(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 406 982**

(51) Int. CI.:

G07C 9/00 (2006.01)
G07C 9/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.01.2009 E 09704074 (5)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2013 EP 2238577**

(54) Título: **Dispositivo de control de acceso**

(30) Prioridad:

24.01.2008 DE 102008005770
31.03.2008 DE 102008016516

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.06.2013

(73) Titular/es:

KABA GALLENSCHÜTZ GMBH (100.0%)
NIKOLAUS-OTTO-STRASSE 1
77815 BÜHL, DE

(72) Inventor/es:

SCHORN, JOSEF

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Dispositivo de control de acceso

La invención se refiere a un dispositivo de control de acceso con al menos un elemento de control de acceso que desbloquea o bloquea el acceso a una zona protegida, un edificio o un recinto, en particular con un molinete, un torniquete, una puerta de batientes, cámara o barrera de bloqueo, así como al menos un dispositivo de lectura para la comprobación al menos de una característica de legitimación que documenta la autorización de acceso y/o al menos un detector, en particular una barrera de luz, para la comprobación al menos de una característica de seguridad, por ejemplo el número de personas que pasan, estando unidos al menos indirectamente los elementos de bloqueo y el dispositivo de lectura y/o los detectores respectivamente con al menos una unidad de ordenador del dispositivo de control de acceso, presentando esta unidad de ordenador un elemento de memoria en el que están archivadas las características de seguridad y las características de legitimación permitidas y realizándose por medio de la unidad de procesamiento una comparación de las características de legitimación leídas con las características de legitimación almacenadas y/o una comprobación de las características de seguridad detectadas por los detectores con las características de seguridad permitidas y dependiendo del resultado de esta comparación puede desbloquearse, preferentemente de manera automática, el elemento de acceso.

Un dispositivo de control de acceso de este tipo se conoce por el documento WO 03/088157 A. Como tecnología de detectores se usan en este dispositivo conocido en particular varias cámaras que están dispuestas de modo que se registran imágenes tridimensionales y se facilitan para la evaluación posterior. Dependiendo del resultado de esta evaluación se desbloquean o no los elementos de bloqueo de acceso. La instalación se configura, se inicializa, se calibra y se somete a prueba por un operario a través de una correspondiente interfaz. La puesta en marcha de esta instalación y posibles ajustes posteriores deben realizarse así por personal especializado correspondiente.

Así se conoce anteriormente, por ejemplo por el documento DE 10 2004 048 403 A1, un dispositivo de control de acceso, en particular para la zona de máxima seguridad y de aeropuertos, en el que a una zona de esclusa definida por una entrada y salida controlada están asignados uno o varios dispositivos de control y dispositivos de comprobación de la identificación, tal como por ejemplo un lector de documentos, una unidad biométrica para la detección de características biométricas, una cámara y/o barreras de luz para el control de diversas características de prueba por ejemplo del control de personas, del aislamiento de personas o identificación de personas o de la autorización de acceso. Todos estos dispositivos de control están conectados entre sí a través de un dispositivo de control central por ejemplo para el ajuste de los resultados de prueba.

De manera complementaria se conoce por el documento US 2006/0080541 A1 un sistema y un procedimiento para la regulación automática o manual de niveles de control de acceso a base de niveles de seguridad preajustados. En el contexto de la elección de los niveles de seguridad definidos puede adaptarse el nivel de control de acceso a la situación actual, por ejemplo día laborable o día festivo, del mismo modo que en la situación local, por ejemplo edificios privados o de empresas. Concretamente, en el contexto del procedimiento de acuerdo con la invención, existe la posibilidad de parametrizar una matriz de seguridad que define los parámetros de acceso y seguridad y de adaptar los parámetros en caso necesario a una situación de seguridad modificada.

Los dispositivos de control de acceso de este tipo sirven para el desbloqueo controlado de un acceso y al mismo tiempo para el aislamiento de personas que quieren acceder a una zona protegida, un edificio o un recinto. A este respecto se entiende que en el contexto de la automatización se deseé cada vez más que se realice en gran parte automáticamente la comprobación de las características de legitimación y/o características de seguridad, o sea que se comparen los datos detectados o leídos con datos almacenados y dependiendo de estos datos se realice o no el desbloqueo del acceso.

A este respecto, las unidades de ordenador cada vez más rápidas así como los elementos de memoria cada vez más económicos y más grandes han facilitado la comprobación de características progresivamente más complejas en relación con el desbloqueo de un acceso. Así, en los últimos años ha sido posible detectar características biométricas, tales como por ejemplo una huella digital, una imagen de una persona o una imagen de iris, y comprobar así con datos almacenados si la persona que solicita el acceso se autoriza realmente. La comprobación de las características biométricas se complementa a este respecto por otras comprobaciones, tales como por ejemplo una comprobación de existencia con respecto a huellas digitales tomadas o una vigilancia por cámara de una habitación cerrada en el sentido de que respectivamente sólo una persona pase el acceso, y otras posibles características de seguridad.

A este respecto es posible accionar los elementos de bloqueo de acceso con frecuencia iguales, o sea por ejemplo puertas giratorias, molinetes, puertas de batientes u otros elementos de bloqueo, con distintos detectores y dispositivos de lectura dependiendo del patrón de seguridad. Cuantas más características se comprueben de manera aditiva, tanto más alto será el patrón de seguridad. A este respecto, las instalaciones para la adaptación posterior a patrones de seguridad aumentados se dotan con frecuencia de detectores y dispositivos de lectura que en el momento de la entrega no se usan inmediatamente.

A este respecto, una adaptación a los patrones de seguridad es con frecuencia imprescindible en el funcionamiento. Esto resulta por un lado del requerimiento de que puede modificarse el patrón de seguridad de edificios durante su uso, por ejemplo en el contexto de un uso modificado. Así es concebible, por ejemplo, que un mero edificio de oficinas originariamente se use progresivamente para fines de investigación y por tanto deba aumentar el patrón de seguridad. Es concebible también que en edificios usados hasta el momento de manera no preocupante en un momento posterior se depositen artículos de alta calidad, otros objetos de valor monetario o incluso dinero, de modo que debe aumentar por tanto el patrón de seguridad. Es concebible también que se modifique por circunstancias externas la situación de riesgo, por ejemplo porque una serie de robos en el entorno exige un aumento del patrón de seguridad.

Finalmente existe también el uso contrario, concretamente que se desee una reducción del patrón de seguridad, por ejemplo por el usuario, ya que se comprueba que el patrón de seguridad deseado originariamente en el funcionamiento real conduce a tiempos de paso indeseablemente largos de las personas afectadas o la cuota de errores se vuelve demasiado alta.

A pesar de toda la precisión de las instalaciones de este tipo no puede evitarse que, por ejemplo en el contexto de la comprobación de que respectivamente sólo una persona pase una esclusa, por ejemplo con bultos acarreados, más grandes, estén interrumpidas varias barreras de luz, de modo que la instalación sospeche de que no sólo quiere pasar una persona la barrera sino dos personas. Así puede comprobarse rápidamente por ejemplo en un edificio de oficinas que cada persona que lleve consigo un portafolios conduzca a una alarma en la instalación con la consecuencia de que una persona del personal de seguridad realice una comprobación y eventualmente deba desbloquear manualmente la instalación. Con frecuencia puede resultar práctico entonces desconectar este control o una barrera de luz individual. Sin embargo puede existir entonces el deseo de conectar, en lugar de la comprobación anterior con dos barreras de luz, otra comprobación por ejemplo por medio de una cámara y de una evaluación de imágenes.

En el funcionamiento práctico se ha demostrado que habitualmente los usuarios en la puesta en funcionamiento de un dispositivo de control de acceso que funciona automáticamente exigen respectivamente en primer lugar el patrón de seguridad máximo posible y de manera correspondiente a esto se realiza una parametrización de la instalación. A lo largo del funcionamiento posterior resulta entonces con frecuencia que este patrón de seguridad sólo difícilmente se concilia con los requerimientos del funcionamiento cotidiano, de modo que se realiza entonces detalladamente parametrizaciones posteriores, hasta que finalmente se encuentre un ajuste en el proceso de “ensayo y error” que ofrezca por un lado un patrón de seguridad óptimo y permita por otro lado un funcionamiento medianamente ininterrumpido, o sea un acceso ininterrumpido y eventualmente también una salida de una zona protegida.

El reequipamiento costoso de las instalaciones con respectiva interrupción del funcionamiento se considera desagradable por todos los participantes y es adecuado además para reducir drásticamente la aceptación de un dispositivo de control de acceso de este tipo. Esto conduce con frecuencia a que los patrones de seguridad pretendidos originariamente en beneficio de un funcionamiento ininterrumpido se coloquen más bien bajos que lo que sería deseable en sí. La rápida aceptación y capacidad de funcionamiento de un dispositivo de control de acceso representa por tanto un requerimiento esencial en una instalación compleja de este tipo.

Partiendo de este estado de la técnica, la invención se basa en el objetivo de crear un dispositivo de control de acceso mejorado que ofrezca en particular un manejo simplificado en el dispositivo y en el funcionamiento de un dispositivo de control de acceso de este tipo.

La solución de este objetivo se consigue con un dispositivo de control de acceso de acuerdo con las características de la reivindicación independiente. Ciertas configuraciones ventajosas de la invención pueden deducirse de las reivindicaciones dependientes.

La solución del objetivo se consigue porque a la unidad de ordenador central para la evaluación y para la comparación de las características de legitimación leídas y de las características de seguridad detectadas está asignada una unidad de mando con la que pueden ajustarse etapas de seguridad predeterminadas. El ajuste de las etapas de seguridad representa la elección de parametrizaciones predeterminadas, ingeniosas de la unidad de ordenador central, o sea por ejemplo una elección de las características de seguridad y/o legitimación detectadas y el umbral de tolerancia asignado respectivamente a la comprobación que va a realizarse de las características. Las etapas de seguridad dispuestas en relación con el elemento de mando representan una elección de las etapas de seguridad convenientes para la respectiva situación de funcionamiento, pudiéndose conectar el elemento de mando con el dispositivo de ordenador dependiendo de la aplicación, estando dotado de distintas parametrizaciones predefinidas.

A diferencia de las parametrizaciones convencionales, las correspondientes instalaciones se ofrecen por tanto con distintas parametrizaciones ya predefinidas. A este respecto, sin embargo, la invención no se reduce a la elección de distintas parametrizaciones posibles del dispositivo de control de acceso, sino que ofrece adicionalmente la posibilidad de realizar por medio del elemento de mando adicional una posibilidad de regulación, sin nueva parametrización de la instalación o reequipamiento o parametrización detallados, simplemente con un elemento de mando y elemento de elección sencillo. A este respecto, un elemento de mando de este tipo puede manejarse por el

personal de seguridad habitual o un portero sin ningún tipo de conocimiento de la instalación como tal.

El elemento de mando adicional permite también ocuparse de manera sencilla directamente de proporciones modificadas, o sea por ejemplo bajar las características de seguridad provisionalmente en caso de una gran aglomeración de gente y a continuación proseguir el funcionamiento de nuevo con un aumento de etapa de seguridad.

Para ello está asignado a la unidad de mando un software de parametrización especial. Por medio de este software pueden parametrizarse directamente las etapas de seguridad seleccionables con el elemento de mando. Sin embargo, el software de parametrización permite también modificar en caso necesario la parametrización realizada una vez, o sea adaptar las etapas de seguridad seleccionadas en su configuración concreta al funcionamiento modificado. El uso del software de parametrización permite por tanto adaptar la unidad de mando a un funcionamiento modificado. La parametrización del software de parametrización queda reservada sin embargo habitualmente para el personal especializado.

En la configuración concreta, en caso del elemento de mando se trata de un interruptor giratorio sencillo con el puede seleccionarse entre distintas etapas de seguridad. A este respecto puede tratarse de un interruptor giratorio escalonado o continuo. En el caso de una realización con un interruptor giratorio continuo se modifican mediante la regulación continua igualmente las características no escalonadas, o sea por ejemplo umbrales de tolerancia o datos de parámetros continuos. Desde el punto de vista técnico puede realizarse un interruptor giratorio continuo de este tipo por ejemplo por medio de un reóstato. La parametrización continua de los dispositivos de control de acceso no es sólo una idea completamente nueva de la técnica de seguridad. Permite también una adaptación individual a las necesidades de seguridad del usuario, que no era posible hasta el momento. Y esto (igualmente por primera vez) sin ningún personal especializado.

A este respecto, al dispositivo de control de acceso en una realización preferente está asignada una red de detectores con varios detectores, de modo que el patrón de seguridad puede modificarse ya fácilmente mediante la conexión y desconexión de detectores individuales o grupos de detectores. También se realiza esto de manera comprensible y sencilla para el operario mediante regulación del elemento de mando central.

En una configuración ventajosa, en caso de la red de detectores puede tratarse al menos parcialmente de detectores ópticos que forman una esclusa óptica de manera perpendicular a la dirección de paso. A este respecto, los detectores ópticos están orientados de modo que sus ejes ópticos se entrecruzan formando rombos con el efecto de que se modifica el número de rombos y con ello la precisión de la vigilancia óptica mediante regulación del elemento de mando central.

En otra configuración de la invención ha dado buen resultado usar el dispositivo de control de acceso mejorado en relación con la comprobación de características biométricas como característica de legitimación. En particular, los requerimientos complejos en la comprobación de características biométricas requieren la posibilidad de un ajuste posterior de un dispositivo de control de acceso de este tipo usando una unidad de mando fácil de usar.

En un perfeccionamiento ventajoso, la unidad de ordenador central para la comprobación de las características de seguridad y/o legitimación puede estar integrada en una red de datos superior y por consiguiente puede realizarse con control remoto una comprobación del control de acceso, sin embargo también un ajuste posterior de la unidad de mando. La integración correspondiente de la unidad de ordenador, sin embargo también de la unidad de mando permite un mantenimiento o ajuste posterior, por ejemplo por parte del fabricante, sin que sea necesaria una correspondiente inspección local de la instalación.

La invención se explica en más detalle a continuación por medio de un ejemplo de realización representado en el dibujo. El ejemplo de realización sirve exclusivamente para la explicación en más detalle, siendo concebibles lógicamente una multiplicidad de otras configuraciones en el contexto de la invención.

Muestran:

la figura 1: una compuerta de acceso en representación en perspectiva con una unidad de ordenador asignada a esta compuerta de acceso y un elemento de mando asignado a esta unidad de ordenador,

la figura 2: un dispositivo de control de acceso con varios elementos de bloqueo de acceso, en representación en perspectiva y

la figura 3: otro dispositivo de control de acceso en una vista en planta como representación básica.

La figura 1 muestra un dispositivo de control de acceso 1, tratándose en el caso concreto de un paso en forma de esclusa con varios elementos de bloqueo de acceso, concretamente varias puertas oscilantes 2, 2' así como bloqueo oscilante doble 3 y eventualmente otros elementos de bloqueo de acceso no representados en este caso. En la dirección de paso está definida por la puerta oscilante delantera 2 una zona vigilada 4 por cámara, marcada por la representación de radiación, en la que se comprueba inicialmente de manera no interesante en este caso si se

queda sólo una persona en la zona cerrada. Adicionalmente, en la zona vigilada 4 puede realizarse, por medio de la cual para la comprobación del aislamiento, también una detección de características biométricas, o sea por ejemplo de la evaluación de la imagen de la cara.

Tanto las puertas oscilantes 2, 2 como también los bloqueos oscilantes dobles 3 están dotados respectivamente de un accionamiento electromotor, que están separados o están en conexión con datos de manera conjunta con una unidad de ordenador central 5. La unidad de ordenador central 5 se encuentra en contacto además con la o las cámara(s) 6 para la vigilancia de la zona vigilada 4.

Sólo cuando la cámara 6 señalice que en la zona vigilada 4 está dispuesta sólo una persona, se abre en una etapa adicional la puerta oscilante 2. Además pueden comprobarse por ejemplo los datos biométricos o por medio de un dispositivo de lectura no representado posteriormente otras características de seguridad y/o legitimación. Sólo cuando también éstas correspondan al menos en un grado predefinido a los datos almacenados o a los datos predeterminados, se abre entonces el bloqueo oscilante doble 3 y la puerta oscilante 2' posterior.

Todas las características detectadas o leídas se asignan a la unidad de ordenador central 5. La unidad de ordenador 5 está conectada además con un dispositivo de memoria 7 en el que están archivadas las características de legitimización por ejemplo permitidas. La unidad de ordenador 5 realiza entonces una comparación con las características almacenadas y tan sólo para el caso que éstas concuerden en una medida predeterminada, realiza el desbloqueo de los elementos de bloqueo de acceso individuales del dispositivo de control de acceso 1.

Adicionalmente, la unidad de ordenador central 5 está dotada de una unidad de mando 8, una denominada "*security wheel*". Según esto se trata de un interruptor giratorio que puede regularse de manera continua, con el que puede predeterminarse por el respectivo personal de vigilancia o de mando la etapa de seguridad deseada respetivamente. Mediante la regulación del elemento de mando 8 se regula por ejemplo el intervalo de tolerancia de la zona vigilada 4, o sea las dimensiones que se aceptan aún para concluir que en la zona vigilada 4 permanece realmente sólo una persona. Además, por medio de la regulación del elemento de mando 8 puede regularse simultáneamente qué desviaciones de los datos biométricos almacenados (foto de carnet) se aceptan aún en comparación con los datos detectados. Se entiende que con una eliminación del patrón de seguridad se reduce la complejidad del ordenador y con ello aumenta la velocidad de control de la instalación. Sin embargo, con la reducción creciente de los umbrales de tolerancia existe el riesgo de que por ejemplo también dos personas, aunque sólo una sea legitima, pasen la instalación. Es concebible también reducir el patrón de seguridad mediante la unidad de mando 8 en momentos de gran aglomeración sólo provisionalmente.

La *security wheel* ofrece a este respecto la posibilidad de adaptar el patrón de seguridad de manera continua a la situación de riesgo actual o de regularlo posteriormente por otros motivos en cualquier momento de manera óptima en el sentido más amplio de la palabra con una maniobra. Esta modificación es posible debido al elemento de mando (8) novedoso sin ningún personal especializado. El ajuste de seguridad del dispositivo de control de acceso puede crecer conjuntamente debido a esta solución por ejemplo con las exigencias del usuario, sin que para ello fuera necesario seleccionar más de un nuevo ajuste en el elemento de mando (8).

En otra realización de acuerdo con la figura 2 se parte de un recinto protegido más grade que está protegido con una multiplicidad de elementos de bloqueo de acceso distintos.

En el caso concreto, por ejemplo para la seguridad de un edificio se han usado dos segmentos circulares deslizables respectivamente combinados con una puerta de batientes, o sea una denominada puerta circular 10, 10', una esclusa de personal 11 protegida con una puerta de madera contrachapada así como dos esclusas de personal 12, 12' protegidas con hojas plegables (entrada y salida) así como un torniquete 13 convencional así como otro torniquete 13' y una barrera de bloqueo 14 para la seguridad de la zona que va a protegerse.

A este respecto, los elementos de bloqueo de acceso están reunidos en unidades funcionales, por ejemplo debido a que protegen una zona definida. Así, por ejemplo las dos puertas circulares 10, 10' con los segmentos circulares deslizables pueden proteger la entrada y salida de una unidad de edificio. También el torniquete 13 convencional con las dos hojas 12, 12' y la esclusa de personal 11 con estructura cúbica puede estar reunidos en una unidad para la seguridad de una zona común, por ejemplo de un recinto con un edificio que se encuentra en el mismo. Otra unidad comprende otro torniquete 13' convencional así como la barrera de bloqueo 14, tal como podrían usarse por ejemplo para la seguridad un parking.

El dispositivo de control de acceso 1 representa por tanto con su multiplicidad de elementos de bloqueo de acceso una protección habitual de un recinto de empresa.

Los elementos de bloqueo de acceso reunidos en unidades funcionales están conectados respectivamente con una interfaz 20 que recoge los datos detectados por los dispositivos de lectura y elementos detectores asignados a los respectivos dispositivos de bloqueo de acceso y eventualmente transmite señales a los accionamientos electromotores de las instalaciones. Todas las interfaces 20 de la instalación se encuentran en conexión de datos entre sí mediante una red de datos 15, por ejemplo la intranet o la internet.

Una interfaz 20 se encuentra en conexión de datos adicionalmente con un banco de datos que está colocado en un correspondiente elemento de memoria 7. Esta interfaz 20 está conectada adicionalmente con la unidad de ordenador central 5. Con la misma interfaz está conectado también el elemento de mando adicional 8 con intercalación de un software de parametrización 16 especial.

En consecuencia se realiza la comprobación de los datos indicados por los elementos de bloqueo de acceso individuales mediante una comparación con las características de legitimación y seguridad almacenadas en el banco de datos con la consideración de la etapa de seguridad predeterminada por el elemento de mando central 8. A este respecto puede realizarse un ajuste posterior de la instalación por medio del software de parametrización 16 en el sentido de que se modifique posteriormente la parametrización asignada a las etapas de seguridad individuales. Por parte de la fábrica se realiza un ajuste previo de la instalación por medio del software de parametrización 16.

El ejemplo de realización 2 muestra de manera especial cómo puede adaptarse el objetivo casi completamente insoslayable en sí para el personal de mando habitual de la parametrización de un dispositivo de control de acceso 1 completo para un recinto de empresa extenso mediante regulación sencilla de un elemento de mando 8 individual a la necesidad respectiva y eventualmente también a condiciones modificadas.

Para la explicación adicional está representado en la figura 3 otro dispositivo de control de acceso 1 que está constituido en este ejemplo únicamente por un paso en forma de esclusa 12 con las hojas 21, 21 que bloquean o desbloquean según la necesidad un paso controlado, estando limitado el paso en ambos lados mediante elementos indicadores 22, 22'. Por la extensión longitudinal de los elementos indicadores están dispuestos detectores ópticos 23 distanciados entre sí según la necesidad en uno o varios planos de control ópticos, cuyos ejes ópticos en la dirección de radiación están dispuestos transversalmente a la dirección de paso por el paso en forma de esclusa 12 y cuyas direcciones de radiación se entrecruzan diagonalmente de manera que mediante esto se forman rombos de control ópticos 25 a lo largo del paso. Además, al paso en forma de esclusa 12 está asignado un interruptor giratorio como elemento de mando central 8. Tal como se indica mediante los números crecientes en el indicador de mando 26 que está asignado al elemento de mando central 8, puede regularse de manera sencilla el patrón de seguridad del paso en forma de esclusa 12 mediante la regulación del interruptor giratorio. En el ejemplo de realización se conectan o desconectan detectores ópticos individuales debido a la regulación del elemento de mando central 8. De acuerdo con la representación básica en la figura 3, el patrón de seguridad aumenta desde la figura 3 a) de derecha a izquierda hasta la figura 3 f) continuamente, conectándose cada vez otros detectores ópticos. Los rombos de control ópticos 25 se vuelven debido a ello cada vez más y cada vez más pequeños, volviéndose la red de la detección óptica cada vez más fina. Así es concebible que un patrón de seguridad de acuerdo con la figura 3 a, sea justamente suficiente para distinguir que una persona pasa la esclusa, pudiéndose distinguir con una red cada vez más fina, por ejemplo de acuerdo con la figura 3 f), también aún de manera exacta si se trata de una o dos personas y eventualmente pudiéndose distinguir también si en la mano de una persona se lleva consigo un niño o un portafolio. Cuanto más fina sea la red mejor será el control de acceso, pero también la probabilidad de falsas alarmas. Mediante el elemento de mando 8 puede adaptarse de manera sencilla el patrón de seguridad de manera óptima a la situación y las necesidades.

Lista de números de referencia

1	dispositivo de control de acceso
2, 2'	puerta oscilante
3	elemento de bloqueo doble
4	zona vigilada
5	unidad de ordenador central
6	cámara
7	unidad de memoria
8	elemento de mando central
10, 10'	puerta circular
11	esclusa de personal
12, 12'	paso en forma de esclusa con hojas
13, 13'	instalación de torniquete
14	barrera de bloqueo
15	red de datos

16 software de parametrización

20 interfaz

21, 21’ hoja

22, 22’ elemento indicador

23 detectores

25 rombos de control

26 indicador de mando

REIVINDICACIONES

1. Dispositivo de control de acceso con al menos un elemento de control de acceso que desbloquea o bloquea el acceso a una zona protegida, un edificio o un recinto, en particular con un molinete, un torniquete, una puerta de batientes, una cámara o una barrera de bloqueo (14), así como al menos un dispositivo de lectura para la comprobación al menos de una característica de legitimación que documenta una autorización de acceso y/o al menos un detector, en particular una barrera de luz, para la comprobación al menos de una característica de seguridad, por ejemplo el número de personas que pasan, estando conectados al menos indirectamente los elementos de bloqueo de acceso y el dispositivo de lectura y/o los detectores respectivamente con al menos una unidad de ordenador (5) del dispositivo de control de acceso (1), presentando esta unidad de ordenador (5) un elemento de memoria (7) en el que están archivados características de legitimación, características de seguridad o valores teóricos permitidos y realizándose por medio de la unidad de procesamiento una comparación de las características de legitimación leídas con las características de legitimación almacenadas y/o una comprobación de las características de seguridad detectadas por detectores con las características de seguridad permitidas y dependiendo del resultado de esta comparación puede desbloquearse, preferentemente de manera automática, el elemento de bloqueo de acceso, estando dotada la unidad de ordenador central (5) del dispositivo de control de acceso (1) adicionalmente de un único elemento de mando (8) para el ajuste de etapas de seguridad predeterminadas y a cada una de estas etapas de seguridad está asignada una parametrización definida de la unidad de ordenador (5) de manera que dependiendo de la etapa de seguridad ajustada respectivamente está predeterminado de manera unívoca el número de las características de seguridad y/o de legitimación comprobadas y su respectivo umbral de tolerancia mediante la elección de la etapa de seguridad por medio del elemento de mando (8),
caracterizado porque el elemento de mando (8) interactúa para ello con un software de parametrización (16) de manera que a las etapas de seguridad que pueden seleccionarse por medio del elemento de mando (8) está asignado de manera ajustable y/o modificable respectivamente un número definido de las características de seguridad y/o de legitimación que van a comprobarse .

2. Dispositivo de control de acceso de acuerdo con la reivindicación 1, **caracterizado porque** el elemento de mando (8) es un interruptor giratorio regulable de manera escalonada o continua.

3. Dispositivo de control de acceso de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** los detectores se unen a una red de detectores y por medio del elemento de mando (8) pueden conectarse y desconectarse detectores individuales de esta red de detectores.

4. Dispositivo de control de acceso de acuerdo con la reivindicación 3, **caracterizado porque** al menos una parte de los detectores son detectores ópticos (23), en particular barreras de luz, cuyos ejes ópticos en dirección longitudinal están dispuestos transversalmente a la dirección de paso por el dispositivo de control de acceso y se entrecruzan uno en otro diagonalmente con la formación de rombos, aumentando o reduciéndose su número como consecuencia de la conexión y desconexión de campos de rombos.

5. Dispositivo de control de acceso de acuerdo con una de las reivindicaciones anteriores, **caracterizado porque** como característica de legitimación puede comprobarse por medio de los detectores al menos una característica biométrica, pudiéndose ajustar por medio del elemento de mando (8) el grado de coincidencia que va a requerirse de la característica biométrica detectada por medio de un dispositivo de lectura respectivamente dependiendo de la etapa de seguridad seleccionada.

6. Dispositivo de control de acceso de acuerdo con una o varias de las reivindicaciones anteriores, **caracterizado porque** la unidad de ordenador (5) está integrada en una red de datos (15), preferentemente una intranet, una red WLAN y/o en la internet, y mediante esto puede manejarse por control remoto el elemento de mando (8) y/o el software de parametrización (16).

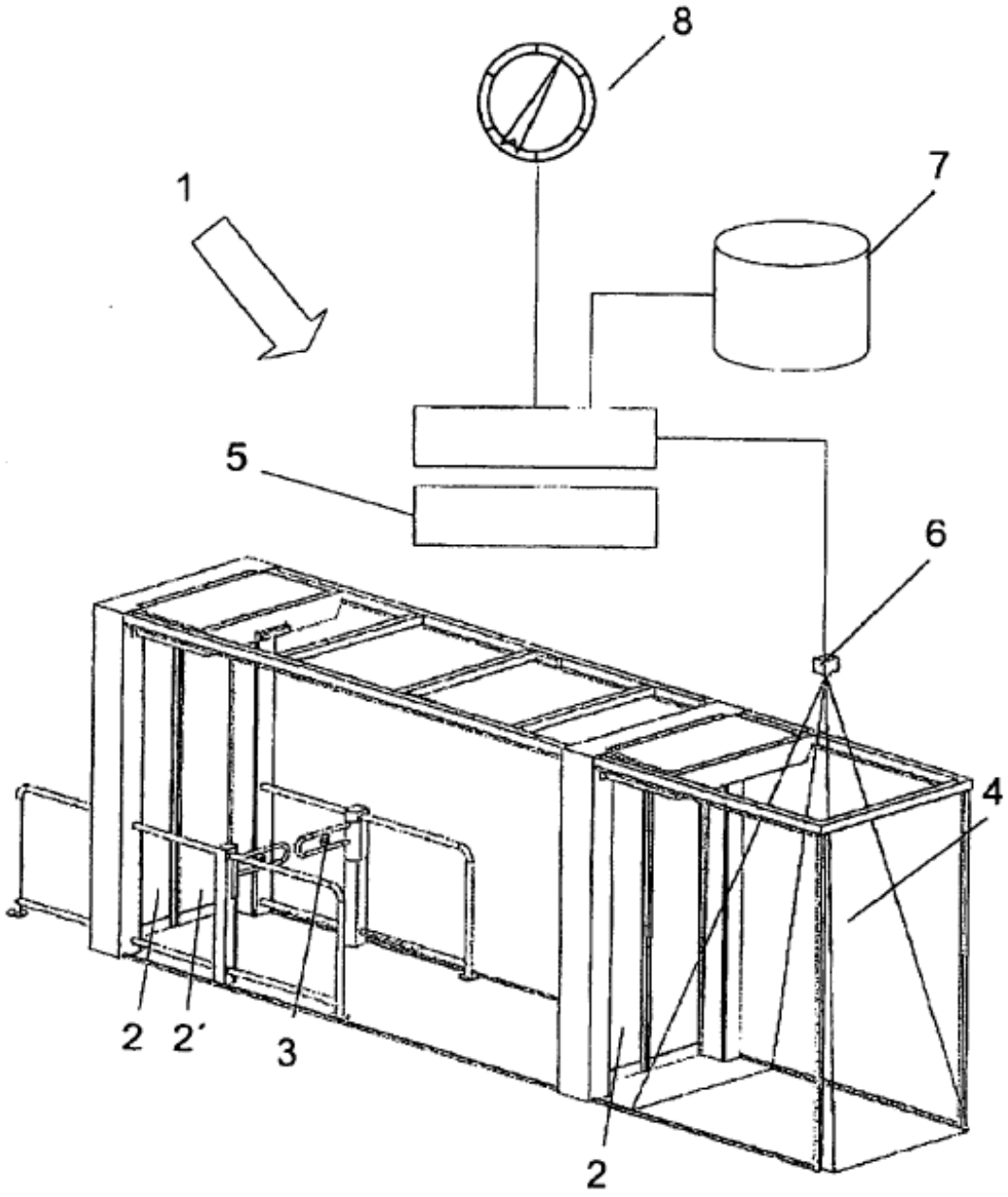

Fig. 1

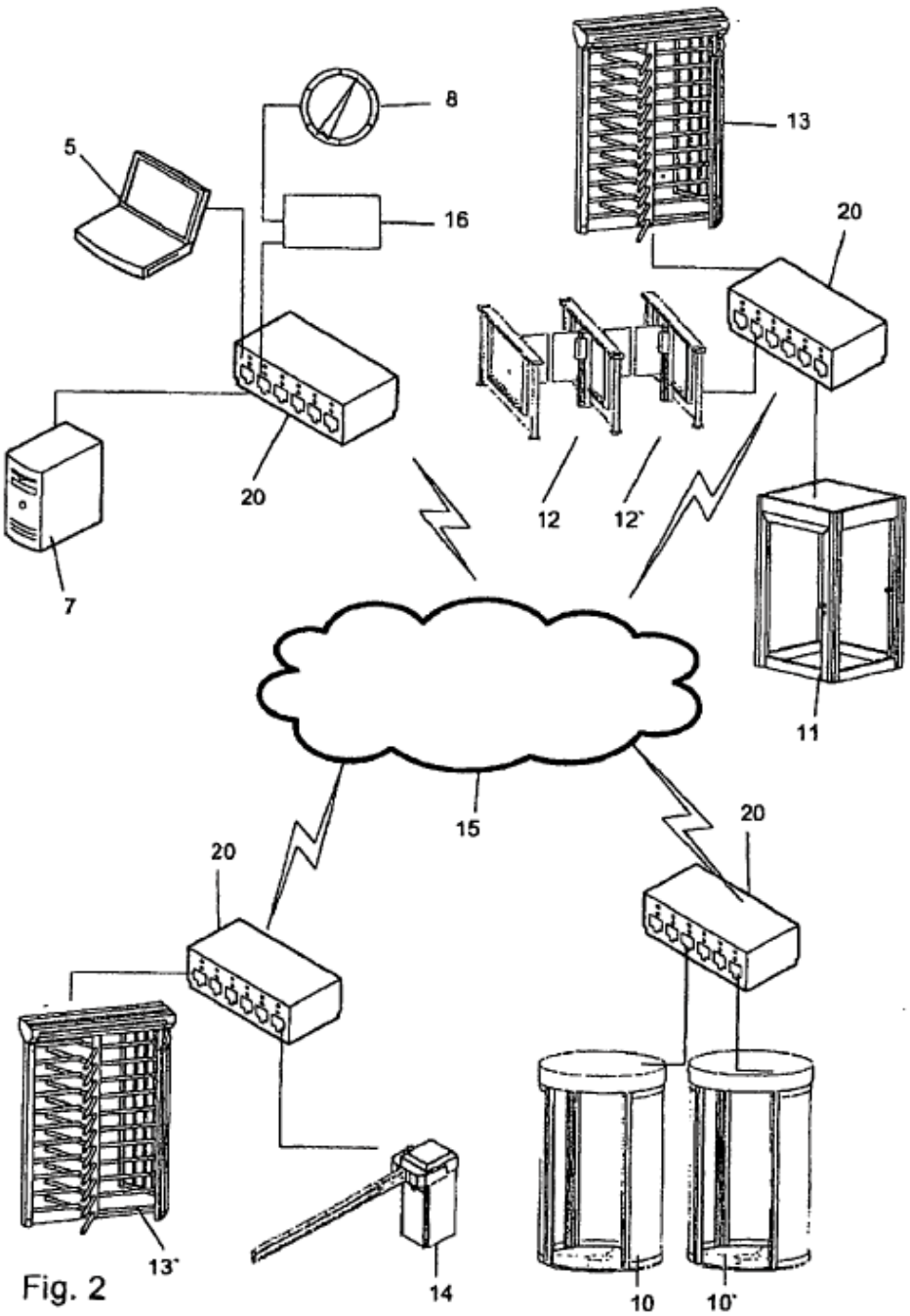

Fig. 2

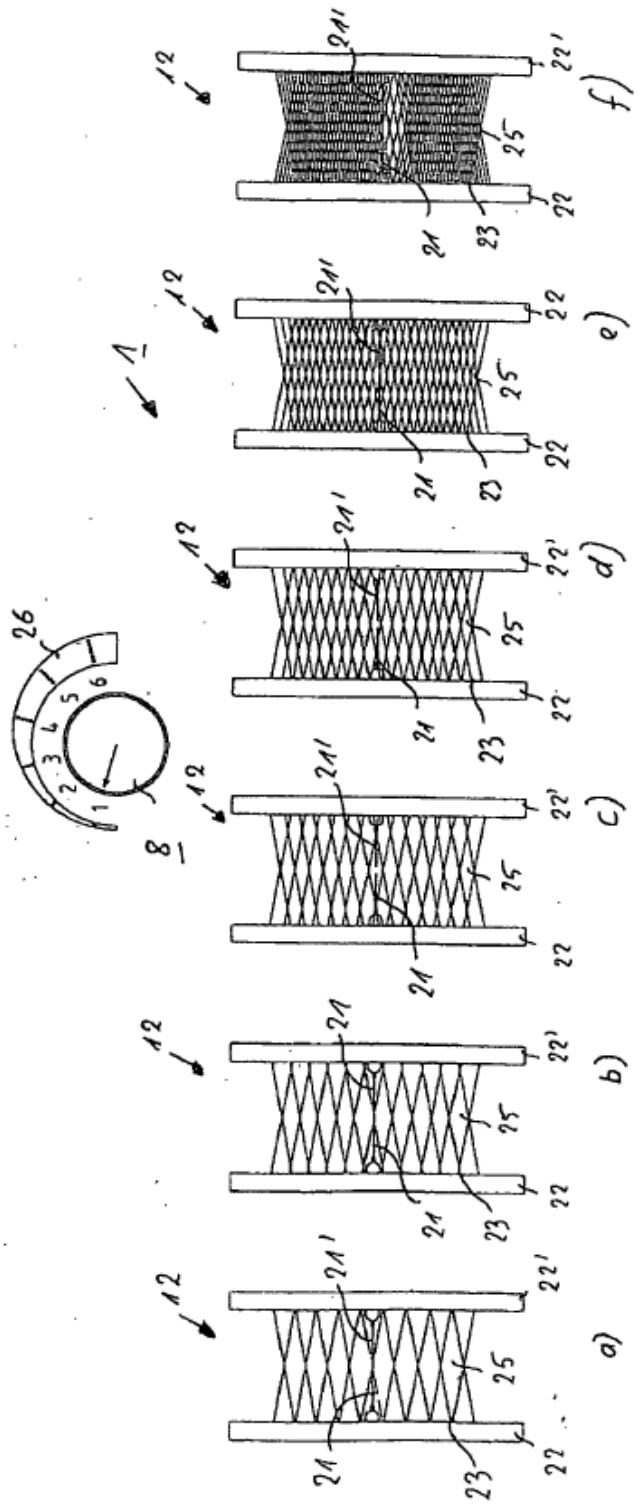

Fig. 3