(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 587 027**

(51) Int. CI.:

B66B 1/46 (2006.01)
B66B 5/00 (2006.01)
G08B 13/196 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.03.2012 PCT/EP2012/055342**

(87) Fecha y número de publicación internacional: **04.10.2012 WO12130808**

(96) Fecha de presentación y número de la solicitud europea: **26.03.2012 E 12710294 (5)**

(97) Fecha y número de publicación de la concesión europea: **18.05.2016 EP 2691330**

(54) Título: **Dispositivo de control de acceso con al menos una unidad de vídeo**

(30) Prioridad:

28.03.2011 EP 11159995

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.10.2016

(73) Titular/es:

INVENTIO AG (100.0%)
Seestrasse 55
6052 Hergiswil , CH

(72) Inventor/es:

WAGNER, PHILIPPE

(74) Agente/Representante:

AZNÁREZ URBIETA, Pablo

DESCRIPCIÓN

Dispositivo de control de acceso con al menos una unidad de vídeo

La invención se refiere a un dispositivo de control de acceso de una instalación de ascensor con al menos una unidad de vídeo, estando conectadas la o las unidades de vídeo a una unidad de control a través de una red de comunicación.

En algunos edificios es necesario un control de acceso para evitar que determinadas zonas de los edificios estén accesibles para el público. En muchos edificios, este control de acceso está en la entrada al edificio. Sin embargo, muchos edificios más grandes, como edificios de oficinas, centros comerciales, edificios de viviendas, etc. tienen zonas que también deben ser públicamente accesibles, mientras que a otras zonas sólo deben poder acceder determinadas personas, por ejemplo porque para tales zonasdebe aplicarse un nivel de seguridad más alto. Por ejemplo, la planta baja de un edificio puede ser públicamente accesible, mientras que las plantas superiores son privadas y no son públicamente accesibles o sólo lo son en determinadas condiciones.

La solicitud de patente europea con el número de solicitud 10167984.3 describe un sistema de control de seguridad para un sistema de ascensor que incluye al menos una cabina de ascensor. El sistema incluye un dispositivo de control de acceso que determina la presencia de un individuo no autorizado dentro de un área definida y emite una señal. La señal emitida se utiliza para bloquear el uso del sistema de ascensor.

El documento D1 US 2009/0208067 A1 describe un sistema de ascensor que controla las puertas del ascensor en función de una cámara de vídeo. Mediante un análisis de índice de color se evalúan imágenes grabadas por la cámara de vídeo en cuanto al lugar de permanencia, la dirección, la velocidad y el tiempo de llegada de una persona a un ascensor. En base a la evaluación se controlan las puertas del ascensor y las funciones de seguridad.

El documento D2 JP 2002046950 describe una cámara de vídeo en una cabina de ascensor que está montada en el techo de la cabina y que graba imágenes de las caras de los pasajeros cuando entran en la cabina.

Para limitar el acceso a plantas individuales se puede limitar el uso de las instalaciones de ascensor de los edificios. Por ejemplo, mediante barreras, compuertas, controles de acceso, torniquetes, personal de seguridad, etc. se puede intentar evitar que personas no autorizadas lleguen a la instalación de ascensor y puedan utilizarla. Este tipo de dispositivos se pueden denominar dispositivos de vigilancia de acceso o de control de acceso.

En la mayoría de los casos, los dueños de los edificios, los arquitectos, los usuarios etc. consideran las barreras, compuertas, controles de acceso, torniquetes, etc. como demasiado voluminosos y antiestéticos. En cambio, los dispositivos de control de acceso más pequeños reducidos al mínimo con frecuencia son poco eficaces y fáciles de eludir. Un objetivo de la invención es proporcionar un dispositivo de control de acceso rentable y eficiente.

La invención se resuelve por medio de las características indicadas en las reivindicaciones independientes. En las reivindicaciones dependientes se indican perfeccionamientos.

Una característica esencial de la invención es que, con ayuda de al menos una unidad de vídeo de un dispositivo de control de acceso de una instalación de ascensor, se detecta la presencia de un objeto en unazona de vigilancia definida del dispositivo de control de acceso y, con los datos determinados o con los resultados de la evaluación determinados por la o las unidades de vídeo, se determina la dirección de movimiento o el lugar de permanencia del objeto dentro delazona de vigilancia. Además, se puede comprobar la autorización del objeto en función de los datos determinados.

El dispositivo de control de acceso, por ejemplo una barrera, una compuerta, una línea o una superficie barrera virtual, etc. de una instalación de ascensor sirve para impedir o dificultar el acceso de objetos no autorizados, por ejemplo personas, visitantes, animales, etc. a una instalación de ascensor. Para ello, el dispositivo de control de acceso incluye al menos una unidad de vídeo conectada a una unidad de control a través de una red de comunicación. La red de comunicación utilizada puede ser de cualquier tipo. Por ejemplo, se podría utilizar una red de comunicación por cable, inalámbrica o por radio. La unidad de control puede estar integrada en la unidad de vídeo o puede constituir una unidad independiente. También se puede concebir que la unidad de control sea una función parcial de la unidad de control de ascensor de la instalación de ascensor,

es decir, que la unidad de control esté integrada en la unidad de control del ascensor.

La o las unidades de vídeo graban al menos una imagen de unazona de vigilancia definida del dispositivo de control de acceso. La zona de vigilancia puede ser, por ejemplo, una compuerta del lugar de paso. El vestíbulo del dispositivo de control de acceso también podría definirse como zona de vigilancia. La zona de vigilancia también se puede definir en forma de un área de vigilancia virtual de un edificio.

Como al menos una unidad de vídeo se puede utilizar cualquier unidad de vídeo analógico o digital, y ésta puede ser, por ejemplo, una cámara de vigilancia comercial, una cámara de vídeo, etc. La o las unidades de vídeo presentan al menos una unidad de grabación de imágenes y una unidad de procesamiento de imágenes o una unidad de control (integrada) para el procesamiento al menos parcial de las imágenes. La o las unidades de vídeo también pueden estar conectadas con la unidad de control (externa) a través de la red de comunicación. Como unidad de control se puede utilizar un procesador, un ordenador, un ordenador o servidor comercial con componentes comerciales y, por ejemplo, con una unidad de memoria. El procesamiento de imágenes se lleva a cabo en la unidad de control, integrada o externa. Para ello se utilizan algoritmos y procedimientos adecuados. De acuerdo con la invención, es posible realizar todo el procesamiento de imágenes en la o las unidades de vídeo o en la unidad de control (externa) conectada a través de la red de comunicación. No obstante, también se puede concebir un procesamiento de imágenes sólo parcial en la unidad de control integrada y un procesamiento de imágenes definitivo en la unidad de control (externa) conectada a través de la red de comunicación.

Una parte invariable de la o las imágenes se filtra. Se puede tratar por ejemplo del fondo, de un objeto que no se mueve, etc. En general, se filtran aquellas partes de las imágenes que no tienen ninguna relevancia para la evaluación. Quedan aquellas partes de las imágenes que son interesantes para detectar un objeto no autorizado en la zona de vigilancia. La parte invariable de la o de las imágenes se puede filtrar por ejemplo de modo que la o las unidades de vídeo comparan la o las imágenes actuales con al menos una imagen previamente grabada. Para ello, se puede utilizar por ejemplo al menos una imagen adecuada, es decir, una imagen de referencia almacenada en una unidad de memoria conectada a la unidad de control a través de la red de comunicación. Evidentemente, la unidad de memoria también puede estar integrada en la unidad de control.

La o las unidades de vídeo evalúan la o las partes de imagen restantes. En este contexto comprueba si en la zona de vigilancia se encuentra un objeto o un objeto de interés. Si en la zona de vigilancia se encuentra un objeto, la o las unidades de vídeo transmiten datos a la unidad de control. Para ello, la o las unidades de vídeo transmiten a la unidad de controlcomo datos por ejemplo el resultado de la evaluación, el resultado de la evaluación con la parte de imagen restante o únicamente la parte restante de una imagen. Por tanto, la o las unidades de vídeo pueden enviar acumulativa o alternativamente la parte restante de la o las imágenes con el resultado de evaluación a la unidad de control.

En función de los datos transmitidos, la unidad de control compruebala autorización del objeto que se encuentra en la zona de vigilancia y determina la dirección de movimiento o el lugar de permanencia del objeto dentro de la zona de vigilancia. Mediante la detección de la dirección de movimiento o del lugar de permanencia del objeto se puede determinar si el objeto intenta llegar a una zona de un edificio asegurada por el dispositivo de control de acceso o si el objeto por ejemplo simplemente permanece delante del dispositivo de control de acceso. Si el objeto no dispone de autorización para la zona asegurada o si se deniega la autorización, a través de una unidad de señalización se puede emitir una señal de aviso o una alarma, por ejemplo una señal óptica, una señal acústica o una combinación de éstas, o al menos se puede enviar un mensaje a una central de seguridad.

El dispositivo de control de acceso puede presentar al menos dos unidades de vídeo. Al menos una primera unidad de vídeo se puede encontrar en el campo visual de al menos una segunda unidad de vídeo. De este modo se pueden evitar intentos de manipulación, por ejemplo por cubrir la unidad de vídeo. De forma ideal, la o las primeras unidades de vídeo y la o las segundas unidades de vídeo están situadas una frente a otra. Las unidades de vídeo en una compuerta o en el dispositivo de control de acceso pueden estar dispuestas paralelas o perpendiculares con respecto a la dirección de paso. La o las primeras cámaras de vídeo y la o las segundas cámaras de vídeo pueden vigilar la zona de vigilancia desde diferentes ángulos de visión. La o las primeras cámaras de vídeo pueden estar conectadas a la o las segundas cámaras de vídeo a través de la red de comunicaciones, directa o indirectamente a través de la unidad de control.

La unidad de control puede comprobar la autorización por medio de al menos una señal de detección o un dato o señal de autorización y autentificación transmitidos

por una unidad de autorización y autentificación, o de acuerdo con al menos una regla. En este contexto, como unidad de autorización y autentificación se puede utilizar cualquier unidad para registrar o leer la o las señales de detección, por ejemplo datos biométricos, un código consistente en números, letras, caracteres especiales o una combinación de éstos, una señal de detección o dato de autentificación o dato de identificación almacenado en una unidad RFID, una imagen, etc. Por ejemplo, la o las unidades de vídeo según la invención podrían emplearse para el reconocimiento facial o para el registro de datos biométricos y, en consecuencia, para la autorización y autentificación.

Una ventaja de la invención es que permite detectar un objeto no autorizado en unazona de vigilancia de un dispositivo de control de acceso de forma sencilla y con una buena relación coste-eficacia.

La invención se explica más detalladamente por medio de un ejemplo de realización mostrado en las figuras. En las figuras:

Fig. 1: representación esquemática de una zona asegurada con un dispositivo de control de acceso;
Fig. 2: un fragmento detallado del dispositivo de control de acceso de la Fig. 1;
Fig. 3: un fragmento detallado de un dispositivo de control de acceso con direcciones de movimiento posibles de un objeto;
Fig. 4: representación esquemática de un dispositivo de control de acceso con dos unidades de vídeo;
Fig. 5: otra representación esquemática de un dispositivo de control de acceso con dos unidades de vídeo; y
Fig. 6: un ejemplo esquemático de procesamiento de imágenes con dos unidades de vídeo.

La Figura 1 muestra una representación esquemática de una zona asegurada AZVR con un dispositivo de control de acceso S, por ejemplo un vestíbulo de ascensores como acceso a los ascensores AZ individuales y a una puerta T de un edificio. La zona asegurada AZVR está separada de la zona públicamente accesible OEB por el dispositivo de control de acceso S. El dispositivo de control de acceso S presenta límites SW, por ejemplo columnas, paredes de compuerta, marcas en el suelo del edificio, etc. En este ejemplo, el dispositivo de control de acceso S presenta varios pasos. No obstante, el dispositivo de control de acceso S también puede presentar un único paso. El dispositivo de control de acceso S

presenta además al menos una unidad de vídeo K o una cámara de vídeo, que vigila al menos unazona de vigilancia definida UER del dispositivo de control de acceso S. Con este fin, la o las unidades de vídeo K están dispuestas frente al dispositivo de control de acceso S. La o las unidades de vídeo K también se pueden disponer en los límites SW. Así, la o las unidades de vídeo K podrían vigilar unazona de vigilancia definida entre los límites SW.

La o las unidades de vídeo también se pueden disponer de forma no permanente, sino en función de las necesidades en el dispositivo de control de acceso o junto al mismo. Por ejemplo, en el dispositivo de control de acceso S o en los límites SW puede estar previsto al menos un dispositivo y/o al menos una interfaz correspondiente para la conexión con la red de comunicación y/o el montaje/desmontaje de la unidad de vídeo.

La Figura 2 muestra un fragmento detallado del dispositivo de control de acceso S de la Figura 1. El dispositivo de control de acceso S separa la zona públicamente accesible OEB de un edificio de una zona asegurada AZVR o una zona que no es accesible al público. Para separa las zonas OEB y AZVR se utilizan límites SW del dispositivo de control de acceso S. Entre los dos límites SW se define la zona de vigilancia UER, que está vigilada por una unidad de vídeo K, no mostrada en esta figura.

La Figura 3 muestra un fragmento detallado del dispositivo de control de acceso S de las Figuras 1 y 2 con direcciones de movimiento posibles de un objeto. El rectángulo representado con líneas discontinuas entre los límites SW representa la zona de vigilancia UER. En este ejemplo, dos unidades de vídeo K1 y K2 están dispuestas de modo que pueden detectar movimientos de objetos, por ejemplo personas, animales, etc., en la zona de vigilancia UER. Para ello, en este ejemplo, las unidades de vídeo K1 y K2 están integradas en los límites SW. En la figura están representadas las posibles direcciones de movimiento 1 a 4 de objetos que entran en la zona asegurada AZVR o que salen de la misma. En el caso de la dirección de movimiento 4 se puede tratar de un objeto que intenta llegar a la zona asegurada AZVR, pero al que se le ha advertido de que no dispone de autorización, por ejemplo mediante una señal de aviso desde al menos una unidad de señalización dispuesta en los límites SW. A continuación, dicho objeto sale de nuevo de la zona asegurada AZVR.

La Figura 4 muestra una representación esquemática de un dispositivo de control de acceso S con, por ejemplo, dos unidades de vídeo K1 y K2. Un objeto O se

encuentra entre los límites SW del dispositivo de control de acceso S. Las dos unidades de vídeo K1 y K2 vigilan el espacio intermedio, la zona de vigilancia definida UER, entre los dos límites SW. En este ejemplo, la primera unidad de vídeo K1 está situada en el campo visual de la segunda unidad de vídeo K2 y viceversa. De este modo se puede evitar, por ejemplo, que se manipule una unidad de vídeo K1 o K2. En cada uno de los límites SW está integrada una unidad de señalización SE, que puede emitir al menos una señal óptica y/o acústica, por ejemplo cuando un objeto O permanece en la zona de vigilancia UER y dicho objeto O no dispone de autorización para ello, es decir, cuando la unidad de control ST ha establecido una denegación de autorización o un resultado de comprobación negativo.

Las dos unidades de vídeo K1 y K2 están dispuestas una frente a la otra y están conectadas con una unidad de control ST a través de una red de comunicación. En este contexto, como red de comunicación se puede utilizar una red de comunicación de cualquier tipo. Por ejemplo, se podría utilizar una red de comunicación por cable, inalámbrica o por radio. Las dos unidades de vídeo K1 y K2 también pueden estar conectadas a través de la red de comunicación, ya sea directa o indirectamente a través de la unidad de control ST.

También se puede prever que las dos unidades de vídeo K1 y K2 vigilen la zona de vigilancia UER desde ángulos de visión diferentes. Para ello, en este ejemplo las dos unidades de vídeo K1 y K2 están dispuestas una frente a la otra. Esto tiene por ejemplo la ventaja de permitir determinar más exactamente la dirección de movimiento o el lugar de permanencia de un objeto O dentro delazona de vigilancia UER. Además de la dirección de movimiento o el lugar de permanencia del objeto O, una unidad de vídeo K, K1, K2 podría estar posicionada para autentificar o identificar por ejemplo el objeto O por reconocimiento facial o reconocimiento de características biométricas.

El dispositivo de control de acceso S puede presentar una unidad de autorización y autentificación KL. Esta unidad (KL) también puede emplearse para identificar un objeto O. La unidad de autorización y autentificación KL registra al menos una señal de detección, por ejemplo una señal biométrica, un dato de autentificación almacenado en una tarjeta RFID, datos para la identificación de un objeto, etc., y transmite la o las señales de detección al menos en un mensaje a la unidad de control ST. La o las unidades de autorización y autentificación KL pueden estar dispuestas en el límite SW del dispositivo de control de acceso S, como en este

ejemplo. No obstante, éstas (KL) también pueden estar situadas en otro lugar, o su función puede ser desempeñada por al menos una unidad de vídeo K, K1, K2. La unidad de control ST puede comprobar la autorización de un objeto O, por ejemploen base a una comparación con datos almacenados. Evidentemente, la evaluación de la señal de detección o de identificación también podría tener lugar en la unidad de autorización y autentificación KL. La autorización también se puede establecer en función de al menos una regla. Por ejemplo, una regla podría indicar que los objetos O que abandonan la zona asegurada AZVR obtengan una liberación de autorización. Otra regla podría indicar que a determinadas horas siempre tenga lugar una liberación de autorización. Otra regla podría indicar que, si no hay ningún mensaje de la unidad de autorización y autentificación KL, la unidad de control ST de por supuesta una denegación de autorización y emita un resultado de comprobación negativo.

Si un objeto O permanece dentro delazona de vigilancia definida UER, las dos unidades de vídeo detectan la presencia del objeto O y transmiten los datos o señales correspondientes a la unidad de control ST y, si la unidad de control ST deniega la autorización para el objeto O, una unidad de señalización SE conectada con la unidad de control ST puede emitir un mensaje de aviso. Este mensaje de aviso puede consistir en señales ópticas y/o acústicas. No obstante, en caso de una denegación de autorización o de falta de autorización, la unidad de control ST también puede enviar al menos un mensaje a una central de seguridad SZ conectada a través de la red de comunicación. La central de seguridad SZ puede ser por ejemplo una unidad de una central de seguridad fuera o dentro del edificio. Con el o los mensajes recibidos en la central de seguridad SZ se pueden tomar después medidas correspondientes, por ejemplo el envío de un vigilante de seguridad al dispositivo de control de acceso S, la grabación de otra imagen del objeto O con al menos una de las unidades de vídeo K, K1, K2, etc.

La Figura 5 muestra otra representación esquemática de un dispositivo de control de acceso S con dos unidades de vídeo K1, K2. El dispositivo de control de acceso S está construido tal como se describe en la Figura 4. La o las unidades de autorización y autentificación KL y la o las unidades de señalización SE se han omitido para una mayor claridad. La diferencia con la Figura 4 es que las dos unidades de vídeo K1 y K2 están dispuestas de un modo distinto al de la Figura 4. En principio, la disposición de las dos unidades de vídeo K1 y K2 se puede elegir a voluntad. Únicamente se ha de asegurar que la zona de vigilancia UER pueda

ser vigilada por las unidades de vídeo K1 y K2. Esto es igualmente aplicable cuando solo se utiliza una unidad de vídeo K, K1, K2.

La Figura 6 muestra un ejemplo esquemático de un procesamiento de imágenes con dos unidades de vídeo K1 y K2. El ejemplo de procedimiento de procesamiento de imágenes también se puede utilizar análogamente en dispositivos de control de acceso S con una sola unidad de vídeo K, K1, K2 o con más de dos unidades de vídeo K, K1, K2.

Cada una de las dos unidades de vídeo K1 y K2 graba a intervalos de tiempo N, N-1, N2 o también de forma continua en este ejemplo en cada caso una imagen BN, BN-1, BN2. Evidentemente también es concebible que las dos unidades de vídeo K1 y K2 solo graben una imagen BN en cada caso.

Cada una de las dos unidades de vídeo K1 y K2 filtra de una parte invariable de las imágenes BN, BN-1, BN2. Esta parte de imagen invariable puede ser, por ejemplo, el fondo de la imagen.

La parte de imagen restante BGN, BGN-1, BGN-2 de las respectivas imágenes BN, BN-1, BN2 se evalúa para comprobar si hay un objeto O en la zona de vigilancia UER. Un objeto O pasa por el dispositivo de control de acceso S con los límites SW y las unidades de vídeo K1 y K2, tal como está descrito (S) en las Figuras 1 a 5. Preferentemente, si el objeto O se encuentra dentro de la zona de vigilancia UER, se transmiten datos a la unidad de control ST. Estos datos pueden ser, por ejemplo, el resultado de la evaluación, o el resultado de la evaluación y las partes de imagen restantes BGN, BGN-1, BGN-2 de las imágenes BN, BN-1, BN2, o solo las partes de imagen restantes BGN, BGN-1, BGN-2 de las imágenes BN, BN-1, BN2, o las imágenes BN, BN-1, BN2, etc. Evidentemente también es concebible que la imagen completa BN, BN-1, BN2 sea transmitida a la unidad de control ST y que allí tenga lugar toda la evaluación, es decir, que la unidad de control ST filtre la parte invariable de la imagen y que la unidad de control ST también lleve a cabo la detección de un objeto O en la zona de vigilancia UER.

Idealmente, como ya se ha mencionado más arriba, la transmisión de los datos, es decir, del resultado de la evaluación y/o de la parte de imagen restante BGN, BGN-1, BGN-2 sólo tiene lugar cuando realmente se ha detectado un objeto O en la zona de vigilancia UER. En caso de un resultado de evaluación negativo, es decir, cuando no hay ningún objeto O en la zona de vigilancia UER, no podría tener lugar ninguna transmisión. Evidentemente también es concebible que las

partes de imagen BGN, BGN-1, BGN-2 o las imágenes completas BN, BN-1, BN2 sean transmitidas a la unidad de control ST independientemente del resultado de la evaluación.

La unidad de control ST comprueba, en función de los datos transmitidos de las dos unidades de vídeo K1, K2, la autorización del objeto O que se encuentra en la zona de vigilancia UER. Por consiguiente, se comprueba si hay un objeto O en la zona de vigilancia UER y, en caso afirmativo, la unidad de control ST comprueba la autorización del objeto O en cuestión. La comprobación de la autorización se lleva a cabo por medio de datos de una unidad de autorización y autentificación KL o de acuerdo con al menos una regla, tal como se describe en las anteriores Figuras 1 a 5. Como regla o reglas se podría utilizar por ejemplo la dirección de movimiento o la hora. Por ejemplo, podría estar regulado que cuando un objeto O sale de la zona asegurada AZVR no es necesaria ninguna autorización. También podría no requerirse ninguna autorización a determinadas horas.

Además, en función de los resultados de evaluación y/o de las respectivas partes de imagen restantes BGN, BGN-1, BGN-2 de las dos unidades de vídeo K1 y K2, también se determina la dirección de movimiento 1, 2, 3, 4 o el lugar de permanencia del objeto O dentro dela zona de vigilancia UER, por ejemplo el objeto O podría estar quieto en la zona de vigilancia UER. Para ello, por ejemplo, la unidad de control ST combina y/o compara las partes de imagen restantes BGN, BGN-1, BGN-2 transmitidas, y/o la determinación de la dirección de movimiento o del lugar de permanencia del objeto O tiene lugar por medio de las partes de imagen restantes de una unidad de vídeo K1 o K2. Para determinar la dirección de movimiento o el lugar de permanencia también se podría recurrir al resultado de evaluación. En este ejemplo, las partes de imagen restantes BGN, BGN-1, BGN-2 de las dos unidades de vídeo K1 y K2 se combinan entre sí, con lo que se forman partes de imagen restantes combinadas CN, CN-1, CN-2. La unidad de control ST puede comprobar la autorización y determinar la dirección de movimiento o el lugar de permanencia del objeto O en función de las partes de imagen restantes combinadas CN, CN-1, CN-2.

Utilizando la dirección de movimiento o el lugar de permanencia determinados y la falta de una autorización del objeto O o la emisión de una denegación de autorización por parte de la unidad de control T, la unidad de control ST podría enviar al menos un mensaje a una central de seguridad SZ, que entonces podría tomar medidas adecuadas, por ejemploenviar un vigilante de seguridad, grabar

una imagen, bloquear el ascensor AZ, cerrar o bloquear la puerta T, etc. Además, una unidad de señalización SE podría emitir un mensaje de aviso, al menos una señal óptica y/o acústica. Como unidad de señalización SE se podría utilizar una unidad que emite luz y/o un sonido o secuencias de sonidos. Las señales ópticas también podrían ser pictogramas, imágenes, etc. La unidad de señalización SE puede estar integrada en el límite SW o constituir una unidad independiente. Por ejemplo, en la Figura 4 está representada una variante de posicionamiento posible.

Reivindicaciones

1. Dispositivo de control de acceso (S) de una instalación de ascensor con al menos una unidad de vídeo (K, K1, K2), estando conectadas la o las unidades de vídeo (K, K1, K2) con una unidad de control (ST) a través de una red de comunicación, donde la o las unidades de vídeo (K, K1, K2) graban al menos una imagen de unazona de vigilancia definida (UER) del dispositivo de control de acceso (S), donde la o las unidades de vídeo (K, K1, K2) filtran una parte invariable de la o las imágenes (BN, BN-1, BN2), donde la o las unidades de vídeo (K, K1, K2) evalúan la parte de imagen restante (BGN, BGN-1, BGN-2) para comprobar si hay un objeto (O) en la zona de vigilancia (UER) y, si hay un objeto (O) en la zona de vigilancia (UER), la o las unidades de vídeo (K) transmiten datos a la unidad de control (ST), y donde la unidad de control (ST), en función de los datos transmitidos, comprueba la autorización del objeto que se encuentra en la zona de vigilancia (UER) y determina la dirección de movimiento o el lugar de permanencia del objeto (O) dentro delazona de vigilancia (UER),

caracterizadoporque al menos una primera unidad de vídeo (K1) y al menos una segunda unidad de vídeo (K2) están dispuestas una frente a la otra, y la o las primeras unidades de vídeo (K1) se encuentran en el campo visual de la o las segundas unidades de vídeo (K2), y viceversa.

2. Dispositivo de control de acceso (S) según la reivindicación 1,caracterizadoporque la o las primeras unidades de vídeo (K1) están conectadas a la o las segundas unidades de vídeo (K2) a través de la red de comunicación.

3. Dispositivo de control de acceso (S) según una de las reivindicaciones 1 a 2,caracterizadoporque la o las primeras unidades de vídeo (K1) y la o las segundas unidades de vídeo (K2) vigilan la zona de vigilancia (UER) desde diferentes ángulos de visión.

4. Dispositivo de control de acceso (S) según una de las reivindicaciones anteriores,caracterizadoporque la unidad de control (ST) comprueba la autorización por medio de al menos una señal de autorización y detección transmitida por una unidad de autorización y autentificación (KL), o de acuerdo con al menos una regla.

5. Dispositivo de control de acceso (S) según la reivindicación 4,caracterizadoporque como regla o reglas están previstas la dirección de movimiento al entrar en la zona de vigilancia (UER) y/o la hora.

6. Dispositivo de control de acceso (S) según las reivindicaciones 4 o 5,caracterizadoporque como señal o señales de detección están previstos un código, una señal biométrica y/o una señal de detección almacenada en una tarjeta RFID.

7. Dispositivo de control de acceso (S) según la reivindicación 1,caracterizadoporque, en caso de una denegación de autorización o una falta de autorización, una unidad de señalización (SE) conectada con la unidad de control (ST) emite al menos una señal de aviso.

8. Dispositivo de control de acceso (S) según la reivindicación 7,caracterizadoporque como señal de aviso está prevista una señal óptica y/o acústica.

9. Dispositivo de control de acceso (S) según la reivindicación 1,caracterizadoporque, en caso de una denegación de autorización o una falta de autorización, la unidad de control (ST) envía al menos un mensaje a una unidad de seguridad conectada a través de la red de comunicación.

10. Dispositivo de control de acceso (S) según una de las reivindicaciones anteriores,caracterizadoporque la o las unidades de vídeo (K, K1, K2) filtran la parte invariable de la o las imágenes de modo que la o las unidades de vídeo (K, K1, K2) comparan la imagen actual con al menos una imagen grabada previamente.

11. Dispositivo de control de acceso (S) según una de las reivindicaciones anteriores,caracterizadoporque la o las unidades de vídeo (K, K1, K2) transmiten como datos a la unidad de control (ST) el resultado de la evaluación o el resultado de la evaluación con la parte de imagen restante (BGN, BGN-1, BGN-2) de la o las imágenes (BN, BN-1, BN2), o la parte de imagen restante (BGN, BGN-1, BGN-2) de la o las imágenes (BN, BN-1, BN2).

12. Procedimiento para la detección de un objeto (O) en unazona de vigilancia (UER) de un dispositivo de control de acceso (S) de una instalación de ascensor vigilada por al menos una unidad de vídeo (K, K1, K2), donde la o

las unidades de vídeo (K, K1, K2) están conectadas con una unidad de control (ST) a través de una red de comunicación, donde la o las unidades de vídeo (K, K1, K2) graban una imagen de unazona de vigilancia definida (UER) del dispositivo de control de acceso (S) y filtran una parte invariable de la o las imágenes (BN, BN-1, BN-2), donde la o las unidades de vídeo (K, K1, K2) evalúan la parte de imagen restante (BGN, BGN-1, BGN-2) para comprobar si hay un objeto (O) en la zona de vigilancia (UER), donde, si hay un objeto (O) en la zona de vigilancia (UER), la o las unidades de vídeo (K, K1, K2) transmiten datos a la unidad de control (ST) y la unidad de control (ST), en función de los datos transmitidos, comprueba la autorización del objeto (O) que se encuentra en la zona de vigilancia (UER) y determina la dirección de movimiento o el lugar de permanencia del objeto (O) dentro delazona de vigilancia (UER),

caracterizadoporque se disponen al menos una primera unidad de vídeo (K1) y al menos una segunda unidad de vídeo (K2) una frente a la otra, y la o las primeras unidades de vídeo (K1) se encuentran en el campo visual de la o las segundas unidades de vídeo (K2), y viceversa.

Fig. 1

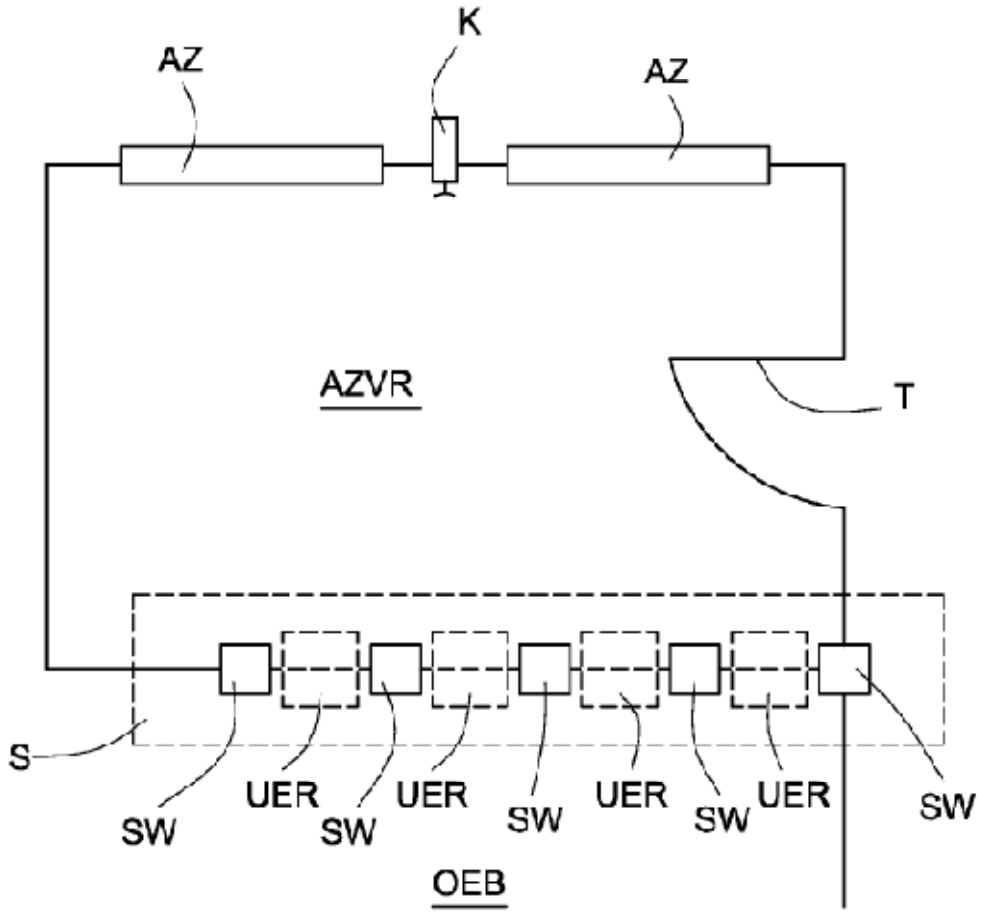

K
AZ
AZ
AZVR
T
S
SW
UER
SW
UER
SW
UER
SW
UER
SW
OEB

Fig. 2

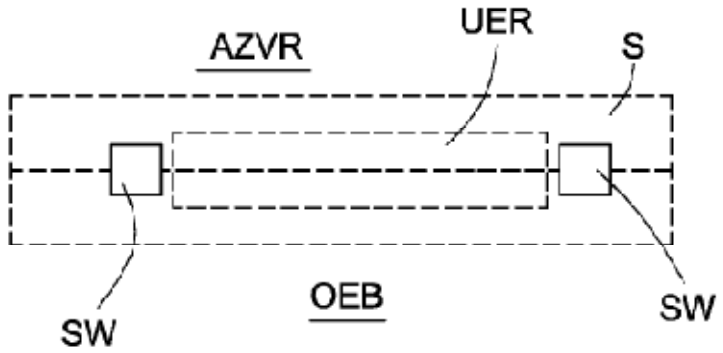

AZVR
UER
S
SW
OEB
SW

Fig. 3

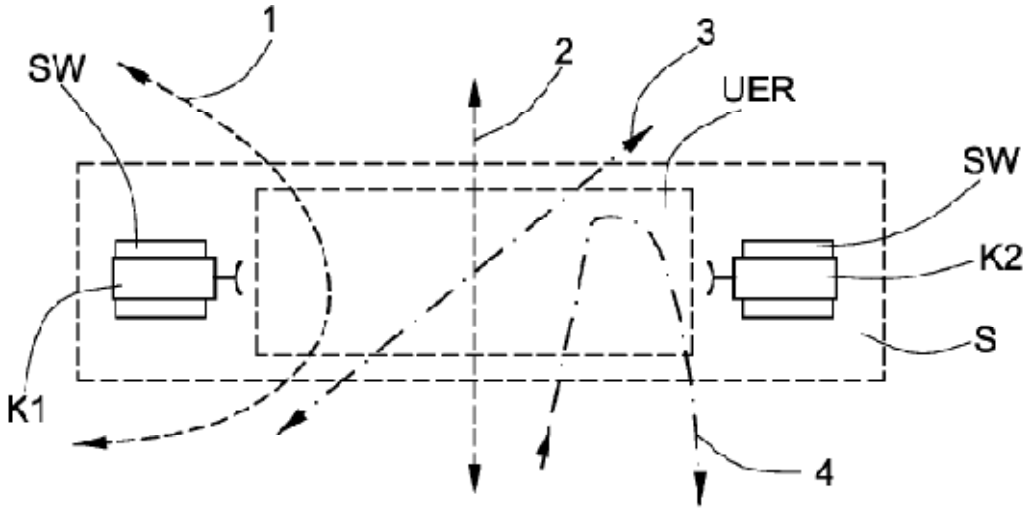


Fig. 4

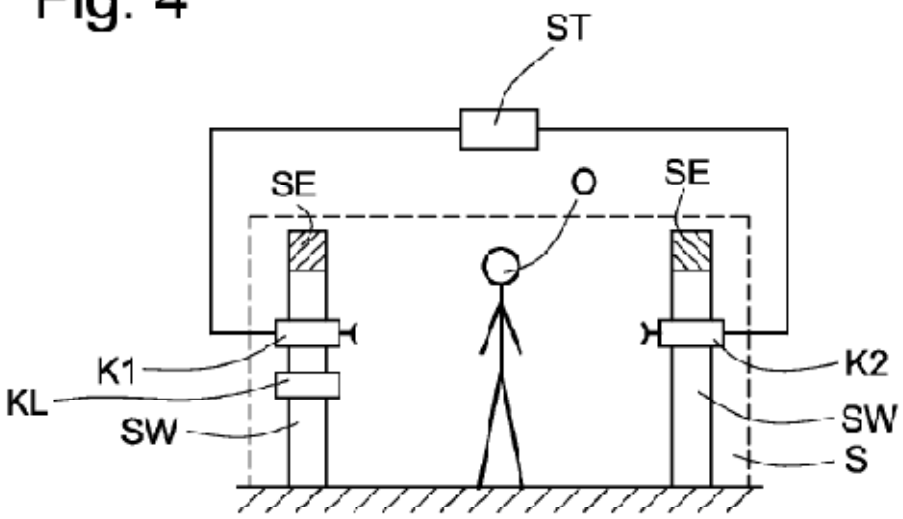


Fig. 5

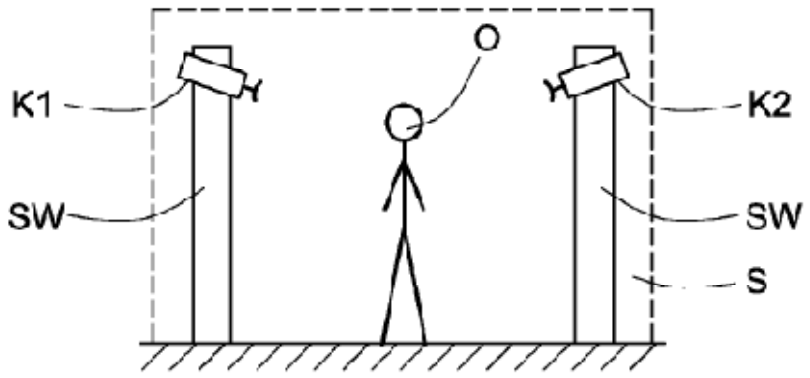
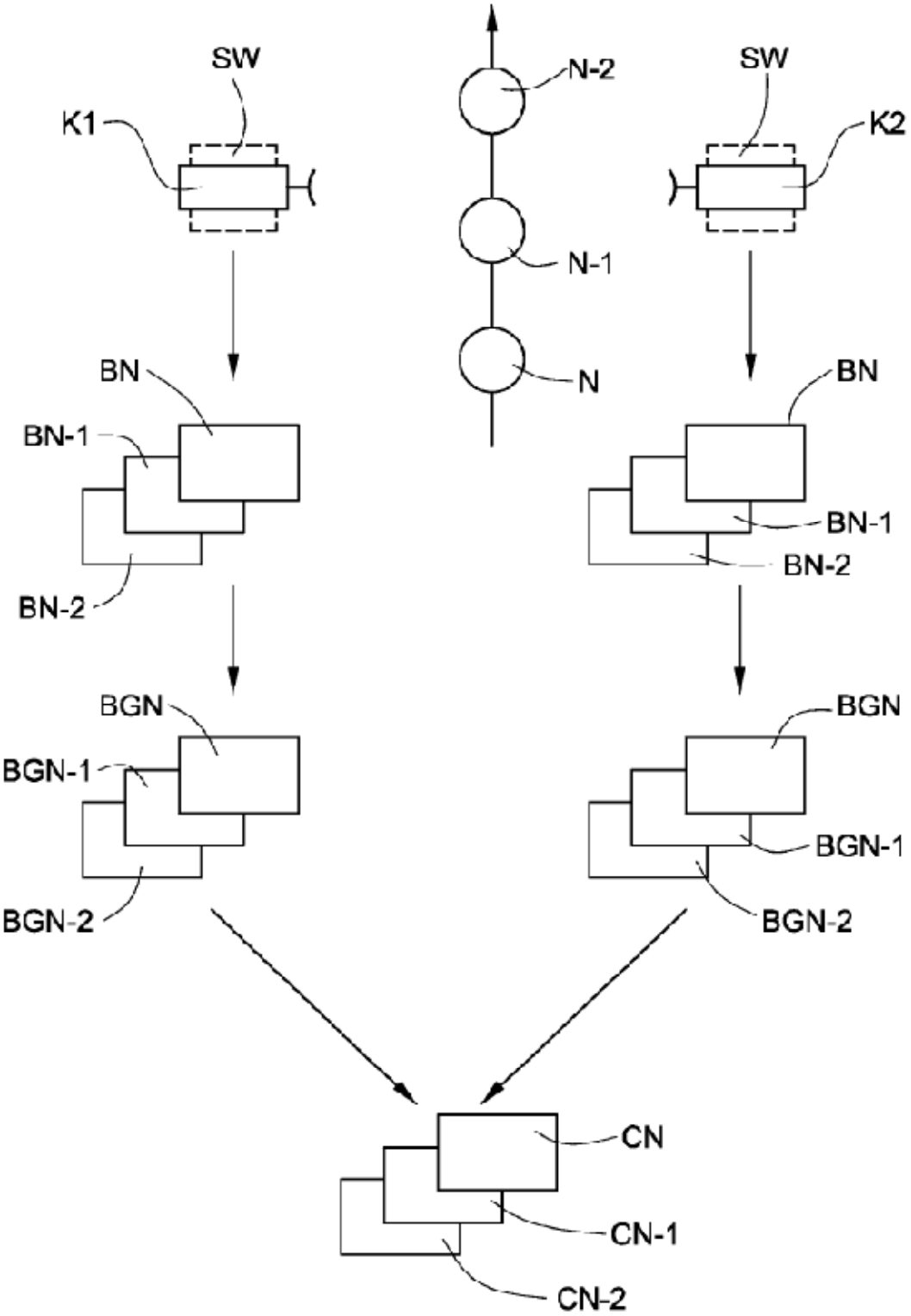


Fig. 6


SW
K1
N-2
N-1
N
SW
K2
BN
BN-1
BN-2
BN
BN-1
BN-2
BGN
BGN-1
BGN-2
BGN
BGN-1
BGN-2
CN
CN-1
CN-2