(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 219 930**

(51) Int. Cl.:
E05B 49/00 (2006.01)
G07C 9/00 (2006.01)
B60R 25/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA MODIFICADA T5

(86) Número de solicitud europea: **98965587 .3**
(86) Fecha de presentación : **20.11.1998**
(87) Número de publicación de la solicitud: **1038080**
(87) Fecha de publicación de la solicitud: **27.09.2000**

(54) Título: **Sistema para controlar la autorización de acceso.**

(30) Prioridad: **11.12.1997 DE 197 55 092**

(45) Fecha de publicación de la mención y de la traducción de patente europea: **01.12.2004**

(45) Fecha de la publicación de la mención de la patente europea modificada BOPI: **16.06.2008**

(45) Fecha de publicación de la traducción de patente europea modificada: **16.06.2008**

(73) Titular/es: **ROBERT BOSCH GmbH**
Postfach 30 02 20
70442 Stuttgart, DE

(72) Inventor/es: **Schmitz, Stephan y**
Mathony, Hans-Joerg

(74) Agente: **Carvajal y Urquijo, Isabel**

ES 2 219 930 T5

DESCRIPCIÓN

Sistema para controlar la autorización de acceso.

Estado de la técnica

La invención se refiere a un sistema para controlar la autorización de acceso, según el concepto genérico de la reivindicación independiente. A partir del documento DE 44 28 947 C1 se conoce ya un dispositivo de cierre para un vehículo con un dispositivo de activación, así como con un transpondedor. Activando un emisor puede generarse una palabra de código variable para un accionamiento a distancia, que se recibe por un aparato de decodificación, se compara con una señal de código variable de un accionamiento a distancia almacenada en el aparato de decodificación y genera una señal de desbloqueo en función de la comparación. Además, para aumentar la seguridad está previsto un transpondedor cuya señal de código variable se valora adicionalmente para una liberación.

A partir del documento DE 195 01 004 A1 se conoce un procedimiento para poner en funcionamiento un sistema de transmisión de datos formado por un transpondedor y un aparato de lectura. Para la transmisión verificable de datos entre un aparato de lectura y un transpondedor, el aparato de lectura envía tras su activación un mensaje - aparato de lectura. Tras su activación, el transpondedor recibe el mensaje - aparato de lectura y transmite un primer mensaje - transpondedor al aparato de lectura. El proceso de verificación se realiza por medio de un código fijo - transpondedor almacenado en el transpondedor y un código fijo - aparato de lectura almacenado en el aparato de lectura. Tras la autentificación satisfactoria entre el transpondedor y el aparato de lectura pueden desbloquearse los aparatos de control conectados al aparato de lectura por medio de líneas de comunicación.

La invención se basa en la tarea de simplificar el sistema del documento DE 44 28 947 C1 sin sufrir una merma de seguridad. La tarea se soluciona mediante las características significativas de la reivindicación independiente.

El sistema según la invención para controlar la autorización de acceso comprende un aparato base que recibe una palabra de código. La palabra de código contiene una respuesta (*Response*) que un ordenador compara con una respuesta teórica (*Sollresponse*). Al coincidir la respuesta y la respuesta teórica se produce una autorización de acceso. Como mínimo un mando a distancia envía la palabra de código. El sistema según la invención se caracteriza porque, para generar la palabra de código en el mando a distancia está almacenada una señal de estímulo (*Challenge*) enviada por el aparato base en el marco de un procedimiento de estímulo - respuesta (*challenge - response*) ya realizado con éxito en el pasado. Por tanto, la señal de estímulo proporciona una indicación sobre una autorización del mando a distancia. Con ello se limitan las posibilidades de manipulación. Además, ya no es necesario un nuevo procedimiento bidireccionado de estímulo - respuesta para iniciar un procedimiento de autorización de acceso puesto que la señal de estímulo ya está almacenada en la memoria del mando a distancia. De esta manera, ya puede enviarse la palabra de código al aparato base con un alcance mayor, mientras que el procedimiento de estímulo - respuesta sólo puede realizarse en el área cercana. Con ello se garantiza un desacoplamiento entre la transmisión bidireccional de datos y la transmisión unidireccional de datos. En el mando a distancia sólo está previsto un emisor de mayor alcance, pero no un receptor correspondiente para la zona lejana. La señal de estímulo puede emplearse para la sincronización entre el aparato base y el mando a distancia. Además, la respuesta o respuesta teórica decisiva directamente para la autorización de acceso no está almacenada ni en el aparato base, ni en el mando a distancia, de tal manera que no es posible el acceso directo a está información relevante para la seguridad.

En un perfeccionamiento conveniente, la respuesta teórica se forma en función de un indicador almacenado en el mando a distancia e incluido en la palabra de código. Con ello se consigue una asignación inequívoca entre el mando a distancia empleado y el cifrado correspondiente almacenado en el aparato base. La asignación inequívoca garantiza una seguridad suficientemente alta frente a intentos de manipulación no autorizados. Con ello puede simplemente suprimirse el algoritmo que cifra en el mando a distancia la señal de estímulo almacenada para dar lugar a una respuesta, por ejemplo, empleando un indicador específico del mando a distancia, y puede estar integrado en un microcontrolador.

En una configuración, tras un número predeterminado de coincidencias erróneas de la respuesta y la respuesta teórica, se elimina la señal de estímulo almacenada en el aparato base. Con ello, en el caso de un número de intentos de apertura fallidos se garantiza que ya no tendrá lugar una autorización de acceso al seguir probando. Sólo debe permitirse un nuevo intento de apertura en combinación con un procedimiento de estímulo - respuesta realizado con éxito. Al fracasar la autorización de acceso por medio del protocolo unidireccional, aumentan los requisitos de seguridad pudiendo lograrse un acceso sólo en combinación con el complejo protocolo bidireccional.

Una configuración ventajosa prevé que en la palabra de código esté contenido un código de contador que el aparato base compara con un código de referencia. Sólo en caso de una divergencia tiene lugar una autorización de acceso. El código de contador se modifica con la activación de un elemento de manejo del mando a distancia. No se libera ninguna autorización de acceso al enviar la palabra de código que se acaba de interceptar. El estado del contador puede estar presente tanto cifrado como no cifrado en la palabra de código.

Como código de referencia se emplea un código enviado. No está prevista para ello una función de contador independiente en el aparato base.

De forma conveniente, la transmisión de la palabra de código tiene lugar a una frecuencia alta y la transmisión de la señal de estímulo, a una frecuencia baja. Debido a la señal de estímulo almacenada, el mando a distancia no requiere ningún receptor en la franja de alta frecuencia.

De las otras reivindicaciones dependientes y de la memoria descriptiva se obtienen otros perfeccionamientos convenientes.

Dibujo

En el dibujo se muestran dos ejemplos de realización posibles de un sistema según la invención para controlar la autorización de acceso y se explican detalladamente en la siguiente memoria descriptiva. Las figuras 1 y 2 muestran un diagrama de bloques y un procedimiento de autorización de acceso de un primer ejemplo de realización, las figuras 3 y 4 muestran un diagrama de bloques y un procedimiento de autorización de acceso de un segundo ejemplo de realización.

Descripción

Varios mandos F1,... Fx,... Fn a distancia se comunican con un aparato BG base que comprende un emisor/receptor 12 y un ordenador 16. El ordenador 16 intercambia datos con el emisor/receptor 12 y tiene acceso a señales C1,... Cx,... Cn de estímulo, indicadores K1,..., Kx,... Kn y un valor G límite almacenados en la memoria. A modo de ejemplo se muestra la estructura del mando Fx a distancia, número x. Un ordenador 20 del mando a distancia tiene acceso al indicador Kx y a la señal Cx de estímulo almacenados en la memoria. Éste emite datos al emisor 22 e intercambia datos con un emisor/receptor 26 del mando a distancia. El estado de señal influenciado por un elemento 24 de manejo se alimenta al ordenador 20 del mando a distancia.

El segundo ejemplo de realización según la figura 3 se diferencia del primer ejemplo de realización según la figura 1 porque en el aparato BG base está prevista, en lugar del valor G límite, una memoria para un código RZ1,..., RZx,... RZn de referencia. El mando Fx a distancia presenta un campo adicional para un código Zx de contador.

A continuación se explica detalladamente el modo de funcionamiento del primer ejemplo de realización mostrado en la figura 1. En el aparato BG base está almacenado un indicador K1,..., Kx,..., Kn correspondiente para cada mando F1,..., Fx,... Fn a distancia. Con ello, el aparato BG base puede identificar de forma inequívoca cada mando Fx a distancia individual o cada grupo Fx de mandos a distancia, si, por ejemplo, está asignado un indicador Kx a varios mandos Fx a distancia. Estos indicadores K1,..., Kx,... Kn pueden ser los espacios de memoria correspondientes o reconocerse mediante el espacio de memoria. En el procedimiento de estímulo - respuesta, el aparato base envía la señal Cx de estímulo al mando Fx a distancia asignado de forma inequívoca mediante el indicador Kx. Un generador de números aleatorios genera esta señal Cx de estímulo. El ordenador 16 almacena la señal Cx de estímulo enviada en un espacio de memoria direccionado por medio del indicador Kx. El ordenador 20 del mando a distancia almacena en una memoria la señal Cx de estímulo enviada en último lugar por el aparato BG base.

El usuario inicia la comunicación unidireccional del mando Fx a distancia con el aparato BG base accionando el elemento 24 de manejo, etapa 101. El ordenador 20 del mando a distancia combina la señal Cx de estímulo almacenada en la memoria con un algoritmo empleando una información específica del mando a distancia para el mando Fx a distancia especial, a partir de lo cual se genera la respuesta Rx. Como información específica del mando a distancia se emplea, por ejemplo, una parte del indicador Kx, un código del fabricante almacenado de forma fija en el mando Fx a distancia. Sin embargo, es fundamental que este cifrado de la señal Cx de estímulo, es decir, el algoritmo y la información específica del mando a distancia, también se conozca y esté almacenado en el aparato BG base para cada mando Fx a distancia. En la palabra CWx de código están incluidos el indicador Kx y la respuesta Rx, dado el caso, instrucciones correspondientes de despertar y acción. El emisor 22 envía la palabra CWx de código al aparato BG base, etapa 103. El ordenador 16 filtra el indicador Kx a partir de la palabra CWx de código recibida. El ordenador 16 elige la señal Cx de estímulo y el cifrado direccionados con este indicador Kx, con los que también se ha determinado la respuesta Rx en el mando Fx a distancia. A partir de la señal Cx de estímulo, el algoritmo y la información específica del mando a distancia, es decir, el cifrado, almacenados en el aparato BG base, el ordenador 16 calcula la respuesta Sx teórica, etapa 105. En el aparato BG base se comparan la respuesta Rx recibida y la respuesta Sx teórica calculada, etapa 107. En el caso de que coincidan, el ordenador 16 proporciona una señal de liberación correspondiente, etapa 109. En otro caso, continua la consulta 111 de si el número de intentos M de apertura fallidos ya ha superado un valor G límite predeterminado. Si es este el caso, no se permite ningún intento de apertura más, etapa 113. Además, se elimina la señal Cx de estímulo almacenada en el aparato BG base. Por tanto, sólo puede conseguirse una autorización de acceso al realizarse con éxito el procedimiento bidireccional de estímulo - respuesta, pero no con el protocolo unidireccional descrito. Si el número de intentos M de apertura fallidos aún no ha sobrepasado el valor G límite, se incrementa el número M, etapa 115. A continuación de esto sigue la etapa 105, el procedimiento posterior se desarrolla tal como ya se ha descrito.

Las etapas a partir de la 111 aumentan la seguridad de la transmisión unidireccional de datos, aunque no son forzosamente necesarias.

El segundo ejemplo de realización descrito a continuación se refiere a las figuras 3 y 4. Tal como ya se ha expuesto para el primer ejemplo de realización, en el mando Fx a distancia está almacenada la señal Cx de estímulo. En el mando

Fx a distancia está almacenado un código Zx de contador que se incrementa al accionar el elemento 24 de manejo. Para cada mando Fx a distancia se almacena en el aparato BG base el último código Zx de contador enviado como código RZ1,..., RZx,... RZn de referencia. Tras activarse el proceso de inicio mediante el accionamiento del elemento 24 de manejo, etapa 121, se calcula la respuesta Rx de acuerdo con el primer ejemplo de realización. El código Zx de contador se aumenta un uno. En la palabra CWx de código está incluido de manera cifrada el código Zx de contador, además de la respuesta Rx y el indicador Kx. El emisor 22 envía la palabra CWx de código al emisor/receptor 12, etapa 123. A su vez, el ordenador 16 filtra el indicador Kx a partir de la palabra CWx de código recibida, por medio del cual lee el código RZx de referencia perteneciente al mando Fx a distancia, etapa 125. A continuación se compara el código Zx de contador con el código RZx de referencia, etapa 127. Puesto que en el aparato BG base está almacenado como código RZx de referencia el último código Zx de contador enviado, en el caso de una activación adecuada del mando Fx a distancia el código Zx de contador y el código RZx de referencia difieren entre sí. Sin embargo, si éstos coinciden, se interrumpe, etapa 129. No tiene lugar una autorización de acceso. En caso contrario, el aparato BG base determina la respuesta Sx teórica, tal como ya se ha indicado para el primer ejemplo de realización, etapa 131. Si no coinciden la respuesta Rx y la respuesta Sx teórica, etapa 133, entonces se interrumpe, etapa 135. En caso contrario, se proporciona la autorización para iniciar un proceso de apertura, etapa 137.

Como segundo ejemplo de realización alternativo, se cifra el código Zx de contador en el mando Fx a distancia. Para determinar el código Rx de referencia, este cifrado debe almacenarse direccionado en el aparato BG base. Para el código Zx de contador sólo es importante que se modifique con cada accionamiento del mando Fx a distancia, sin ser esencial si es a través de una función de contador u otro algoritmo.

Asimismo, los dos ejemplos de realización pueden combinarse en el sentido de que, por ejemplo, en el desarrollo según la figura 4, la consulta se realiza tras la etapa 111. Con ello puede aumentarse adicionalmente la seguridad frente a intentos de apertura no autorizados.

El procedimiento de estímulo - respuesta no expuesto de forma más detallada tiene lugar preferiblemente en la zona cercana del espacio al que se va a entrar, por ejemplo, de un vehículo, con una frecuencia menor que la transmisión de la señal a través del emisor 22 que permite un alcance mayor. No está previsto un receptor correspondiente para el mando Fx a distancia. El algoritmo para cifrar la señal Cx de estímulo para obtener la respuesta Rx, puede realizarse preferiblemente de forma tan sencilla que puede implementarse también en un microcontrolador.

REIVINDICACIONES

1. Sistema para controlar la autorización de acceso,

- con un aparato (BG) base que recibe una palabra (CWx) de código que contiene una respuesta (Rx) que un ordenador (16) compara con una respuesta (Sx) teórica, produciéndose una autorización de acceso al coincidir la respuesta (Rx) y la respuesta (Sx) teórica,

- con como mínimo un mando (F1,..., Fx,... Fn) a distancia que envía la palabra (CWx) de código, estando almacenada en el como mínimo un mando (F1,..., Fx,... Fn) a distancia, para generar la palabra (CWx) de código, una señal (Cx) estímulo enviada por el aparato (BG) base en el marco de un procedimiento de estímulo - respuesta ya realizado satisfactoriamente en el pasado,

caracterizado porque la señal (Cx) estímulo almacenada en el aparato (BG) base se elimina cuando el número de coincidencias erróneas de la respuesta (Rx) y la respuesta (Sx) teórica sobrepasa un valor (G) límite que puede fijarse previamente.

2. Sistema según la reivindicación 1, **caracterizado** porque la respuesta (Sx) teórica se forma en función de un indicador (K1,..., Kx,... Kn) almacenado en el mando (F1,..., Fx,... Fn) a distancia e incluido en la palabra (CWx) de código.

3. Sistema según una de las reivindicaciones precedentes, **caracterizado** porque la señal (Cx) de estímulo está almacenada en el aparato (BG) base.

4. Sistema según una de las reivindicaciones precedentes, **caracterizado** porque en la palabra (CWx) de código está incluido un código (Zx) de contador que el aparato (BG) base compara con un código (RZx) de referencia.

5. Sistema según la reivindicación 4, **caracterizado** porque el código (Zx) de contador se modifica al accionar un elemento (24) de manejo del mando (F1,..., Fx,... Fn) a distancia.

6. Sistema según una de las reivindicaciones precedentes 4 o 5, **caracterizado** porque como código (RZx) de referencia se emplea un código (Zx) de contador enviado.

7. Sistema según una de las reivindicaciones precedentes 4 a 6, **caracterizado** porque el código (Zx) de contador está incluido de manera cifrada en la palabra (CWx) de código.

8. Sistema según una de las reivindicaciones precedentes, **caracterizado** porque la transmisión de la palabra (CWx) de código tiene lugar con una frecuencia más alta que la transmisión de la señal (Cx) de estímulo.

Fig. 1

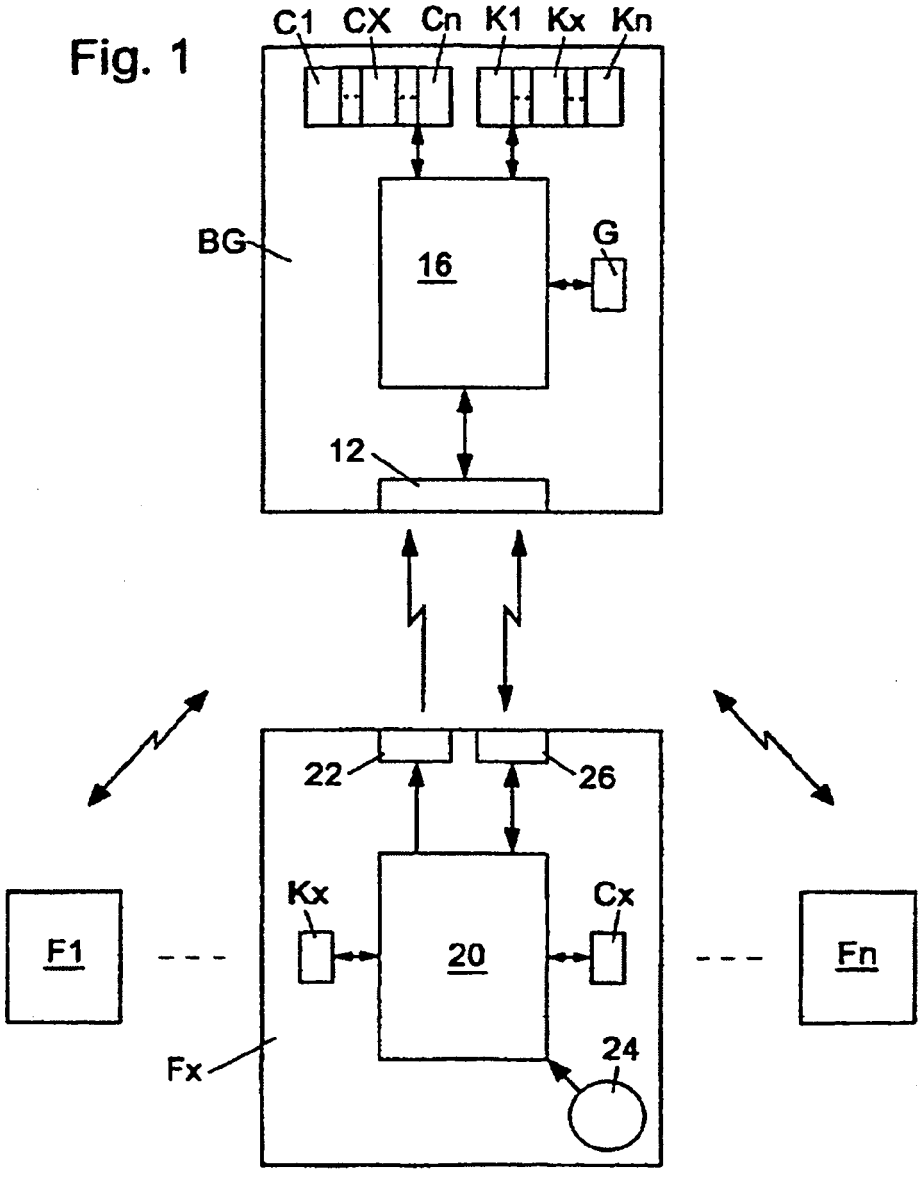


Fig. 2

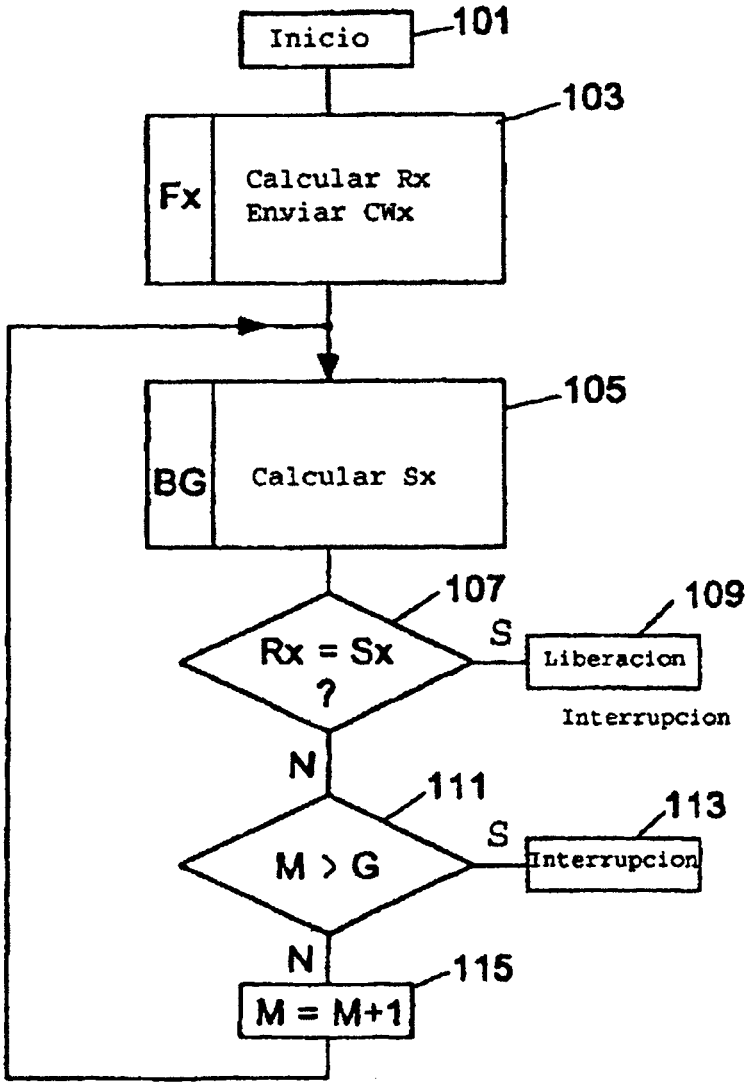

Inicio
101
103
Fx
Calcular Rx
Enviar CWx
105
BG
Calcular Sx
107
Rx = Sx
?
S
109
Liberacion
Interrupcion
N
111
M > G
S
113
Interrupcion
N
115
M = M+1

Fig. 3

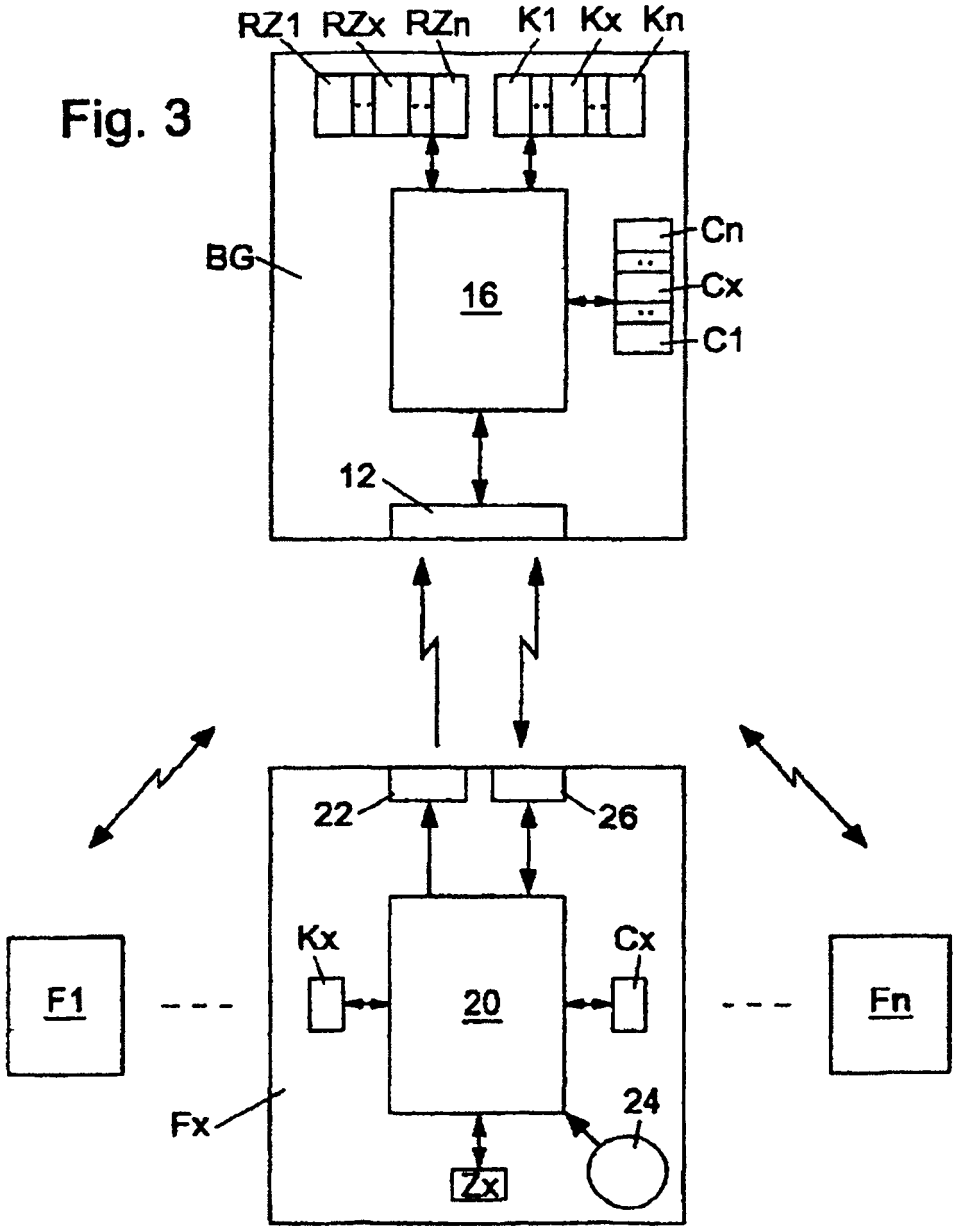
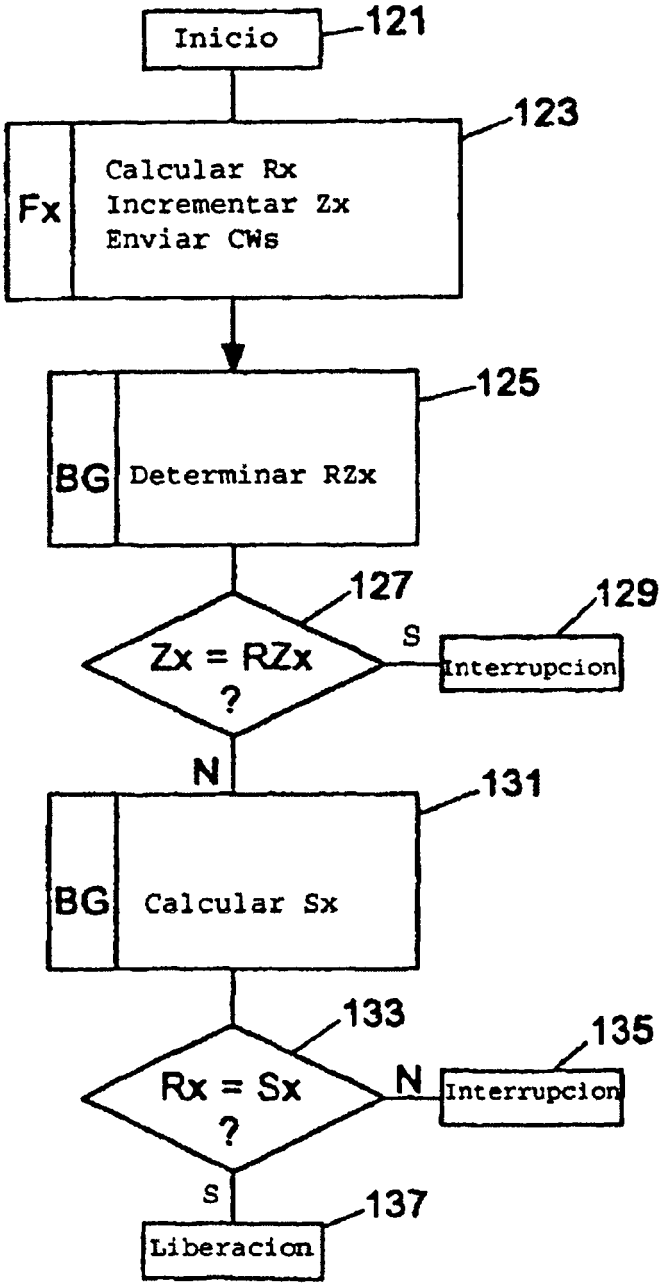


Fig. 4


Inicio
121
123
Fx
Calcular Rx
Incrementar Zx
Enviar CWs
125
BG
Determinar RZx
127
Zx = RZx
?
S
129
Interrupcion
N
131
BG
Calcular Sx
133
Rx = Sx
?
N
135
Interrupcion
S
137
Liberacion