



INPI
INSTITUTO NACIONAL
DA PROPRIEDADE
INDUSTRIAL
Assinado
Digitalmente

REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0906440-0

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0906440-0

(22) Data do Depósito: 23/01/2009

(43) Data da Publicação do Pedido: 30/07/2009

(51) Classificação Internacional: G07C 9/02.

(30) Prioridade Unionista: DE 10 2008 005 770.3 de 24/01/2008; DE 10 2008 016 516.6 de 31/03/2008.

(54) Título: DISPOSITIVO DE CONTROLE DE ACESSO

(73) Titular: KABA GALLENSCHUETZ GMBH. Endereço: Nikolaus-Otto-Str. 1, Bühl (Baden), ALEMANHA(DE)

(72) Inventor: JOSEF SCHORN.

Prazo de Validade: 10 (dez) anos contados a partir de 30/04/2019, observadas as condições legais

Expedida em: 30/04/2019

Assinado digitalmente por:
Liane Elizabeth Caldeira Lage
Diretora de Patentes, Programas de Computador e Topografias de Circuitos Integrados

Relatório Descritivo da Patente de Invenção para **"DISPOSITIVO DE CONTROLE DE ACESSO"**.

A presente invenção refere-se a um dispositivo de controle de acesso com pelo menos um elemento de controle de acesso que libera ou
5 bloqueia o acesso a uma região protegida, a uma edificação ou a um terreno, especialmente com um bloqueio giratório, um torniquete, uma porta com batentes giratória, câmara ou barreira de bloqueio, bem como com pelo menos um dispositivo de leitura para a verificação de pelo menos uma característica de legitimação que documente a autorização de acesso e/ou com pelo
10 menos um sensor, especialmente uma barreira de luz, para a verificação de pelo menos uma característica de segurança, como por exemplo a quantidade das pessoas que passem, sendo que os elementos de bloqueio e o dispositivo de leitura e/ou os sensores encontram-se respectivamente conectados ao menos indiretamente com pelo menos uma unidade de computador
15 do dispositivo de acesso, sendo que essa unidade de computador apresenta um elemento de memória, no qual são depositadas características de legitimação e características de segurança permitidas e sendo que por meio da unidade de processador ocorre uma comparação das características de legitimação lidas com as características de legitimação armazenadas e/ou uma
20 verificação das características de segurança detectadas por sensor com as características de segurança permitidas, e, em função do resultado dessa comparação, o elemento de acesso pode ser liberado, de preferência automaticamente.

Nesse sentido, por exemplo, pelo DE 10 2004 048 403 A1 já se
25 conhece um dispositivo de controle de acesso, especialmente para a região de alta segurança e região de aeroportos, na qual a uma região de um portão definido por uma entrada e uma saída controlada é associada a um ou mais dispositivos de controle e de verificação de identificação, como por exemplo um leitor de documentos, uma unidade biométrica para a detecção
30 de características biométricas, uma câmera e/ou barreiras de luz para o controle das mais diferentes características de teste, como por exemplo do controle de pessoas, individualização de pessoas ou identificação de pessoas

ou da autorização de acesso. Todos esses dispositivos de controle estão conectados em rede entre si através de um dispositivo de controle central, por exemplo para o nivelamento dos resultados de teste.

De modo complementar conhece-se pelo US 2006/0080541 A1 um sistema e um processo para a regulação automática ou manual de níveis de controle de acesso com base em níveis de segurança pré-ajustados. No âmbito da seleção dos níveis de segurança definidos, o nível de controle de segurança pode ser adaptado à situação atual, como por exemplo um dia de trabalho ou um feriado, assim como à situação local, como por exemplo 5 edificações privadas ou de empresas. Concretamente, no âmbito do processo de acordo com a invenção, há a possibilidade de parametrizar uma matriz de segurança que defina os parâmetros de acesso e de segurança, e de adaptar em caso de necessidade os parâmetros de uma situação de segurança modificada. 10

Os dispositivos de controle de acesso desse tipo servem para a liberação controlada de um acesso e, ao mesmo tempo, para a separação de pessoas que desejam entrar em uma região protegida, em uma edificação ou em um terreno. Nesse caso, é evidente que no âmbito da automa- 15 zação cada vez é mais desejável que a verificação das características de legitimação e/ou das características de segurança ocorra amplamente automaticamente, ou seja, que os dados detectados, respectivamente lidos, sejam comparados com dados armazenados e, em função desses dados, ocorra ou não a liberação do acesso. 20

Nesse sentido, unidades de computador cada vez mais rápidas, bem como elementos de memória cada vez mais apropriados e maiores 25 possibilitaram que características cada vez mais complexas sejam verificadas em correlação com a liberação de um acesso. Assim, nos últimos anos tornou-se possível detectar características biométricas, tais como uma impressão digital, uma imagem de pessoa ou uma imagem da íris, e compará-las com dados armazenados a fim de se verificar se a pessoa que tenta entrar no acesso realmente será admitida. Nesse caso, a verificação das características biométricas é complementada com outras verificações, tais como 30

uma verificação de vida quanto a impressões digitais tomadas ou uma verificação por câmera de um compartimento fechado no sentido de que só somente uma respectiva pessoa passe pelo acesso, e outras características de segurança possíveis.

- 5 Nesse caso, é possível que sempre os mesmos elementos de bloqueio de acesso, tais como portas giratórias, portões giratórios, portas com batentes giratórios ou outros elementos de bloqueio, sejam operados com diferentes sensores e dispositivos de leitura conforme o padrão de segurança. Quanto mais características sejam verificadas adicionalmente, tanto mais elevado será o padrão de segurança. Nesse sentido, frequentemente as instalações são equipadas com sensores e dispositivos de leitura que no momento do fornecimento não serão usados imediatamente, para uma adaptação posterior a padrões de segurança mais elevados.

- 15 Uma adaptação do padrão de segurança, nesse caso, é frequentemente complexa estando-se em operação. Isso se deve, por um lado, à exigência de que o padrão de segurança de edificações possa ser modificado durante o uso, tal como no âmbito de um uso modificado. Nesse sentido, é possível, por exemplo, que um prédio originalmente só comercial seja cada vez mais usado para atividades de pesquisas e, por isso, se tenha que aumentar o nível de segurança. Também é possível que em edificações até então usadas sem planejamento, em um momento posterior sejam guardados bens de elevado valor, como objetos onerosos ou mesmo dinheiro, de tal modo que por isso seja possível elevar o nível de segurança. Também é possível que a situação de risco se modifique em função de circunstâncias
- 20 externas, porque, por exemplo, uma série de arrombamentos na vizinhança exija um maior nível de segurança.

- 25 Por fim, existe também o uso inverso, ou seja, em que uma redução do nível de segurança seja desejada pelo usuário porque se constatou que o nível inicialmente desejado de segurança durante a operação leva a longos períodos de passagem das respectivas pessoas ou que a quota de erros é muito elevada.

30 Apesar de toda a precisão das instalações desse tipo, não é

possível evitar, por exemplo, que no âmbito da verificação, que apenas uma pessoa passe por uma portão, várias barreiras de luz sejam rompidas no caso, por exemplo, de pacotes maiores conduzidos, de tal modo que a instalação suponha que não apenas uma pessoa, mas sim duas pessoas desejam passar pela barreira. Nesse sentido, por exemplo, no caso de um prédio comercial pode-se constatar rapidamente que cada pessoa que conduza uma pasta de documentos provoque um alarme na instalação, com a consequência de que uma pessoa do pessoal de segurança tenha que executar uma verificação e que a instalação tenha que ser eventualmente liberada manualmente. Pode ser então frequentemente prático desligar esses controles ou uma única barreira de luz. No entanto, pode haver o desejo de em vez da verificação atual com duas barreiras de luz, executar uma outra verificação por meio de uma câmera e uma avaliação de imagem, por exemplo.

Durante a operação na prática comprovou-se que, na entrada em operação de um dispositivo de controle de acesso que trabalhe automaticamente, usualmente os clientes exigem o nível mais alto possível de segurança e, de acordo com isso, é executada uma parametrização da instalação. No decorrer da operação constata-se, então, frequentemente, que esse nível de segurança dificilmente pode ser combinado com as exigências da operação diária, de tal modo que, então, são executadas reparametrizações complicadas, até que por fim seja encontrado um ajuste no decorrer do "Try and Error", que, por um lado, proporcione um nível ótimo de segurança e, por outro lado, possibilite uma operação sem interferências, ou seja, um acesso sem interferências e eventualmente também uma saída de uma região protegida.

O re-equipamento complexo das instalações com uma respectiva interrupção da operação é percebido por todos os envolvidos como sendo desagradável e, além disso, é próprio para reduzir drasticamente a aceitação desse tipo de dispositivo de controle de acesso. Frequentemente, isso leva a que o nível de segurança original pretendido seja colocado muito menor do que seria desejável, no interesse de uma operação sem interferência. A rápida aceitação e funcionalidade de um dispositivo de controle de acesso re-

presenta, portanto, um requisito essencial para uma instalação complexa desse tipo.

A partir desse estado da técnica, a invenção tem como objetivo criar um melhor dispositivo de controle de acesso, que proporcione especialmente um manejo facilitado na instalação e na operação de um dispositivo de controle de acesso desse tipo.

Esse objetivo é alcançado com um dispositivo de controle de acesso segundo as características da reivindicação principal. Configurações vantajosas da invenção podem ser encontradas nas demais reivindicações.

O objetivo é alcançado devido ao fato de que à unidade de computador central, para a avaliação e para o nivelamento das características de legitimação lidas e das características de segurança detectadas, é alocada uma unidade de manejo, com a qual é possível ajustar níveis de segurança predefinidos. O ajuste dos níveis de segurança representa a seleção de parametrizações adequadas predefinidas da unidade de computador central, ou seja, por exemplo, uma seleção das características de legitimação e/ou de segurança detectadas e o respectivo limiar de tolerância combinado à verificação das características a ser executada. Os níveis de segurança dispostos em conexão com o elemento de manejo representam uma seleção dos níveis de segurança adequados para a respectiva situação de operação, sendo que conforme a aplicação, o elemento de manejo, equipado com diferentes parametrizações predefinidas, pode ser conectado com a unidade de computador.

Diferentemente das parametrizações convencionais, as instalações correspondentes são oferecidas, portanto, com diferentes parametrizações já predefinidas. No entanto, a invenção não se esgota na seleção de diferentes parametrizações possíveis do dispositivo de controle de acesso, senão que oferece adicionalmente a possibilidade de executar, através do elemento de manejo adicional, uma possibilidade de regulação sem nova parametrização da instalação ou re-equipamento complicado ou parametrização, simplesmente com um simples elemento de manejo e elemento de seleção. Nesse caso, um elemento de manejo desse tipo pode ser manejado

pelo pessoal de segurança usual ou por um porteiro sem qualquer conhecimento da instalação como tal.

O elemento de manejo adicional também permite, de modo fácil, passar imediatamente para condições modificadas, ou seja, por exemplo, no caso de uma fila grande, reduzir provisoriamente as características de segurança e, em seguida, continuar a operação novamente com um nível mais elevado de segurança.

Concretamente, no caso do elemento de manejo se trata de um simples comutador giratório, com o qual se pode escolher entre diferentes níveis de segurança. Nesse caso, pode se tratar de um comutador giratório escalonado ou sem escala. No caso de uma forma de execução com um comutador giratório sem escalas, através da regulação sem escalas também são modificadas as características sem escalas, ou seja, por exemplo, indicadores de parâmetros ou limiares de tolerância contínuos. Do ponto de vista técnico, um comutador giratório sem escalas desse tipo pode ser concretizado, por meio de uma resistência corrediça. A parametrização sem escalas de dispositivos de controle de acesso não é apenas uma concepção totalmente nova da técnica de segurança. Ela também possibilita uma adaptação individual às necessidades de segurança do cliente, tal como não era possível até agora. E isso – também pela primeira vez – sem pessoal qualificado.

Mais uma vez em uma configuração vantajosa, à unidade de manejo acha-se combinado um software especial de parametrização de tal modo que por meio desse software seja possível parametrizar os níveis de segurança que podem ser selecionados com o elemento de manejo. No entanto, o software de parametrização também permite modificar em caso de necessidade a parametrização uma vez executada, ou seja, adaptar os níveis de segurança selecionados, em sua configuração concreta, à operação modificada. O emprego do software de parametrização permite, portanto, através da melhor possibilidade de adaptação através da unidade de manejo, também adaptar a própria unidade de manejo a uma operação modificada. No entanto, a parametrização do software de parametrização continua

reservada usualmente ao pessoal especializado.

Nesse caso, em uma forma de execução preferida, ao dispositivo de controle de acesso acha-se associada uma rede de sensores com vários sensores, de tal modo que o nível de segurança já possa ser modificado
5 com facilidade através da conexão e desconexão de sensores individuais ou de grupos de sensores. Isso também é feito de um modo simples e viável para o pessoal de manejo através de regulação do elemento de manejo central.

Em uma configuração vantajosa, no caso da rede de sensores
10 pode se tratar, ao menos parcialmente, de sensores óticos que formam um portão ótico transversalmente à direção de passagem. Nesse caso, os sensores óticos ficam alinhados de tal modo que seus eixos óticos se cruzem formando losangos, com o efeito de que a quantidade de losangos e, portanto, a precisão do monitoramento ótico, se modificam através da regulação
15 do elemento de manejo central.

Em outra configuração da invenção, foi aprovado o procedimento de empregar o dispositivo de controle de acesso aperfeiçoado em ligação com a verificação de características biométricas como sendo característica de legitimação. Em especial, as exigências complexas na verificação de características biométricas requerem a possibilidade de um ajuste posterior de
20 um dispositivo de controle de acesso desse tipo através do emprego de uma unidade de manejo que pode ser empregada com facilidade.

Em uma forma vantajosa de desenvolvimento, a unidade central de computador pode estar conectada a uma rede de dados superior para a
25 verificação das características de segurança e/ou de legitimação e, desse modo, é possível executar por controle remoto uma verificação dos controles de acesso, assim como também um reajuste da unidade de manejo. A ligação correspondente da unidade de computador, mas também da unidade de manejo, possibilita uma manutenção ou reajuste, por exemplo por parte do
30 fabricante, sem que seja necessária uma observação correspondente no local da instalação.

A seguir, a invenção será explicada em detalhes com base em

um exemplo de execução representado no desenho. O exemplo de execução serve exclusivamente para a explicação detalhada, sendo que, evidentemente, é concebível uma série de outras formas de execução no âmbito da invenção.

5 Mostra-se:

Figura 1: um portão de acesso representado em perspectiva, com uma unidade de computador combinada a esse portão de acesso e com um elemento de manejo combinada a essa unidade de computador;

10 Figura 2: um dispositivo de controle de acesso com vários elementos de bloqueio de acesso, visto em perspectiva;

Figura 3: um outro dispositivo de controle de acesso, em uma vista de cima, como forma básica de representação.

A figura 1 mostra um dispositivo de controle de acesso 1, sendo que, nesse caso concreto, trata-se de um portão de passagem com vários
15 elementos de bloqueio de acesso, ou seja, várias portas pivotantes 2, 2', assim como um bloqueio pivotante duplo 3 e, eventualmente, outros elementos de bloqueio de acesso que não são mostrados aqui. Na direção de passagem, através da porta pivotante dianteira 2 acha-se definida uma região 4 monitorada por câmera e assinalada pela representação de raios, região
20 esta na qual, de um modo que não interessa aqui, inicialmente se verifica se apenas uma pessoa se encontra na região fechada. Adicionalmente, na região 4 monitorada pode ser executada também uma detecção de características biométricas, tal como a avaliação da imagem de rosto, para a verificação da individualização.

25 Tanto as portas pivotantes 2, 2', como também o bloqueio pivotante duplo 3, são respectivamente providos de um acionamento por motor elétrico, os quais estão sob conexão de dados separadamente ou em conjunto com uma unidade central de computador 5. Além disso, a unidade central de computador 5 encontra-se em conexão com a(s) câmera(s) 6 para o
30 monitoramento da região monitorada 4.

Somente quando a câmera 6 sinaliza que na região monitorada 4 se encontra apenas uma pessoa, é que a porta pivotante 2 será aberta em

uma etapa adicional. Além disso, por exemplo, podem ser verificados os dados biométricos ou, por meio de um dispositivo de leitura não mostrado aqui, outras características de segurança e/ou de legitimação. Somente quando também estas correspondem, ao menos em um grau predefinido, aos dados armazenados ou aos dados predeterminados é que serão abertos então o bloqueio pivotante duplo 3 e a porta pivotante seguinte 2'

Todas as características detectadas ou lidas são alocadas à unidade central de computador 5. A unidade de computador 5 acha-se conectada, além disso, com um dispositivo de memória 7, no qual estão depositadas as características de legitimação admissíveis. A unidade de computador 5 executa então uma comparação com as características armazenadas, e somente no caso em que estas coincidam em um grau predeterminado é que ocorre a liberação de cada um dos elementos de bloqueio de acesso do dispositivo de controle de acesso 1.

Adicionalmente, a unidade central de computador 5 está provida de uma unidade de manejo 8, uma assim chamada "Security Wheel". Nesse caso, trata-se de um comutador giratório regulável sem escalas, com o qual o nível de segurança respectivamente desejado pode ser predeterminado pelo respectivo pessoal de monitoramento ou de serviço. Através da regulação da unidade de manejo 8 regula-se, por exemplo, a faixa de tolerância da região monitorada 4, ou seja, as dimensões que ainda são aceitas para se concluir que na região monitorada 4 se encontra efetivamente apenas uma pessoa. Além disso, através da regulação da unidade de manejo 8 pode-se, ao mesmo tempo, regular quais desvios dos dados biométricos (imagem de identidade) armazenados são aceitos em relação aos dados detectados. É evidente que com um afrouxamento do nível de segurança reduz-se o esforço com computador e, com isso, aumenta-se a velocidade de controle da instalação. No entanto, com a crescente redução dos limiares de segurança há o risco de que, por exemplo, também duas pessoas passem pela instalação, mesmo que só uma esteja legitimada. Também é possível que através da unidade de manejo 8 seja reduzido o nível de segurança apenas provisoriamente em períodos de grandes filas.

Nesse caso, a Security-Wheel proporciona a possibilidade de se adaptar o nível de segurança sem escalas à atual situação de risco ou, por outros motivos quaisquer, reajustá-lo a qualquer momento de modo perfeito por meio de uma intervenção manual no sentido estrito do termo. Essa modificação é possível sem um pessoal especializado devido ao elemento de manejo de novo tipo (8). Devido a essa solução, o ajuste de segurança do dispositivo de controle de acesso pode se desenvolver conforme as exigências do cliente, sem que para isso não seja nada mais necessário do que escolher um novo ajuste no elemento de manejo (8).

10 Em uma outra forma de execução segundo a figura 2, parte-se de um terreno maior e protegido, o qual está protegido por meio de uma série de diferentes elementos de bloqueio de acesso.

Nesse caso concreto, por exemplo, para a segurança de uma edificação são empregados dois segmentos de círculo deslocáveis, respectivamente combinados com uma porta de batentes giratória, ou seja, uma assim chamada porta redonda 10, 10', um portão para pessoas 11 protegido por uma porta de bloqueio, bem como dois portões para pessoas 12, 12' (entrada e saída) protegido por dois flaps pivotantes, assim como um torniquete convencional 13, bem como um outro torniquete giratória 13' e uma barreira de bloqueio 14 para a segurança da região a ser protegida.

Nesse caso, os elementos de bloqueio de acesso estão reunidos em unidades funcionais, por exemplo, porque eles protegem uma região definida. Nesse sentido, por exemplo, as duas portas redondas 10, 10' com os segmentos de círculo deslocáveis podem proteger a entrada e a saída de uma unidade de edificação. Também se pode reunir em uma unidade o torniquete convencional 13 com os dois flaps 12, 12' e o portão para pessoas 11 construído em forma cúbica, para a segurança de uma região em comum, como por exemplo um terreno com uma edificação situada. Um outra unidade inclui um outro torniquete convencional 13', bem como a barreira de bloqueio 14, tal como podem ser empregadas, por exemplo, para a proteção de um estacionamento.

O dispositivo de controle de acesso 1 com sua série de elemen-

tos de bloqueio de acesso representa, portanto, uma segurança usual de um terreno de serviços.

Os elementos de bloqueio de acesso reunidos em unidades funcionais estão respectivamente ligados com uma interface 20, a qual recebe os dados detectados pelos respectivos dispositivos de leitura e elementos sensores combinados aos respectivos dispositivos de bloqueio de acesso e, eventualmente transmite sinais aos acionamentos por motor elétrico das instalações. Todas as interfaces 20 da instalação encontram-se em conexão de dados entre si através de uma rede de dados 15, como por exemplo a intranet ou a internet.

Uma interface 20 encontra-se adicionalmente em conexão de dados com um banco de dados, que se encontra depositado em um correspondente elemento de memória 7. Essa interface 20 encontra-se adicionalmente conectada com a unidade central de computador 5. À mesma interface encontra-se conectada a unidade de manejo adicional 8, mediante a intercalação de um software especial de parametrização 16.

Como resultado, a verificação dos dados mencionados por cada um dos elementos de bloqueio de acesso ocorre através de um nivelamento com as características de legitimação e de segurança armazenadas no banco de dados, levando-se em consideração os níveis de segurança determinados pela unidade central de manejo 8. Nesse caso, por meio do software de parametrização 16 pode ocorrer um re-ajuste da instalação no sentido de que a parametrização associada aos níveis individuais de segurança seja modificada posteriormente. Pelo lado operacional, executa-se um pré-ajuste da instalação por meio do software de parametrização 16.

O exemplo de execução 2 mostra, de modo particular, como a tarefa de parametrização, quase que completamente não pode deixar de ser entendida pelo pessoal de serviço comum, de um dispositivo completo de controle de acesso 1 para um terreno ampliado de serviços através de simples regulagem de um único elemento de manejo 8 pode ser adaptada à respectiva necessidade e, eventualmente, também a condições modificadas.

Para a continuação da explicação, na figura 3 é mostrado um

outro dispositivo de controle de acesso 1, o qual, nesse exemplo, é constituído apenas por uma portão de passagem 12 com os flaps 21, 21' que bloqueiam ou liberam uma passagem controlada, conforme a necessidade, sendo que a passagem encontra-se delimitada de ambos os lados por elementos condutores 22, 22'. Ao longo da extensão longitudinal dos elementos condutores estão dispostos sensores óticos 23, distanciados um do outro, e caso necessário em um ou mais planos de controle óticos, sensores estes cujos eixos óticos estão dispostos na direção de raio transversalmente à direção de passagem através do portão de passagem 12 e cujas direções de raios se cruzam diagonalmente de um modo tal que desse modo sejam formados losangos de controle 25 ao longo da passagem. Além disso, ao portão de passagem 12 acha-se associado um comutador giratório servindo de elemento central de manejo 8. Tal como indicado pelos números crescentes no painel de serviço 26, que está associado ao elemento central de manejo 8, é possível regular o nível de segurança da portão de passagem 12 com facilidade através da regulagem do comutador giratório. Nesse exemplo de execução, devido à regulagem do elemento central de manejo 8, os sensores óticos individualmente são ligados ou desligados. Segundo a exposição básica na figura 3, o nível de segurança é aumentado continuamente da figura 3 a) da direita para a esquerda até a figura 3 f), na medida em que sejam conectados cada vez mais sensores óticos. Desse modo, os losangos de controle óticos 25 tornam-se cada vez mais numerosos e cada vez mais menores, e a rede da detecção ótica cada vez mais fina. Nesse sentido é possível que um nível de segurança segundo a figura 3a seja suficiente para identificar que uma pessoa passa pela portão, sendo que com uma rede cada vez mais fina, por exemplo segundo a figura 3 f), ainda é possível se diferenciar com exatidão se trata-se de uma ou duas pessoas e eventualmente também se diferenciar se na mão de uma pessoa encontra-se conduzida uma criança ou uma pasta de documentos. Quanto mais fina for a rede, melhor será o controle de acesso, porém também a probabilidade de alarmes falsos. Através do elemento de manejo 8 pode-se adaptar de modo ótimo e facilmente o nível de segurança à situação e às necessidades.

LISTAGEM DE REFERÊNCIA

	1	dispositivo de controle de acesso
	2, 2'	porta pivotante
	3	elemento de bloqueio duplo
5	4	região monitorada
	5	unidade central de computador
	6	câmera
	7	unidade de memória
	8	elemento central de manejo
10	10, 10'	porta redonda
	11	portão para pessoas
	12, 12'	portão de passagem com flaps
	13, 13'	instalação de torniquete
	14	barreira de bloqueio
15	15	rede de dados
	16	software de parametrização
	20	interface
	21, 21'	flap
	22, 22'	elemento condutor
20	23	sensores
	25	losangos de controle
	26	painel de manejo

REIVINDICAÇÕES

1. Dispositivo de controle de acesso com pelo menos um elemento de controle de acesso que libera ou bloqueia o acesso a uma região protegida, a uma edificação ou a um terreno, especialmente com um bloqueio giratório, um torniquete, uma porta de batentes giratória, câmera ou uma barreira de bloqueio (14), bem como pelo menos um dispositivo de leitura para a verificação de pelo menos uma característica de legitimação que documenta uma autorização de acesso e/ou pelo menos um sensor, especialmente uma barreira de luz, para a verificação de pelo menos uma característica de segurança, como por exemplo a quantidade das pessoas passando, sendo que os elementos de bloqueio de acesso e o dispositivo de leitura e/ou os sensores estão respectivamente conectados ao menos indiretamente com pelo menos uma unidade de computador (5) do dispositivo de controle de acesso (1), sendo que essa unidade de computador (5) apresenta um elemento de memória (7), no qual estão depositadas características de legitimação admissíveis, características de segurança ou valores teóricos e sendo que, por meio da unidade de processador, ocorre uma comparação das características de legitimação lidas com as características de legitimação armazenadas e/ou uma verificação das características de segurança detectadas por sensor com as características de segurança admissíveis, e, em função do resultado dessa comparação, o elemento de bloqueio de acesso pode ser liberado, de preferência automaticamente, caracterizado pelo fato de que a unidade central de computador (5) do dispositivo de controle de acesso (1) está munida adicionalmente de um elemento de manejo (8) para o ajuste de níveis de segurança predeterminados e a cada um desses níveis de segurança acha-se associada uma parametrização definida da unidade de computador (5), de tal modo que, em função do nível de segurança respectivamente ajustado, seja predeterminada inequivocamente a quantidade das características verificadas de segurança e/ou de legitimação e os seus respectivos limiares de tolerância através de seleção dos níveis de segurança por meio do elemento de manejo (8).

2. Dispositivo de controle de acesso de acordo com a reivindica-

ção 1, caracterizado pelo fato de que o elemento de manejo (8) é um comutador giratório regulável com escalas ou sem escalas.

3. Dispositivo de controle de acesso de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que à unidade de manejo (8) acha-se
5 associado um software de parametrização (16) de um modo tal que aos níveis de segurança selecionáveis por meio da unidade de manejo (8) está associada de modo ajustável e/ou regulável, por meio do software de parametrização (16), uma quantidade definida de características de segurança e/ou de legitimação a serem verificadas.

10 4. Dispositivo de controle de acesso de acordo com qualquer uma das reivindicações 1 a 3, caracterizado pelo fato de que os sensores se complementam para formar uma rede de sensores, e, por meio da unidade de manejo, sensores individualmente dessa rede de sensor podem ser ligados e desligados.

15 5. Dispositivo de controle de acesso de acordo com a reivindicação 4, caracterizado pelo fato de que no mínimo uma parte dos sensores é de sensores óticos (23), especialmente barreiras de luz, cujos eixos óticos estão dispostos em direção longitudinal transversalmente à direção de passagem através do dispositivo de controle de acesso, e se cruzam diagonalmente formando losangos, sendo que, devido à conexão e desconexão de
20 campos de losangos, a sua quantidade aumenta e diminui.

6. Dispositivo de controle de acesso de acordo com qualquer uma das reivindicações anteriores, caracterizado pelo fato de que como característica de legitimação pelo menos uma característica biométrica é verificável por meio dos sensores, sendo que por meio da unidade de manejo (8)
25 é possível ajustar o grau da coincidência a ser exigida da característica biométrica detectada por meio de um dispositivo de leitura, respectivamente em função do nível de segurança selecionado.

7. Dispositivo de controle de acesso de acordo com qualquer
30 uma das reivindicações 1 a 6, caracterizado pelo fato de que a unidade de computador (5) está conectada a uma rede de dados (15), de preferência uma intranet, uma rede WLAN e/ou à internet e, desse modo, é possível

manejar por controle remoto a unidade de manejo (8) e/ou o software de parametrização (16).

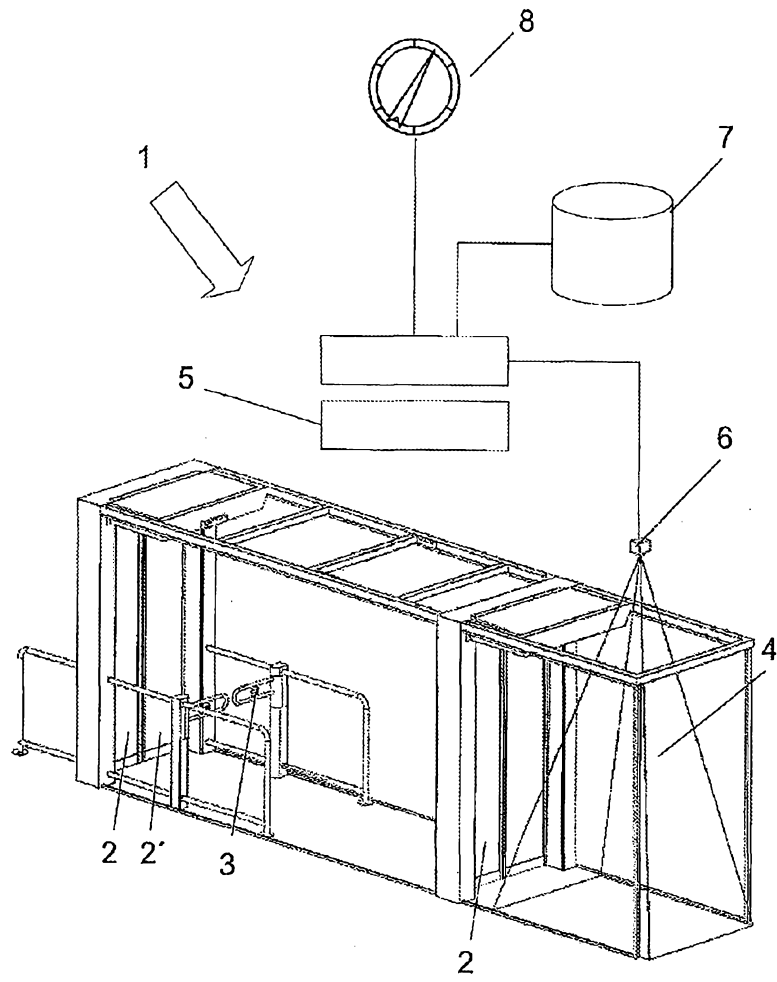


Fig. 1

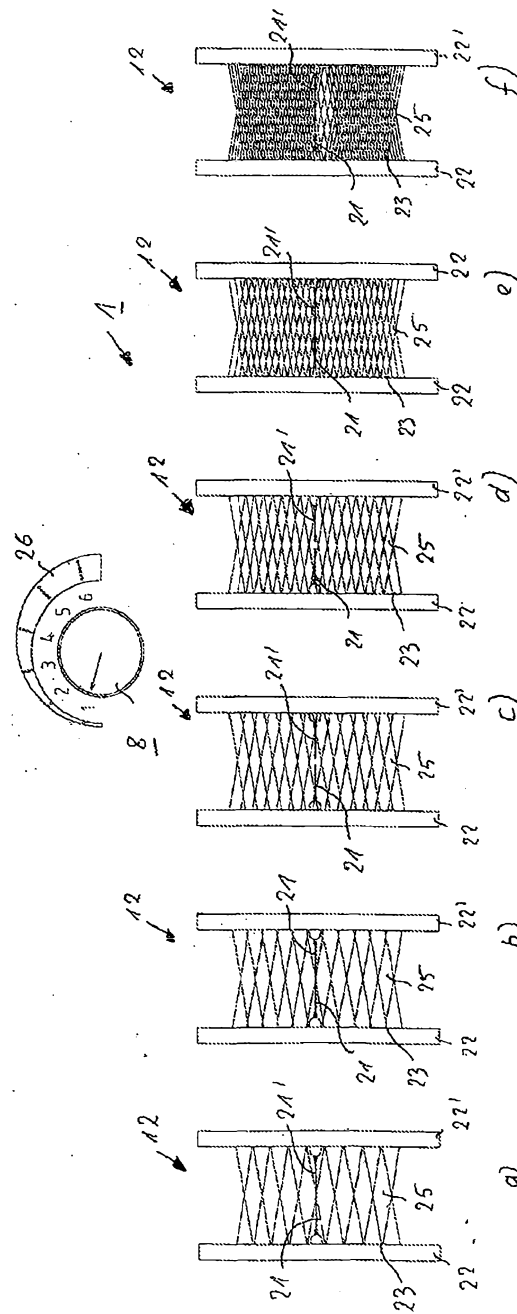


FIG. 3