual tal como cámaras de vídeo o micrófonos situados en la primera ubicación. Esos medios de grabación se conectan aquí a un primer sistema de procesamiento de datos situado en la primera ubicación y se accionan de acuerdo con un protocolo de comunicación determinado. El sistema de acuerdo con la presente invención comprende, además, un cuarto de control situado en la segunda ubicación para mostrar los datos registrados a un observador, por ejemplo, mediante una señal de advertencia tal como una luz o un sonido, o una indicación en un monitor.

[0026] Los datos registrados pueden generarse mediante un sistema de grabación o reproducción de vídeo tal como una cámara, un DVS (emisor de vídeo digital), un DVR (grabadora de vídeo digital) o un sistema CCTV, mediante un sistema de grabación o reproducción de audio tal como un micrófono o un altavoz, mediante un sistema de grabación o reproducción de datos tal como un sensor de movimiento o contacto, un detector de ruptura, un conmutador, un detector de incendios, un sistema de reconocimiento de matrículas o de caras, o un detector de movimiento en vídeo.

[0027] Entre el primer y segundo sistema de procesamiento de datos se encuentra una conexión de comunicación, por lo menos para intercambiar datos registrados generados por el medio de grabación. En una realización de la presente invención, la señal de alarma del sensor también se intercambia mediante la conexión de comunicación. La

conexión de comunicación comprende por lo menos una conexión inaccesible al tráfico de datos de acuerdo con el protocolo de comunicación utilizado.

5 **[0028]** Debido al uso de una conexión que es inaccesible de acuerdo con el protocolo de comunicación utilizado, el sistema de acuerdo con la presente invención no puede intercambiar datos no deseados, tal como virus informáticos, correo electrónico (spam) y datos de personas maliciosas, de la red de comunicación por lo menos parcialmente accesible al público al primer o segundo sistema de procesamiento de datos o desde el primer sistema de procesamiento de datos hasta el segundo sistema de procesamiento de datos o viceversa, aparte de lo que se ha definido para esta conexión inaccesible.

10 **[0029]** El sistema de comunicación de acuerdo con la presente invención puede estar adaptado para este propósito de manera que el primer sistema de procesamiento de datos se conecte al medio de grabación para proporcionar datos grabados desde una primera ubicación, por ejemplo a una cámara de vídeo o a un micrófono, y el primer sistema de procesamiento de datos está adaptado para transmitir los datos grabados de acuerdo con el protocolo de Internet al segundo sistema de procesamiento de datos mediante la red de comunicación, mientras que el segundo sistema de procesamiento de datos está adaptado para reproducir los datos grabados a un observador
15 en una segunda ubicación. La primera conexión entre el primer sistema de procesamiento de datos y la red de comunicación por lo menos parcialmente accesible al público aquí puede ser inaccesible mediante por ejemplo el protocolo de Internet, y la segunda conexión entre el segundo sistema de procesamiento de datos y la red de comunicación por lo menos parcialmente accesible al público puede ser inaccesible mediante por ejemplo el protocolo de Internet, donde el primer y segundo sistema de procesamiento de datos pueden comprender uno o más
20 sistemas de procesamiento de datos.

[0030] El segundo sistema de procesamiento de datos puede estar adaptado, además, para recibir órdenes del observador y para convertir las órdenes recibidas en datos de comando de acuerdo con el protocolo de Internet. El segundo sistema de procesamiento de datos está adaptado aquí entonces para transmitir datos de comando de acuerdo con el protocolo de Internet al primer sistema de procesamiento de datos, el cual está adaptado para recibir
25 datos de comando y reenviar los datos de comando a un dispositivo que está conectado al primer sistema de procesamiento de datos y el cual está adaptado para ejecutar los datos de comando, los cuales además pueden comprender una señal de sonido, un mensaje hablado, una señal de vídeo, un sistema de respuesta de voz, un sistema DTMF, una señal de control para un dispositivo tal como iluminación, una cámara PTZ, un dispositivo de bloqueo o una máquina de producción.

30 **[0031]** De esta manera, el dispositivo puede utilizarse para permitir que un operario en el cuarto de control hable a una persona presente en la primera ubicación, o por ejemplo para abrir una entrada a una parte de la primera ubicación para un proveedor que realice una entrega nocturna, para encender o apagar la iluminación en tal situación o en caso de un problema sospechoso, o por ejemplo para accionar una máquina cuando se ha determinado, de manera remota o de otra manera, que es necesario un ajuste o un encendido o apagado.

35 **[0032]** Además de la vigilancia de objetos, el sistema de comunicación de acuerdo con la presente invención puede utilizarse para controlar personas, por ejemplo personas de la tercera edad o pacientes que requieren cuidado. En tal caso, el cuarto de control es atendido por cuidadores o el cuarto de control proporciona acceso a cuidadores. Además de controlar personas o ubicaciones, es posible utilizar adicionalmente la presente invención para asegurar datos presentes en uno de los sistemas de procesamiento de datos, tal como archivos de pacientes o
40 información similar relacionada con la persona.

[0033] Es el caso en todas las aplicaciones de la presente invención que, a diferencia de un conexión entre una pluralidad de sistemas de procesamiento de datos que se basa en el protocolo de comunicación, el tráfico de datos en la conexión no accesible mediante el protocolo de comunicación se hace posible mediante ajustes físicos de la conexión que es inaccesible mediante el protocolo de comunicación. Por consiguiente no es posible que una
45 persona maliciosa entre en el primer o el segundo sistema de procesamiento de datos desde la red de comunicación por lo menos parcialmente pública, o entre el segundo sistema de procesamiento de datos desde el primer sistema de procesamiento de datos o que haya entrado en el mismo, o viceversa; para entrar en el primer sistema de procesamiento de datos desde el segundo sistema de procesamiento de datos o que haya entrado en el mismo, puesto que no es posible el intercambio de datos no deseado mediante la conexión. El intercambio de datos no deseado no es particularmente posible por medio de un uso inadecuado, tal como el uso inadecuado de errores de
50 software, el uso inadecuado de ajustes de software, tal como ajustes de usuario.

[0034] En una realización de la presente invención, el medio de grabación en la primera ubicación genera una señal audiovisual de banda ancha, la cual debe llevarse al cuarto de control. El cuarto de control está adaptado aquí para permitir que un operario seleccione diferentes cámaras dispuestas en el espacio para vigilancia, para poder
55 seguir las imágenes generadas por estas cámaras. Se disponen, además, medios de accionamiento para accionar cámaras móviles o para el accionamiento remoto de iluminación u otros dispositivos, tales como máquinas de producción. Además, el operario puede hablar de manera remota a una persona presente en la primera ubicación,

tal como un conductor que hace una entrega, desde la segunda ubicación por medio de una conexión de comunicación de dos vías. El medio de grabación se conecta aquí a un primer sistema de procesamiento de datos el cual es accionado de acuerdo con el protocolo de Internet. El primer sistema de procesamiento de datos se conecta por Internet al segundo sistema de procesamiento de datos situado en el cuarto de control. Entre el primer sistema
 5 de procesamiento de datos y el segundo sistema de procesamiento de datos se encuentran uno o más conversores de protocolo, los cuales convierten los datos grabados de acuerdo con el protocolo de Internet en un formato seguro, el cual no permite la inclusión de datos no deseados. Un ejemplo de una señal la cual se ha encontrado que es adecuada aquí es una señal de vídeo (analógica), una señal de audio (analógica), o una interfaz RS-232 con un protocolo de datos muy específico predefinido. El convertor de protocolo está formado aquí por medio de un primer
 10 sub-dispositivo el cual convierte una señal de vídeo de acuerdo con un protocolo de Internet (denominado señal de vídeo continua) en una señal de vídeo analógica. Un dispositivo que se ha encontrado adecuado para este fin es un emisor de vídeo. La señal de vídeo generada de este modo se limita a un segundo sub-dispositivo que, una vez más, la convierte en una señal que puede ser transportada mediante el protocolo de Internet y la cual se envía al segundo sistema de procesamiento de datos en el cuarto de control mediante la red de comunicación utilizada. El
 15 segundo sub-dispositivo puede estar formado igualmente por un dispositivo emisor de vídeo. En una realización de la presente invención, la segunda conexión comprende un segundo convertor de protocolos, el cual puede ser idéntico al primero, con el fin de incrementar adicionalmente el nivel de seguridad.

[0035] En otra realización, el operario puede realizar una conexión con la primera ubicación desde la segunda ubicación para llevar a cabo una comprobación preventiva, o para llevar a cabo una ronda de inspección virtual o
 20 para realizar servicios adicionales para clientes, tal como por ejemplo asistir a entregas nocturnas controladas a distancia o comprobar y operar instalaciones y máquinas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0036] La invención se describirá ahora con referencia a las siguientes figuras, en las cuales:

- 25 - La Figura 1 muestra una primera realización de un sistema para intercambiar datos de acuerdo con la presente invención;
- La Figura 2 muestra una segunda realización de un sistema para intercambiar datos de acuerdo con la presente invención;
- La Figura 3 muestra una tercera realización de un sistema para intercambiar datos de acuerdo con la presente invención;
- 30 - La Figura 4 muestra una cuarta realización de un sistema para intercambiar datos de acuerdo con la presente invención;
- La Figura 5 muestra una quinta realización de un sistema para intercambiar datos de acuerdo con la presente invención.

[0037] La figura 1 muestra una primera realización de la presente invención, en la cual se conectan una serie de
 35 sensores del grupo de marcadores de alarma, medios de grabación de audio y vídeo y equipo de visualización en la primera ubicación 105 a un sistema de procesamiento de datos formado por el sistema de circuito cerrado de televisión (CCTV) 100. El sistema de circuito cerrado de televisión 100 está conectado en una comunicación de datos con un primer convertor de protocolo 200. Pueden enviarse datos de vídeo 115, datos de audio 125 o datos de control 135 o combinaciones de los mismos, al convertor de protocolo 200 mediante la conexión para ser
 40 convertidos por el convertor de protocolo 200 en datos 405 de acuerdo con el protocolo de Internet o protocolo de comunicación de red similar. Estos datos 405 se transmiten mediante el convertor de protocolo 200 a la red de comunicación por lo menos parcialmente accesible al público 400. Mediante la red de comunicación por lo menos parcialmente accesible al público 400, los datos 405 de acuerdo con el protocolo de Internet se reenvían a un primer cuarto de control 300 que se conecta mediante un segundo convertor de protocolo 310 a la red de comunicación por
 45 lo menos parcialmente accesible al público 400. El segundo convertor de protocolo convierte los datos 405 de acuerdo con el protocolo de Internet en datos de vídeo 115', datos de audio 125', y datos de control 135', los cuales se reenvían al primer cuarto de control 300.

[0038] La Figura 2 muestra una siguiente realización de la presente invención en la cual se conectan una serie de
 50 sensores del grupo de marcadores de alarma, medios de grabación de audio y vídeo y equipo de visualización a una primera ubicación 106 a un sistema de procesamiento de datos formado por un sistema de circuito cerrado de televisión 100. El sistema de circuito cerrado de televisión 100 está conectado en una comunicación de datos con un primer convertor de protocolo 206. Pueden enviarse datos de audio 126 o datos de control 136 o combinaciones de los mismos al convertor de protocolo 206 mediante la conexión. También se encuentra conectada al convertor de protocolo 200 una cámara de vídeo 103 que proporciona datos de vídeo 116 al convertor de protocolo 206. El
 55 convertor de protocolo 206 convierte datos de vídeo 116, datos de audio 126 y datos de control 136 en datos 406 de

acuerdo con el protocolo de Internet. Estos datos 406 de acuerdo con el protocolo de Internet se transmiten mediante el conversor de protocolo 206 en la red de comunicación por lo menos parcialmente accesible al público 400. Mediante la red de comunicación por lo menos parcialmente accesible al público 400, los datos 406 de acuerdo con el protocolo de Internet se reenvían al primer cuarto de control 300, el cual se conecta mediante un segundo conversor 310 de protocolo a la red de comunicación por lo menos parcialmente accesible al público 400. El segundo conversor de protocolo convierte datos 405 de acuerdo con el protocolo de Internet en datos de vídeo 115', datos de audio 125' y datos de control 135', los cuales se reenvían al primer cuarto de control 300.

[0039] La realización mostrada en la figura 2 tiene la ventaja de que el conversor de protocolo 206 está provisto de medios para comunicarse con la cámara de vídeo 103 por sí conocidos. El conversor de protocolo 206 puede estar formado aquí, por ejemplo, por un emisor de vídeo que puede controlar la cámara de vídeo 103 mediante por ejemplo señales *Pan Tilt Zoom* (PTZ). Como resultado, esta realización puede aplicarse particular y ventajosamente en situaciones donde se dispone un sistema de circuito cerrado de televisión existente en una ubicación, cuyo sistema existente no puede eliminarse o reemplazarse. Las razones de ello pueden ser una aprobación previamente concedida o certificados de seguridad, o inversiones realizadas recientemente para tal sistema de circuito cerrado de televisión. La presente invención hace posible, basándose en un sistema ya existente, proporcionar un sistema de seguridad con menos posibilidades de que un sistema de procesamiento de datos sea pirateado, donde puede obtenerse también una mejor calidad de imagen o velocidad de transmisión de imagen al conectar la cámara 103 existente directamente al conversor de protocolo 206.

[0040] La Figura 3 muestra una tercera realización de la presente invención en la que los sistemas de circuito cerrado de televisión 100, 105, 106 dispuestos en la primera ubicación 105 de la figura 1 y en la primera ubicación 106 de la figura 2 se conectan mediante los respectivos conversores de protocolo 200 y 206 a la red de comunicación por lo menos parcialmente accesible al público 400. Tal realización puede aplicarse particularmente cuando debe controlarse una pluralidad de ubicaciones desde un cuarto de control. El tráfico de datos no puede producirse entre las ubicaciones para vigilancia de cualquier manera mediante el protocolo de Internet, puesto que cada una de las ubicaciones se conecta a la red de comunicación por lo menos parcialmente accesible al público 400 mediante un conversor de protocolo que es inaccesible al protocolo de Internet.

[0041] La Figura 4 muestra una cuarta realización de la presente invención, donde un segundo cuarto de control 320 se conecta mediante un tercer conversor de protocolo 330 a la red de comunicación por lo menos parcialmente accesible al público 400 de modo que los datos 405 de acuerdo con el protocolo de Internet se reenvían al segundo cuarto de control 320, el cual se conecta mediante un tercer conversor de protocolo 330 a la red de comunicación por lo menos parcialmente accesible al público 400.

[0042] Puede realizarse aquí simultáneamente una conexión con dos cuartos de control 300, 320. El segundo conversor de protocolo 310 convierte los datos 405 de acuerdo con el protocolo de Internet en datos de vídeo 115', datos de audio 125' o datos de control 135', los cuales se transmiten al primer cuarto de control 300. El tercer conversor de protocolo 330 convierte los datos 405 de acuerdo con el protocolo de Internet en datos de vídeo 115", datos de audio 125" o datos de control 135", los cuales se transmiten al segundo cuarto de control 320.

[0043] Dicha realización proporciona la ventaja de que, además de múltiples ubicaciones para salvaguardar, también hay presentes múltiples cuartos de control, en el que es posible volver a enrutar una conexión de comunicación existente desde un primer cuarto de control a un segundo cuarto de control. Tal realización por ejemplo puede proporcionar una disposición de respaldo para el primer cuarto de control. También pueden utilizarse cuando los cuartos de control diferentes tienen diferentes potencias. Puede autorizarse aquí a un primer cuarto de control para detectar y tratar robos de banco, mientras que puede autorizarse un segundo cuarto de control para, por ejemplo, tratar situaciones con rehenes.

[0044] La figura 5 muestra todavía otra realización de la presente invención. Esta realización comprende la realización de la figura 4, que está conectada a una realización similar. Dicha conexión proporciona la ventaja de, por ejemplo una señal de vídeo, que genera el sistema de circuito cerrado de televisión 100 y recibe un primer cuarto de control 300, puede reenviarse a un cuarto de control 520 adicional conectado mediante un conversor 510 de protocolo a la red de comunicación por lo menos parcialmente accesible al público 400, que se muestra dos veces en el dibujo para mayor claridad. El primer cuarto de control 300 puede ser aquí un cuarto de control de una empresa de seguridad privada, mientras que el segundo cuarto de control 520 puede ser de un cuerpo oficial tal como la policía. De esta manera, se proporciona la funcionalidad de "enrutamiento externo", y un intercambio de datos no deseado mediante esta conexión inaccesible se hace aun más difícil.

[0045] Además de las realizaciones mostradas, la presente invención presenta otras muchas variaciones las cuales quedan cubiertas todas por las siguientes reivindicaciones.

REIVINDICACIONES

1. Sistema de comunicación para intercambiar datos entre

- una primera red de comunicación, con por lo menos un primer sistema de procesamiento de datos, adaptado para comunicarse de acuerdo con el protocolo de Internet;

5 y

- una segunda red de comunicación, con por lo menos un segundo sistema de procesamiento de datos, adaptado para comunicarse de acuerdo con el protocolo de Internet;

a través de:

- una tercera red de comunicación por lo menos parcialmente accesible al público,

10 en el que:

- el primer sistema de procesamiento de datos está conectado a través de una primera conexión a la tercera red de comunicación; y

- el segundo sistema de procesamiento de datos está conectado a través de una segunda conexión a la tercera red de comunicación;

15 caracterizado por el hecho de que

- por lo menos una de las conexiones comprende una conexión de vídeo inaccesible al tráfico de datos de acuerdo con el protocolo de Internet, en el que

- una de dichas conexiones comprende, además

20

- un primer emisor de vídeo adaptado para convertir una señal de vídeo de acuerdo con el protocolo de internet en una señal de vídeo (analógica); y

- un segundo emisor de vídeo adaptado para convertir la señal de vídeo (analógica) en una señal que sea transportable a través del protocolo de internet.

2. Sistema de comunicación según la reivindicación 1, caracterizado por el hecho de que la tercera red de comunicación por lo menos parcialmente accesible al público es una red de comunicación del grupo de:

25

- una red de comunicación fija basada en IP tal como la Internet, Intranet, extranet, LAN, WAN, VPN, HFC, cable o X-DSL;

- una red de comunicación inalámbrica basada en IP, que incluye GPRS, W-LAN, WIMAX, EDGE, UMTS o satélite;

- un GSM, GSMdata, HSCSD;

30

- una ISDN;

- una PSTN.

3. Sistema de comunicación según cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que por lo menos una de las conexiones comprende por lo menos uno de:

- una conexión de datos analógica;

35

- una conexión de datos digital.

4. Sistema de comunicación según cualquiera de las reivindicaciones anteriores, caracterizado por el hecho de que:

- el primer sistema de procesamiento de datos está conectado al medio de grabación para proporcionar datos grabados de una primera ubicación;

40

- el primer sistema de procesamiento de datos está adaptado para transmitir los datos grabados de acuerdo con el protocolo de comunicación utilizado al segundo sistema de procesamiento de datos mediante la tercera red de comunicación;

- el segundo sistema de procesamiento de datos está adaptado por lo menos para reproducir los datos grabados a un observador en una segunda ubicación.

5. Sistema de comunicación según la reivindicación 4, caracterizado por el hecho de que el medio de grabación para proporcionar datos grabados comprende medios del grupo de:

- 5
- un sistema de grabación o reproducción de vídeo tal como una cámara, un DVS (emisor de vídeo digital), un DVR (vídeo grabadora digital) o un sistema de CCTV;
 - un sistema de grabación o reproducción de audio tal como un micrófono o un altavoz;
 - un sistema de grabación o reproducción de datos tal como un sensor de movimiento o de contacto, un detector de ruptura, un conmutador, un detector de incendios, un sistema de reconocimiento de matrículas o de caras, o un detector de movimiento en vídeo.
- 10

6. Sistema de comunicación según la reivindicación 4 o 5, caracterizado por el hecho de que

- el segundo sistema de procesamiento de datos está adaptado para recibir órdenes del observador;
- el segundo sistema de procesamiento de datos está adaptado para convertir órdenes recibidas a datos en formatos de datos adecuados de acuerdo con el protocolo de comunicación utilizado;

- 15
- el segundo sistema de procesamiento de datos está adaptado para transmitir datos de comando de acuerdo con el protocolo de comunicación utilizado al primer sistema de procesamiento de datos;
 - el primer sistema de procesamiento de datos está adaptado para recibir los datos de comando;
 - el primer sistema de procesamiento de datos está adaptado para reenviar los datos de comando a un dispositivo que está conectado al primer sistema de procesamiento de datos y el cual está adaptado para ejecutar los datos de comando.
- 20

7. Sistema de comunicación según la reivindicación 8, caracterizado por el hecho de que los datos de comando se seleccionan del grupo de:

- una señal de sonido;
- un mensaje hablado;
- una señal de vídeo;
- un sistema de respuesta de voz;
- un sistema DTMF;
- una señal de control para un dispositivo tal como iluminación, una cámara PTZ, un dispositivo de bloqueo o una máquina de producción.

30 8. Procedimiento para intercambiar datos,

entre:

- una primera red de comunicación, con por lo menos un primer sistema de procesamiento de datos, adaptado para comunicarse de acuerdo con el protocolo de Internet;

y

- 35
- una segunda red de comunicación, con por lo menos un segundo sistema de procesamiento de datos, adaptado para comunicarse de acuerdo con el protocolo de Internet;

a través de:

- una tercera red de comunicación por lo menos parcialmente accesible al público,

en el que:

- 40
- el primer sistema de procesamiento de datos está conectado a través de una primera conexión a la tercera red de comunicación; y

- el segundo sistema de procesamiento de datos está conectado a través de una segunda conexión a la tercera red de comunicación;

caracterizado por el hecho de que

5 - por lo menos una de las conexiones comprende una conexión de vídeo inaccesible al tráfico de datos de acuerdo con el protocolo de Internet,

que comprende las etapas de:

- convertir mediante un primer emisor de vídeo incluido en uno de dichas conexiones una señal de vídeo de acuerdo con el protocolo de internet en una señal de vídeo (analógica); y

10 - convertir mediante un segundo emisor de vídeo incluido en uno de dichas conexiones la segunda señal de vídeo (analógica) en una señal que sea transportable a través del protocolo de internet.

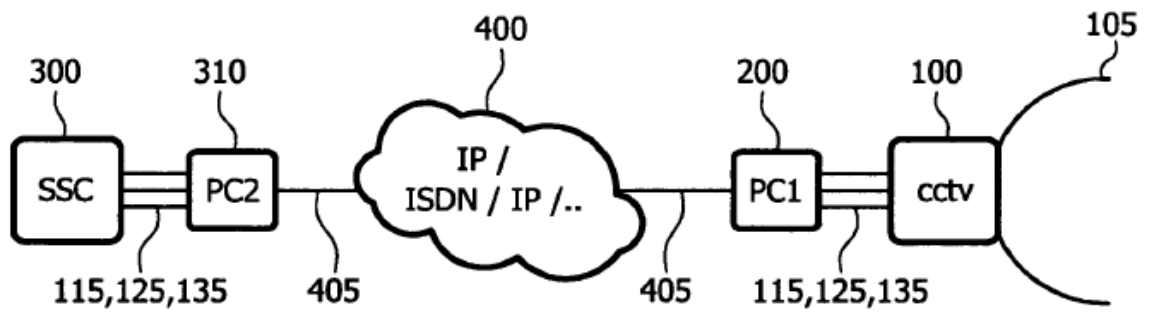


FIG. 1

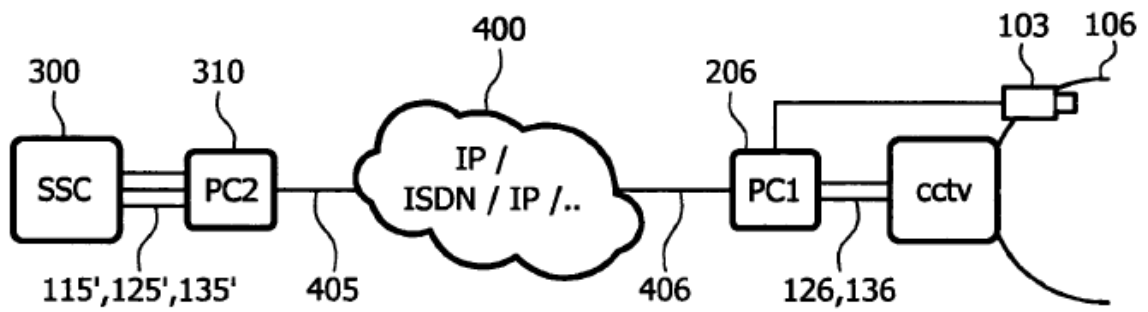


FIG. 2

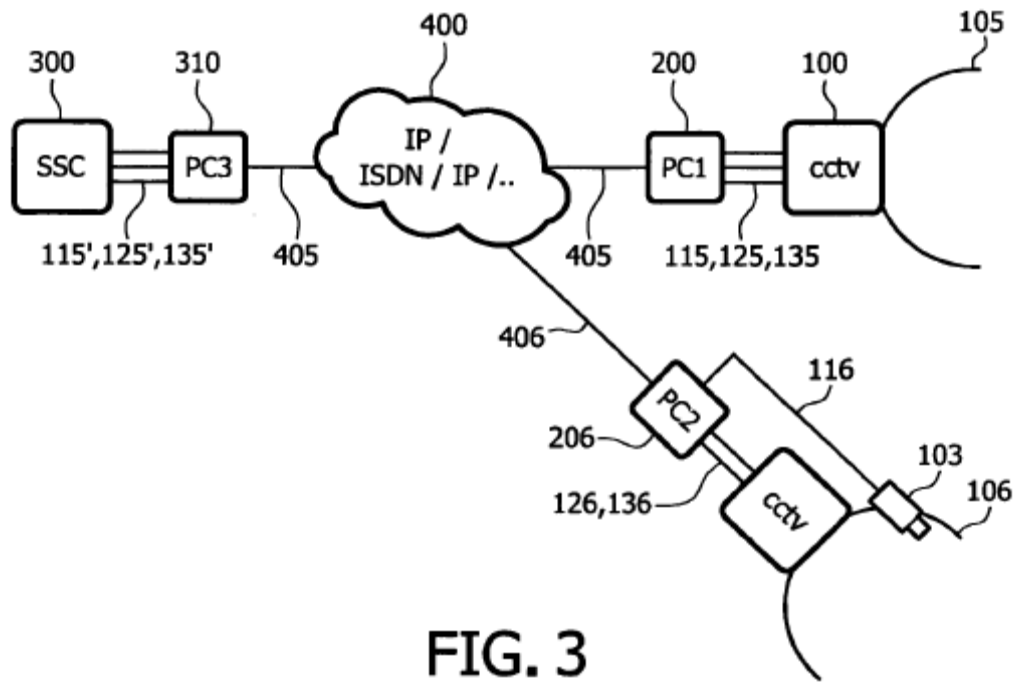


FIG. 3

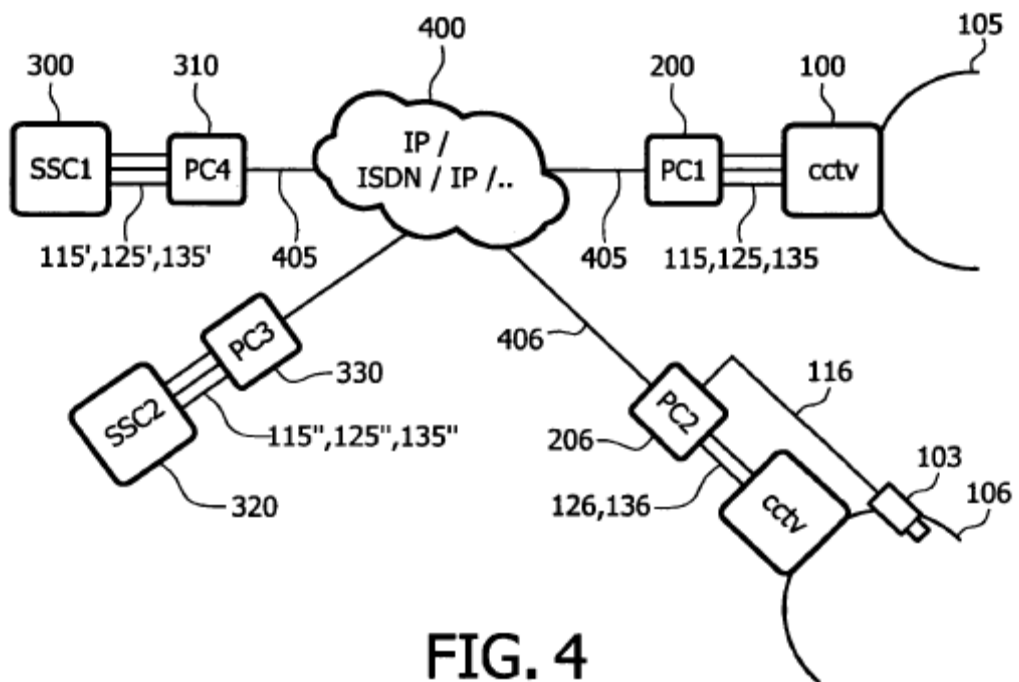


FIG. 4

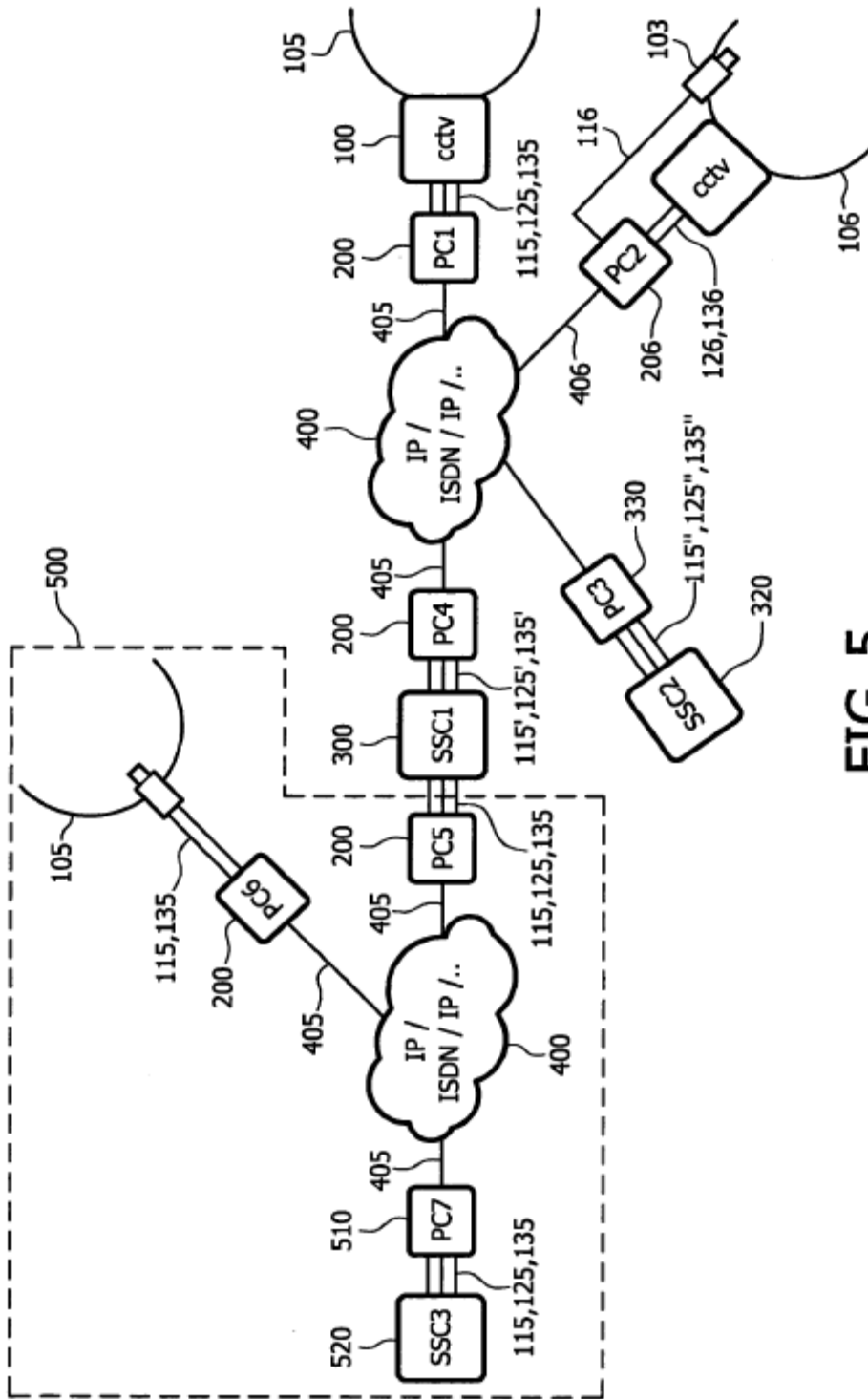


FIG. 5