(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 593 831**

(51) Int. CI.:

G05B 19/418 (2006.01)
G05B 19/048 (2006.01)
H04L 12/40 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.02.2014 E 14154711 (7)**

(97) Fecha y número de publicación de la concesión europea: **06.07.2016 EP 2767877**

(54) Título: **Sistema de control y transmisión de datos para transmitir datos relativos a la seguridad a través de un bus de campo**

(30) Prioridad:

13.02.2013 DE 102013101413

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.12.2016

(73) Titular/es:

PHOENIX CONTACT GMBH & CO. KG (100.0%)
Flachsmarktstrasse 8
32825 Blomberg, DE

(72) Inventor/es:

MEYER-GRÄFE, KARSTEN

(74) Agente/Representante:

LOZANO GANDIA, José

SISTEMA DE CONTROL Y TRANSMISIÓN DE DATOS PARA TRANSMITIR DATOS RELATIVOS A LA SEGURIDAD A TRAVÉS DE UN BUS DE CAMPO

DESCRIPCIÓN

La presente invención se refiere a un sistema de control y transmisión de datos para transmitir datos relativos a la seguridad a través de un medio de comunicación.

En la técnica de la automatización es necesario a menudo implementar funciones de seguridad o procesos críticos para la seguridad para proteger a la persona, la máquina o el entorno, con los cuales por ejemplo puede desconectarse una máquina tras abrir una puerta de protección o accionar un interruptor de desconexión en emergencia, o puede llevarse a un estado seguro.

Para ello se sustituyen cada vez más conceptos de seguridad convencionales por funciones de seguridad alojadas en sistemas de automatización a prueba de fallos. Estos sistemas incluyen abonados conectados a prueba de fallos de forma descentralizada a la red de un sistema de bus de automatización, es decir, a un sistema de bus de campo, pudiendo estar realizadas en los abonados por lo general tanto las funciones de seguridad propiamente dichas como también las medidas que detectan las faltas y que dominan las faltas.

En instalaciones automatizadas actuales se utilizan en función del grado de automatización y de la extensión de las instalaciones sistemas de comunicación que conectan los aparatos de entrada/salida (aparatos E/S) descentralizados y sistemas de control. Los aparatos de E/S y los sistemas de control pueden ser tanto abonados estándar como también abonados con funciones de seguridad. Para el transporte de datos relativos a la seguridad a través de sistemas de comunicación comunes se conoce el apoyo de la red mediante protocolos de red seguros. El control de funciones estándar y de funciones de seguridad puede realizarse a través de una red común tanto mediante una estructura central con un sistema de control estándar y de seguridad como también mediante sistemas lógicos de control y seguridad descentralizados, que se encuentran distribuidos en la red de un sistema de comunicación o bien de bus de campo y que controlan procesos críticos para la seguridad con independencia entre sí.

Por el documento EP 1 887 444 A1 se conoce un sistema para el control de procesos en el que al menos un equipo de proceso a controlar se controla mediante al menos un módulo de proceso y al menos un módulo de seguridad, combinando lógicamente entre sí señales de proceso no relevantes para la seguridad del módulo de procesos y señales de seguridad relativas a la seguridad del proceso del módulo de seguridad. Para poder realizar una función de desconexión rápida, se conduce una señal de seguridad local de un sensor de seguridad local, puenteando esta combinación lógica, a través de un circuito de conexión rápida a una salida de control de una unidad de control local asociada al equipo de proceso.

Por el documento DE 198 01 137 A1 se conoce un sistema de automatización que presenta una unidad de entrada a prueba de fallos y una unidad de salida a prueba de fallos. La unidad de entrada a prueba de fallos transmite en instantes predeterminados un telegrama a la unidad de salida a prueba de fallos, evaluando la unidad de salida a prueba de fallos la recepción continua del telegrama como indicio de una relación de comunicación intacta y trasladando caso contrario una periferia que esté conectada a un estado seguro.

Por el documento EP 2 202 599 A2 se conoce un sistema de control industrial para una instalación industrial automatizada, en el que el sistema de control industrial puede asumir un primer y un segundo modo de servicio, alimentándose con energía en el primer modo de servicio y en el segundo modo de servicio distintos grupos de componentes del sistema de control industrial.

Un sistema de control para controlar procesos críticos para la seguridad con al menos un equipo de control seguro descentralizado, desplazado de un sistema de control estándar, se conoce por ejemplo por el documento EP 1 188 096 B1. En el sistema de control conocido es competente el equipo de control seguro dispuesto descentralizado exclusivamente para el control del proceso crítico para la seguridad que tiene asignado. Esto significa que el mismo controla el proceso crítico para la seguridad independientemente de otros sistemas de control, en particular independientemente de un equipo de control estándar.

Este sistema de control conocido tiene el inconveniente de que islas de seguridad descentralizadas, que son procesos críticos para la seguridad descentralizados, no pueden controlarse de manera sencilla y rápida, tal como demandan algunas aplicaciones.

Además ha llegado al mercado en los últimos años un sistema de control bajo la denominación “Safety-Bridge” (puente de seguridad), que hace posible descentralizar el tratamiento de procesos relevantes para la seguridad, sin que para ello sea necesario un sistema de control de seguridad explícito. Un módulo de entrada de seguridad genera entonces una señal relevante para la seguridad, en la que se transmite a un sistema de control central un dato de seguridad, por ejemplo una información del estado de sensores seguros. El sistema de control central copia solamente los datos recibidos relativos a la seguridad en un módulo de salida seguro predeterminado. El módulo de salida desempaqueta los datos relativos a la seguridad y realiza la evaluación relevante para la seguridad de los datos. Además puede enviar el módulo de salida seguro por su parte datos a través del sistema de

control central a otros abonados descentralizados, con lo que es posible una realización en cascada de procesos de seguridad. Además de los puros datos de proceso, puede transmitir el sistema de control conocido también datos redundantes, que sirven para asegurar la transmisión de los datos relativos a la seguridad.

La invención tiene como objetivo básico lograr un sistema de control y transmisión de datos que sea capaz de controlar procesos o subprocesos críticos para la seguridad con más sencillez y rapidez. Otro objetivo adicional de la invención ha de considerarse que es poder desconectar con rapidez procesos críticos para la seguridad individualmente o varios procesos críticos para la seguridad en forma de grupos en un único ciclo de comunicación y mediante una única orden.

Una idea central de la invención puede considerarse que es la activación de un modo de desconexión rápida con ayuda de un equipo central, como por ejemplo un equipo central de control, para poder desconectar una o varias islas de seguridad, es decir, procesos o subprocesos descentralizados críticos para la seguridad.

El objetivo técnico antes citado puede lograrse mediante las características de la reivindicación 1.

La invención se describirá a continuación más en detalle en base a varios ejemplos de ejecución en relación con los dibujos adjuntos. Se muestra en:

figura 1 un sistema de automatización a modo de ejemplo,
figura 2 una trama sumatoria a modo de ejemplo,
figura 3 un sistema de automatización a modo de ejemplo, en el que se ha llevado a cabo la invención y
figura 4a un telegrama de datos según la invención y
figura 4b una trama sumatoria según la invención, a modo de ejemplo.

La figura 1 muestra un sistema de automatización a modo de ejemplo en forma de un sistema de control y transmisión de datos 10, configurado entre otros para controlar procesos críticos para la seguridad y para controlar procesos no críticos para la seguridad. Al respecto se trata de una forma de ejecución que sirve de ayuda para comprender la invención. El sistema de automatización 10 se describirá a modo de ejemplo en base al sistema Interbus, pudiendo utilizarse también otros sistemas de bus de campo. El Interbus se conoce desde hace desde hace mucho tiempo y se describe extensamente por ejemplo en el libro especializado A. Baginski y colab. Fundamentos y práctica del INTERBUS, 2ª edición revisada, Editorial Hüthig Heidelberg, 1998.

Tal como se muestra en la figura 1, está conectado un equipo de control de orden superior 20 por ejemplo juntamente con un primer equipo de control seguro 40, una unidad de señales segura 50, un segundo equipo de control seguro 80, otra unidad de señales segura 90 y un abonado de bus no seguro 120 a un bus de campo basado en Interbus 30. El equipo de control seguro 40 puede estar configurado para vigilar y controlar mediante la unidad de señales 50 un proceso crítico para la seguridad 70. El equipo de control seguro 80 puede estar configurado para vigilar y controlar mediante la unidad de señales 90 un proceso crítico para la seguridad 110. También puede pensarse en conectar al bus de campo 30 más de dos equipos de control seguros, cada uno de los cuales puede estar conectado con varias unidades de señales, para controlar de manera descentralizada procesos críticos para la seguridad.

El equipo de control de orden superior 20 puede presentar un master de bus 22 estandarizado tradicional, que en el presente ejemplo de ejecución está configurado como master de bus Interbus y que controla de manera conocida la comunicación sobre el bus de campo 30. El equipo de control de orden superior 20 está configurado además para controlar un proceso no seguro 140 de manera centralizada a través del abonado de bus no seguro 120. El abonado del bus no seguro 120 es con preferencia un aparato E/S, que pueden comunicar mediante canales de E/S 130 y 132 con el proceso no crítico para la seguridad 140. En la práctica puede estar conectado el aparato de E/S a través del canal 132 con un actuador (no representado) y a través del canal 130 con un sensor (no representado). El sensor aporta datos sobre el estado del proceso no crítico para la seguridad 140 a través del aparato de E/S 120 al equipo de control de orden superior 20, mientras que el aparato de E/S 120 conduce al actuador los datos de control provenientes del equipo de control de orden superior 20.

Además presenta el equipo de control de orden superior 20 un equipo relativo a la seguridad 24, que puede recibir, evaluar y caso necesario modificar selectivamente datos especiales relativos a la seguridad, con preferencia informaciones de desconexión rápida, de los equipos de control seguros 40 y 80 y/o de las unidades de señal 50 y 90. La forma de funcionamiento exacta del equipo orientado a la seguridad 24 se describirá extensamente más tarde.

El primer equipo de control seguro 40 está conectado mediante una interfaz de bus 42 al bus de campo 30. La interfaz de bus 42 puede ser una interfaz de bus tradicional basada en Interbus. Además presenta el primer equipo de control 40 un equipo relativo a la seguridad 44, configurado para garantizar con un equipo relativo a la seguridad 54 de la unidad de señales 50, de manera de por sí conocida, una comunicación a prueba de fallos. La unidad de señales 50 presenta a su vez una interfaz de bus 52, a través de la cual puede comunicar la unidad de señales 50 con el primer equipo de control 40, el equipo de control de orden superior 20 y los demás abonados de bus.

El primer equipo de control 40 puede estar configurado para proporcionar a través del bus de campo 30 primeros datos relativos a la seguridad para la unidad de señales 50, para controlar el proceso crítico para la seguridad 70. El equipo de control seguro 40 es con preferencia capaz además de proporcionar segundos datos relativos a la seguridad, que son datos especiales relativos a la seguridad y transmitirlos al equipo de control de orden superior 20, para posibilitar un control centralizado, en particular una desconexión rápida del proceso crítico para la seguridad 70.

El proceso crítico para la seguridad 70 está conectado mediante canales de E/S 60 y 62 con una entrada segura y una salida segura a la unidad de señal 50. En la práctica puede estar conectada la unidad de señales 50 a través del canal 62 con un actuador (no representado) y a través del canal 60 con un sensor (no representado). El sensor aporta datos sobre el estado del proceso crítico para la seguridad 70 a través de la unidad de señales 50 al equipo de control de orden superior 20 y/o al primer equipo de control seguro 40, mientras que la unidad de señales 50 puede aportar al actuador los datos especiales relativos a la seguridad procedentes del equipo de control de orden superior 20 y/o los datos relativos a la seguridad proporcionados por el primer equipo de control 40.

La unidad de señales 50 puede presentar también varias entradas y salidas seguras, que están conectadas mediante canales de E/S con el proceso crítico para la seguridad 70.

Señalemos aquí que el primer equipo de control 40, la unidad de señales 50 y el proceso crítico para la seguridad 70 pueden denominarse también isla de seguridad.

El segundo equipo de control seguro 80 está conectado a través de una interfaz de bus 82 al bus de campo 30. La interfaz de bus 82 puede ser una interfaz de bus tradicional basada en Interbus. Además presenta el segundo equipo de control 80 un equipo relativo a la seguridad 84, configurado para garantizar con un equipo relativo a la seguridad 94 de la unidad de señales 90, de manera de por sí conocida, una comunicación a prueba de fallos. La unidad de señales 90 presenta a su vez una interfaz de bus 92, a través de la cual puede comunicar la unidad de señales 90 con el segundo equipo de control 80, el equipo de control de orden superior 20 y los demás abonados de bus.

El segundo equipo de control 80 puede estar configurado para proporcionar a través del bus de campo 30 primeros datos relativos a la seguridad para la unidad de señales 90, para controlar el proceso crítico para la seguridad 110. El equipo de control seguro 80 es además con preferencia capaz de proporcionar segundos datos relativos a la seguridad, que son datos especiales relativos a la seguridad y transmitirlos al equipo de control de orden superior 20, para hacer posible un control centralizado, en particular una desconexión rápida del proceso crítico para la seguridad 110.

El proceso crítico para la seguridad 110 está conectado mediante canales de E/S 100 y 102 con una entrada segura y una salida segura de la unidad de señales 90. En la práctica puede estar conectada la unidad de señales 90 a través del canal 102 con un actuador (no representado) y a través del canal 100 con un sensor (no representado). El sensor aporta datos de estado del proceso crítico para la seguridad 110 a través de la unidad de señales 90 al equipo de control de orden superior 20 y/o al primer equipo de control seguro 80, mientras que la unidad de señales 90 puede aportar al actuador los datos especiales relativos a la seguridad procedentes del equipo de control de orden superior 20 y/o los datos relativos a la seguridad proporcionados por el segundo equipo de control 80.

La unidad de señales 90 puede presentar también varias entradas y salidas seguras, que están conectadas mediante canales de E/S con el proceso crítico para la seguridad 110.

Señalemos aquí que el segundo equipo de control 80, la unidad de señales 90 y el proceso crítico para la seguridad 110 pueden denominarse también isla de seguridad.

Para asegurar que los segundos datos relativos a la seguridad también llegan realmente del equipo de control de orden superior 20 y se han retransmitido correctamente, puede estar configurado el equipo de control de orden superior 20, es decir, con preferencia el equipo relativo a la seguridad 24, para generar datos dinámicos y transmitir los mismos a los equipos de control seguros 40 y 80 y/o directamente a las unidades de señal 50 y 90. Los equipos de control seguros 40 y 80 y/o las unidades de señales 50 y 90 están configurados/as entonces correspondientemente para detectar si los datos dinámicos se han generado según definición. Caso negativo, provocan las unidades de señales 50 y 90 que el proceso crítico para la seguridad 70 y/o el proceso crítico para la seguridad 110 se traslade/n a un estado seguro. También puede pensarse en que las unidades de señal 50 y 90 o los equipos de control seguros 40 y 80 generen datos dinámicos, transmitan los mismos al equipo de control de orden superior 20 y a continuación evalúen los datos dinámicos modificados por el equipo de control de orden superior 20 y reaccionando a los datos dinámicos modificados, activen etapas definidas.

A continuación se describirá más en detalle el funcionamiento del sistema de control 10 mostrado en la figura 1 en relación con la figura 2.

Al ser el bus de campo 30 puesto como ejemplo, tal como se ha mencionado al principio, el Interbus con forma anular, están configurados el master de bus 22 y las interfaces de bus 42, 52, 82, 92 y 122 para hacer posible

una transmisión bidireccional de datos de entrada y salida de todos los abonados mediante las llamadas tramas sumatorias. Una trama sumatoria 150 a modo de ejemplo con una ampliación correspondiente a la invención se representa en la figura 2.

Según el protocolo de comunicación de Interbus, comienza cada trama sumatoria colocada por el master de bus 22 en el bus de campo 30 con un campo de datos 210, en el que está inscrita una loopbackword (palabra de retorno al bucle) LBW. A la loopbackword le siguen otros campos de datos 200 a 160, que están asociados inequívocamente a los abonados del bus conectados al bus de campo 30, en función de su correspondiente posición física en el bus de campo 30. En el sistema de automatización 10 mostrado está asociado el campo de datos 200 al abonado de bus 120, el campo de datos 190 a la unidad de señales 90, el campo de datos 180 al equipo de control seguro 80, el campo de datos 170 a la unidad de señales 50 y el campo de datos 160 al equipo de control seguro 40.

En una forma de ejecución preferente están divididos los campos de datos 170 y 190 respectivamente asociados a las unidades de señales 50 y 90, cada uno en tres subcampos. Solamente se representa detalladamente en la figura 2 el campo de datos 170, dividido en tres subcampos 171, 172 y 173. El equipo orientado a la seguridad 44 del equipo de control seguro 40 puede escribir en el subcampo 171 primeros datos relativos a la seguridad y en el subcampo 172 segundos datos relativos a la seguridad, que están destinados al equipo de control de orden superior 20. En el subcampo 173 puede escribir el equipo orientado a la seguridad 44 del equipo de control 40 o el equipo orientado a la seguridad 54 de la unidad de señales 50 datos dinámicos, que pueden transmitirse para su evaluación y procesamiento igualmente al equipo de control de orden superior 20.

De manera similar puede escribir el equipo orientado a la seguridad 84 del segundo equipo de control 80 en un primer subcampo del campo de datos 190 primeros datos relativos a la seguridad y en un segundo subcampo del campo de datos 190 segundos datos relativos a la seguridad, destinados al equipo de control de orden superior 20. En un tercer subcampo del campo de datos 190 puede escribir el equipo orientado a la seguridad 84 del equipo de control 80 o el equipo orientado a la seguridad 94 de la unidad de señales 90 datos dinámicos, que pueden transmitirse para su evaluación y procesamiento igualmente al equipo de control de orden superior 20.

Los datos especiales relativos a la seguridad que pueden transmitirse en los segundos subcampos de los campos de datos 170 y 190 contienen con preferencia un único bit de información, que según una implementación ventajosa puede ser colocado en cero por el equipo de control seguro 40 u 80 respectivamente o la unidad de señales 50 ó 90 respectivamente.

Supongamos ahora que el sistema de automatización 20 funciona correctamente y que no se ha presentado ningún fallo.

En consecuencia no tienen que activar los equipos de control seguros 40 y 80 ninguna función de seguridad mediante las unidades de señales 50 y 90 respectivamente. El equipo relativo a la seguridad 44 del primer equipo de control 40 escribe en este caso un cero en el subcampo 172 destinado a la unidad de señales 50 y como dato dinámico por ejemplo un número predeterminado en el subcampo 173, mientras que el equipo relativo a la seguridad 84 del equipo de control seguro 80 escribe un cero en el segundo subcampo del campo de datos 190 destinado a la unidad de señales 90 e igualmente un número predeterminado en el tercer subcampo del campo de datos 190.

De manera de por sí conocida pueden además recibir todos los abonados conectados al bus de campo 30 datos de salida de otros abonados y escribir datos de entrada en los campos de datos a ellos asociados y transmitirlos al equipo de control de orden superior 20 o a otros abonados conectados al bus de campo 30. El equipo de control de orden superior 20 o bien su equipo relativo a la seguridad 24 está configurado para evaluar los segundos y terceros campos de datos de los campos de datos 170 y 190 selectivamente, es decir, en particular modificarlos de forma definida y transmitirlos con la siguiente trama sumatoria a las unidades de señales 50 y 90. En función de la implementación sustituye el equipo relativo a la seguridad 24 del equipo de control de orden superior 20 por ejemplo el cero trasmitido en los segundos subcampos de los campos de datos 170 y 190 por un uno, mientras que el número predeterminado trasmitido en los terceros subcampos de los campos de datos 170 y 190 se incrementa por ejemplo en el valor 1.

Los equipos relativos a la seguridad 54 y 94 de las correspondientes unidades de señales leen los segundos y terceros subcampos de los campos de datos 170 y 190 respectivamente, a ellos asociados, y detectan en base al número modificado contenido en el tercer subcampo que los segundos datos relativos a la seguridad contenidos en el segundo subcampo proceden del equipo de control de orden superior 20 y han sido transmitidos correctamente. Como reacción al uno contenido en el correspondiente segundo subcampo, detecta la unidad de señales 50 y 90 respectivamente que deben seguir corriendo los procesos críticos para la seguridad 70 y 110.

Supongamos ahora que el sistema de automatización 10 o bien una persona de servicio ha comunicado al equipo de control de orden superior 20 que los procesos críticos para la seguridad 70 y 110 deben desconectarse inmediatamente. En este caso se ocupa el equipo relativo a la seguridad 24 de que en los segundos subcampos de los campos de datos 170 y 190 de la siguiente trama sumatoria se escriban respectivos ceros y los datos dinámicos contenidos en el tercer subcampo se modifiquen de una forma predeterminada.

Los equipos relativos a la seguridad 54 y 94 de las unidades de señales 50 y 90 respectivamente, leen los segundos y terceros subcampos a ellos asignados de los campos de datos 170 y 190 respectivamente y detectan en base al número modificado contenido en el tercer subcampo que los datos especiales relativos a la seguridad contenidos en el respectivo segundo subcampo proceden del equipo de control de orden superior 20 y se han transmitido correctamente. Como reacción al cero contenido en el correspondiente segundo subcampo, detecta la unidad de señales 50 y 90 respectivamente que los procesos críticos para la seguridad 70 y 110 deben desconectarse inmediatamente. Por ello se colocan a continuación inmediatamente en cero las correspondientes salidas seguras de las unidades de señales 50 y 90 y se desconectan los procesos críticos para la seguridad 70 y 110. De esta manera se vigilan centralmente los procesos descentralizados críticos para la seguridad 70 y 110. Esto significa que el equipo de control de orden superior 20 siempre vigila los equipos de control seguros 40 y 80. Los equipos de control seguros 40 y 80 no pueden por lo tanto ya intervenir independientemente del equipo de control de orden superior 20 en los procesos críticos para la seguridad.

También puede pensarse en que el equipo relativo a la seguridad 24 del equipo de control de orden superior 20 genere datos dinámicos y los escriba en los correspondientes terceros subcampos de los campos de datos 170 y 190, destinados al primer equipo de control 40 y al segundo equipo de control 80.

Señalemos aquí que el equipo de control de orden superior 20 puede estar constituido para modificar selectivamente en cada ciclo de comunicación los segundos datos relativos a la seguridad transmitidos en los segundos subcampos de los campos de datos 170 y 190, para evitar que los procesos críticos para la seguridad 70 y 110 tengan una desconexión rápida no deseada.

También puede pensarse en que fuentes de información, que son por ejemplo los equipos de control seguros 40 y 80 y/o las unidades de señales 50 y 90, se trasladen a un estado de casi-seguridad, en el que los mismos dejan correr el proceso crítico para la seguridad 70 y el proceso crítico para la seguridad 110 respectivamente. Los procesos críticos para la seguridad 70 y 110 envían entonces por su parte al equipo de control seguro 40 y 80 respectivamente la información de que se ha solicitado una desconexión rápida. Los equipos de control seguros 40 y 80 o las correspondientes unidades de señales 50 y 90 deben entonces anular las informaciones asociadas a los mismos que contienen la información de desconexión rápida en el segundo subcampo del campo de datos 170 y 180 respectivamente. El estado de casi-seguridad puede mantenerse hasta que ha transcurrido un tiempo máximo de reacción ajustado en los equipos de control 40 y 80 o en las unidades de señales 50 y 90. En este caso cambia el equipo de control 40 y 80 respectivamente del estado de casi-seguridad al estado de seguridad.

De esta manera es posible una desconexión rápida de componentes seguros individuales o grupos de componentes seguros sin que tenga que preverse una costosa programación en los equipos de control descentralizados 40 y 80.

En lugar de informaciones de desconexión rápida, que se escriben en los segundos subcampos de los campos de datos 170 y 190 de cada trama sumatoria, podría colocar el equipo de control de orden superior 20 también cíclicamente una información de broadcast (radiodifusión) que contiene la información de desconexión rápida. Los equipos de control seguros 40 y 80 y/o las unidades de señales 50 y 90 evalúan a continuación estas informaciones.

Los equipos de control seguros 40 y 80 y/o las unidades de señales 50 y 90 pueden además estar configurados/as para confirmar una desconexión rápida activada en la siguiente trama sumatoria, lo cual puede originar un aumento adicional de la seguridad.

Un aspecto de la invención puede considerarse que es que una fuente de información, por ejemplo una unidad de señales segura añada, junto a primeros datos relativos a la seguridad, también segundos datos relativos a la seguridad para la desconexión rápida de islas individuales relevantes para la seguridad. Los segundos datos relativos a la seguridad llegan a un control de orden superior, que evalúa estos datos y los modifica selectivamente. Con preferencia incluyen los segundos datos relativos a la seguridad un bit de información, que de manera estándar es colocado por la unidad de señales en cero. En el equipo de control de orden superior se coloca el bit de información recibido en uno y a continuación se transmite a una determinada salida segura, que también puede denominarse sumidero de información. El sumidero de información evalúa de manera de por sí conocida los primeros datos relativos a la seguridad.

Adicionalmente comprueba el mismo las segundas informaciones relativas a la seguridad asociadas y coloca dado el caso todas o algunas de las distintas salidas seguras en cero, con lo que el correspondiente proceso crítico para la seguridad puede ser conducido mediante un sistema de control central a un estado seguro.

La figura 3 muestra como sistema de control y transmisión de datos 310 un sistema de automatización a modo de ejemplo, configurado entre otros para controlar procesos críticos para la seguridad 432, 434 y 436, dado el caso de al menos un proceso no crítico para la seguridad 438 y para transmitir datos relativos a la seguridad a través de un medio de comunicación 330. El sistema de control y transmisión de datos 310 presenta varias unidades de señales seguras, habiéndose representado en la figura 3 a modo de ejemplo tres unidades de señales seguras 340, 360, 380. Cada una de las unidades de señales seguras 340, 360, 380 está conectada mediante al menos una

salida y/o al menos una entrada con un proceso crítico para la seguridad. El proceso crítico para la seguridad pueden ser también subprocesos críticos para la seguridad o islas de seguridad, asociadas a respectivas unidades de señales seguras 340, 360, 380. Cada unidad de señales segura puede presentar por ejemplo una entrada y dos salidas, a través de las cuales está conectada la misma por ejemplo con un subproceso crítico para la seguridad.

Las unidades de señales seguras 340, 360 y 380 están conectadas al medio de comunicación 330. Además está conectado al menos un equipo central 320 y/o 420 al medio de comunicación 330. Las unidades de señales seguras 340, 360, 380 presentan respectivos equipos de seguridad 343, 363 y 383 y están configuradas cada una para proporcionar datos relativos a la seguridad y transmitir esos datos a través del medio de comunicación 330. Cada unidad de señales segura 340, 360, 380 está configurada para proporcionar una señal definida, previamente ajustada, con preferencia una palabra de un solo bit. La señal definida puede ser un cero lógico. Para ello puede estar implementado en cada unidad de señales segura un equipo de control y evaluación 342, 362 y 382. Tanto la señal definida como también los datos relativos a la seguridad se transmiten al equipo central 320 y/o 420. El equipo central 320 y/o 420 está configurado para evaluar sólo la señal definida y en función de la señal definida evaluada, generar una orden de control central y transmitir la orden de control central junto con los datos relativos a la seguridad a al menos una unidad de señales segura predeterminada de las varias unidades de señales seguras 340, 360, 380. La orden de control central es con preferencia igualmente una palabra de un solo bit. Al menos la unidad de señales segura predeterminada está configurada para evaluar los datos relativos a la seguridad y la orden de control central, para controlar al menos una parte del proceso crítico para la seguridad.
La evaluación de la orden de control central puede realizarse en el correspondiente equipo de control y evaluación 342, 362 y/o 382, mientras que pueden evaluarse datos relativos a la seguridad en el correspondiente equipo de seguridad 343, 363 y/o 383, de manera de por sí conocida.

Gracias a la utilización de una señal definida, que con preferencia se transmite en cada ciclo de comunicación al equipo central y allí se evalúa y se modifica de una forma predeterminada, puede realizarse un control central y seguro, con lo que procesos descentralizados, críticos para la seguridad, que según el documento EP 1 188 096 B1 solo pueden controlarse independientemente y descentralizadamente uno de otro, pueden controlarse ahora también centralmente.

Las unidades de señales seguras pueden ser aparatos de entrada y/o salida, también conocidos como abonados de bus de E/S ó I/O. Una tal unidad de señales segura es capaz por ejemplo de recibir datos de entrada de sensores de un proceso crítico para la seguridad, transformarlos en un equipo de seguridad, de una manera de por sí conocida, en datos relativos a la seguridad y retransmitir los datos relativos a la seguridad al equipo central, así como transmitir señales de salida a actuadores que controlan el proceso crítico para la seguridad. No obstante, las unidades de señales seguras no tienen que estar constituidas iguales o similares. Así pueden tener las mismas por ejemplo un número diferente de entradas y salidas.

Señalemos que los datos relativos a la seguridad de una unidad de señales segura pueden utilizarse para controlar el proceso crítico para la seguridad independientemente del equipo central. El equipo central puede ser un equipo de control de orden superior en forma de un master de bus o de un módulo de conexión. El equipo central puede estar implementado también como equipo de vigilancia.

A continuación se entenderán bajo datos relativos a la seguridad con preferencia datos que contienen tanto los datos de entrada por ejemplo de un sensor como también datos relevantes para la seguridad, como por ejemplo una suma de comprobación, que permiten una transmisión a prueba de fallos de los datos de entrada.

Como medio de comunicación puede utilizarse un bus de campo, como por ejemplo el Interbus, bus CAN o Profibus o un sistema basado en Ethernet.

El Interbus es conocido desde hace mucho tiempo y se describe extensamente en el libro especializado A. Baginski y colab. Fundamentos y práctica del INTERBUS, 2ª edición revisada, Editorial Hüthig Heidelberg, 1998.

Tal como se muestra en la figura 3 a modo de ejemplo, están conectados el equipo central 320 mediante una interfaz de comunicación 322 y adicional o alternativamente un equipo central 420 a través de una interfaz de comunicación 422 al medio de comunicación 330. El equipo central 320 puede ser un equipo de control de orden superior, mientras que el equipo central 420 puede ser un equipo de vigilancia.

Al medio de comunicación 330 están conectadas las unidades de señales seguras 340, 360 y 380, así como por ejemplo una unidad de señales no segura 400. Las unidades de señales pueden denominarse abonados de bus. Solamente para simplificar la representación se representan sólo tres unidades de señales seguras y una unidad de señales no segura 400.

Las unidades de señales seguras 340, 360 y 380 están asociadas por ejemplo a respectivos subprocesos críticos para la seguridad 432, 434 y 436, mientras que la unidad de señales no segura 400 puede estar asociada a un subproceso no crítico para la seguridad 438. En el ejemplo de ejecución mostrado en la figura 3 forman los subprocesos 432, 434, 436 y 438 un proceso completo 430. También puede pensarse en que estén unidas cada unidad de señales segura y cada unidad de señales no segura con un proceso crítico para la seguridad y un proceso no crítico para la seguridad respectivamente, que no dependen uno de otro.

El equipo de control de orden superior 320 puede presentar un master de bus 324 estandarizado tradicional, que puede estar configurado como master de bus Interbus y que puede controlar la comunicación sobre el medio de comunicación 330 de manera de por sí conocida. El equipo de control de orden superior 320 está configurado además para controlar centralmente el proceso no crítico para la seguridad 438 mediante la unidad de señales no segura 400.

La unidad de señales segura 340 presenta por ejemplo una salida o módulo de salida 344, que mediante un canal de salida 350 está conectada/o con el proceso crítico para la seguridad 432. Por ejemplo está conectado a la salida 344 un contactor (no mostrado), mediante el cual puede conectarse el proceso crítico para la seguridad 432, por ejemplo una máquina para un proceso de doblado, a una alimentación de energía (no mostrada). La salida 344 está conectada con un equipo de control y evaluación 342, que a su vez está conectado con una interfaz de comunicación 341. El equipo de control y evaluación 342 puede estar configurado para generar una señal definida, previamente ajustada, con preferencia un cero lógico y trasmitir esta señal al equipo central 320 ó 420. El sentido y la finalidad de la señal definida se describirán más abajo. Mediante la interfaz de comunicación 341 está conectada la unidad de señales segura 340 al medio de comunicación 330, para poder comunicar con el equipo central 320, el equipo central 420 y/o las demás unidades de señales. La unidad de señales 340 presenta además un equipo de seguridad 343, que está conectado con una entrada 345 y una salida 346. La entrada 345 y la salida 346 pueden también denominarse módulo de entrada de seguridad y módulo de salida de seguridad respectivamente. La entrada 345 puede estar conectada mediante un canal de entrada 351 con un sensor, por ejemplo un interruptor de desconexión en emergencia (no representado) dentro del proceso crítico para la seguridad 432. La salida 346 puede estar conectada mediante un canal de salida 352 con un actuador (no representado), con cuya ayuda puede llevarse el subproceso crítico para la seguridad a un estado seguro. Por ejemplo se lleva una máquina a funcionar sólo en vacío. Además está conectado el equipo de seguridad 343 con la interfaz de comunicación 341 y el equipo de control y evaluación 342. En función de la implementación de la unidad de señales 340 puede estar conectado el equipo de seguridad 343 también con la salida 344. La forma de funcionamiento del equipo de seguridad 343 es conocida de por sí. El mismo puede generar a partir de los datos de entrada recibidos en la entrada 345 datos relativos a la seguridad, añadiendo por ejemplo una suma de comprobación a los datos de entrada. El equipo de seguridad 343 garantiza así de manera de por sí conocida una comunicación a prueba de fallos a través del medio de comunicación 300. Señalemos que los datos relativos a la seguridad se transmiten sin manipulación mediante el equipo central 320 ó 340 a través del medio de comunicación.

Además puede evaluar el equipo de seguridad 343 los datos relativos a la seguridad recibidos a través del medio de comunicación 330 y generar las correspondientes señales de salida y conducir las mismas selectivamente a una salida, por ejemplo la salida 346, para iniciar una función de seguridad. También puede pensarse en que el equipo de seguridad 343 esté implementado al menos parcialmente en la entrada 345 y/o la salida 346.

La unidad de señales segura 360 presenta por ejemplo una salida o módulo de salida 364, que a través de un canal de salida 370 está conectada/o con el proceso crítico para la seguridad 434. Por ejemplo puede estar conectado a la salida 364 un contactor (no mostrado), mediante el cual el proceso crítico para la seguridad 434, por ejemplo una máquina para un proceso de taladrado, puede conectarse a una fuente de energía (no representada). La salida 364 está conectada con un equipo de control y evaluación 362, que a su vez está conectado con una interfaz de comunicación 361. El equipo de control y evaluación 362 puede estar configurado al respecto para generar una señal definida previamente ajustada, con preferencia un cero lógico y trasmitir esta señal al equipo central 320 ó 420. El sentido y la finalidad de la señal definida se describirán con posterioridad. Mediante la interfaz de comunicación 361 está conectada la unidad de señales 340 con el medio de comunicación 330, para poder comunicar con el equipo central 320, el equipo central 420 y/o las demás unidades de señales. La unidad de señales 360 presenta además un equipo de seguridad 363, que está conectado con una entrada 365 y una salida 366. La entrada 345 puede estar conectada mediante un canal de entrada 371 con un sensor, por ejemplo una rejilla de protección (no representada) dentro del proceso crítico para la seguridad 434. La salida 366 puede estar conectada mediante un canal de salida 372 con un actuador (no representado), con cuya ayuda puede llevarse el subproceso crítico para la seguridad 434 a un estado seguro. Por ejemplo se lleva una máquina a funcionar sólo en vacío. Además está conectado el equipo de seguridad 363 con la interfaz de comunicación 361 y el equipo de control y evaluación 362. En función de la implementación de la unidad de señales 360, puede estar conectado el equipo de seguridad 363 también con la entrada 364. La forma de funcionamiento del equipo de seguridad 363 es de por sí conocida. El mismo puede generar a partir de los datos de entrada recibidos en la entrada 365 datos relativos a la seguridad, añadiendo por ejemplo una suma de comprobación a los datos de entrada. El equipo de seguridad 363 garantiza así de manera de por sí conocida una comunicación a prueba de fallos a través del medio de comunicación 330. Señalemos que los datos relativos a la seguridad se transmiten sin manipulación mediante el equipo central 320 ó 340 a través del medio de comunicación. Además puede evaluar el equipo de seguridad 364 los datos relativos a la seguridad recibidos a través del medio de comunicación 330 y generar las correspondientes señales de salida y conducir las mismas selectivamente a una salida, por ejemplo la salida 366, para iniciar una función de seguridad. Puede pensarse en que el equipo de seguridad 363 esté implementado al menos parcialmente en la entrada 365 y/o la salida 366.

La unidad de señales segura 380 presenta por ejemplo una salida o módulo de salida 384, que está conectada/o a través de un canal de salida 390 con el proceso crítico para la seguridad 436. Por ejemplo puede estar conectado a la salida 384 un contactor (no mostrado), mediante el cual el proceso crítico para la seguridad

436, por ejemplo una máquina para un proceso de doblado, puede conectarse a una fuente de energía (no representada). También puede pensarse en que por ejemplo la salida 384 esté conectada con un interruptor central (no representado), con cuya ayuda se desconecta el proceso completo 430, es decir, puede separarse de la fuente de energía. La salida 384 está conectada con un equipo de control y evaluación 382, que a su vez está conectado con una interfaz de comunicación 381. El equipo de control y evaluación 382 puede estar configurado al respecto para generar una señal definida previamente ajustada, con preferencia un cero lógico y trasmitir esta señal al equipo central 320 ó 420. El sentido y la finalidad de la señal definida se explicarán con posterioridad. Mediante la interfaz de comunicación 381 está conectada la unidad de señales 380 segura con el medio de comunicación 330, para poder comunicar con el equipo central 320, el equipo central 420 y/o las demás unidades de señales. La unidad de señales 380 presenta además un equipo de seguridad 383, que está conectado con una entrada 385 y una salida 386. La entrada 385 puede estar conectada mediante un canal de entrada 391 con un sensor, por ejemplo una rejilla de protección, sensor de temperatura o medidor de la velocidad de giro (no representados) dentro del proceso crítico para la seguridad 436. La salida 386 puede estar conectada mediante un canal de salida 352 con un actuador (no representado), con cuya ayuda puede llevarse el subproceso crítico para la seguridad 436 a un estado seguro. Por ejemplo se opera una máquina sólo en vacío. Además está conectado el equipo de seguridad 383 con la interfaz de comunicación 381 y el equipo de control y evaluación 382. En función de la implementación de la unidad de señales 380, puede estar conectado el equipo de seguridad 383 también con la entrada 384. La forma de funcionamiento del equipo de seguridad 383 es de por sí conocida. El mismo puede generar a partir de los datos de entrada recibidos en la entrada 385 datos relativos a la seguridad, añadiendo por ejemplo una suma de comprobación a los datos de entrada. El equipo de seguridad 383 garantiza así de manera de por sí conocida una comunicación a prueba de fallos a través del medio de comunicación 330. Señalemos que los datos relativos a la seguridad se transmiten sin manipulación mediante el equipo central 320 ó 340 a través del medio de comunicación. Además puede evaluar el equipo de seguridad 383 los datos relativos a la seguridad recibidos a través del medio de comunicación 330 y generar las correspondientes señales de salida y conducir las mismas selectivamente a una salida, por ejemplo la salida 386, para iniciar una función de seguridad. También puede pensarse en que el equipo de seguridad 383 esté implementado al menos parcialmente en la entrada 385 y/o la salida 386.

Señalemos aquí que cada uno de los equipos de seguridad 343, 363 y 383 está configurado con preferencia para no evaluar y no procesar los datos relativos a la seguridad transmitidos a la correspondiente unidad de señales segura 340, 360 y 380 respectivamente cuando la correspondiente unidad de señales segura ha recibido una orden de desconexión del equipo central 320 ó 420. En este caso se desconecta el correspondiente proceso crítico para la seguridad sólo como reacción a la orden de desconexión.

La unidad de señales no segura 400 presenta por ejemplo una entrada 402, a la que puede estar conectado mediante un canal de entrada 410 un sensor (no representado) del proceso no crítico para la seguridad 438. A una entrada 403 puede estar conectado mediante un canal de salida 411 un actuador (no representado) del proceso no crítico para la seguridad. Mediante una interfaz de comunicación 401 está conectada la unidad de señales no segura 400 al medio de comunicación 330.

Señalemos aquí que la unidad de señales segura 340 y el proceso crítico para la seguridad 432 también pueden denominarse isla de seguridad. De manera similar puede formar también la unidad de señales 360 y el proceso crítico para la seguridad 434, así como la unidad de señales 380 y el proceso crítico para la seguridad 436, otras respectivas islas de seguridad.

Señalemos además que las interfaces de comunicación 322, 422, 341, 361, 381 y 401 pueden ejecutaren función del medio de comunicación utilizado, por ejemplo la función de interfaces de bus tradicionales basadas en Interbus o de interfaces de comunicación basadas en Ethernet.

Para que las unidades de señales seguras 340, 360 y 380 puedan comprobar si la orden de control central procedente del equipo central 320 ó 420 también procede en realidad del correspondiente equipo central y se ha transmitido correctamente, puede estar configurado el equipo central 320 ó 340 para generar datos dinámicos de manera definida y trasmitirlos a las unidades de señales seguras 340, 360 y 380. Las unidades de señales seguras están configuradas para detectar si los datos dinámicos se han generado según definición. En caso negativo, se ocupan las unidades de señales seguras de que el correspondiente proceso crítico para la seguridad 432, 434 y/o 436 se conduzca a un estado seguro. También puede pensarse en que las unidades de señales seguras 340, 360, 380 generen datos dinámicos de manera definida, los transmitan al equipo central 320 ó 420 y a continuación evalúen los datos dinámicos modificados de manera definida por el equipo central 320 ó 420 y activen etapas definidas como reacción a los datos dinámicos modificados.

A continuación se describirá más en detalle el funcionamiento del sistema de control 10 mostrado en la figura 3, básicamente en relación con la figura 4b.

Supongamos por lo tanto que el medio de comunicación 330 es por ejemplo un Interbus con forma anular, estando configurados el master de bus 324 y las interfaces de comunicación 341, 361, 381 y 401 para hacer posible una transmisión de datos bidireccional de datos de entrada y/o de salida de todas las unidades de señales a través de la llamada trama sumatoria. Una trama sumatoria 450 a modo de ejemplo con una modificación según la invención se representa en la figura 4b.

Según el protocolo de comunicación de Interbus comienza cada trama sumatoria colocada por el master de bus 324 en el bus de campo 330 con un campo de datos 455, en el que está escrita una palabra de loopback LBW. A la palabra de loopback le siguen otros campos de datos 454 a 451, que están inequívocamente asociados a las unidades de señales 340, 360, 380 y 400 conectadas al bus de campo 330, en función de las correspondientes posiciones físicas en el bus de campo 330. En el presente ejemplo de ejecución está asociado el campo de datos 454 a la unidad de señales no segura 400, el campo de datos 453 a la unidad de señales segura 380, el campo de datos 452 a la unidad de señales segura 360 y el campo de datos 451 a la unidad de señales segura 451.

En una forma de ejecución preferente están divididos los campos de datos 451, 452 y 453 asociados a cada una de las unidades de señales seguras 340, 360 y 380 en tres subcampos. Solamente se representan detalladamente en la figura 4b los subcampos del campo de datos 453. Los datos relativos a la seguridad sD se encuentran en el subcampo 453_1, la orden de control central en el subcampo 453_2 y dado el caso datos dinámicos en el subcampo 453_3. Se utilizan datos dinámicos para dar a la correspondiente unidad de señales segura la posibilidad de comprobar si los datos relativos a la seguridad recibidos han sido transmitidos correctamente por el equipo de control de orden superior 320. Cuando se transmite la trama sumatoria al equipo de control de orden superior 320, se encuentra en el subcampo 453_2 la señal definida generada por la unidad de señales segura 380, con preferencia una palabra de un solo bit en forma de un cero lógico. Los datos relativos a la seguridad del subcampo 453_1 pueden contener de manera de por sí conocida, junto a datos de entrada, también una suma de comprobación.

Ahora se considerará un primer escenario, en el que se supone de todas las unidades de señales conectadas al bus de datos y el equipo central 320 funcionan sin fallos y en el proceso completo 430 no se ha presentado ninguna perturbación.

Mientras en el sistema de control y transmisión de datos 320 no se haya presentado ningún fallo, o bien no se haya activado ninguna función de seguridad, como por ejemplo el accionamiento de un interruptor de desconexión en emergencia o la apertura de una puerta de protección, no debe realizarse tampoco ninguna desconexión o desconexión rápida de los procesos orientados a la seguridad. Para asegurar esto puede estar previsto que las unidades de señales seguras 340, 360 y 380 transmitan como señal definida un cero lógico al equipo de control de orden superior 320, que entonces sustituye activamente el cero lógico por un uno lógico, cuando no se ha presentado ningún fallo o bien no ha disparado un proceso crítico para la seguridad. En este caso interviene el equipo de control de orden superior 320 en coincidencia con el principio de corriente de reposo forzosamente en el control de los procesos críticos para la seguridad 432, 434 y 436.

En el escenario que sirve de base escribe por lo tanto cada unidad de señales seguras en el primer subcampo del campo de datos asociado a los mismos datos relativos a la seguridad, que no obstante no activan ninguna función de seguridad. Además escribe cada unidad de señales segura en el segundo subcampo la señal previamente ajustada, por ejemplo un cero lógico.

Este proceso se describirá a continuación más en detalle solamente en cuanto a la unidad de señales segura 380.

Los datos de estado recibidos en la entrada 385 de un sensor asociado al proceso crítico para la seguridad 436, por ejemplo de una rejilla de protección, se conducen al equipo de seguridad 383 y pueden transformarse de una manera de por sí conocida en datos relativos a la seguridad. Los datos del sensor señalizan en el ejemplo de que se trata una rejilla de protección cerrada. Puesto que el equipo de señales 380 funciona sin fallos, genera la unidad de control y evaluación 382 un cero lógico. En función de la implementación pueden escribirse los datos relativos a la seguridad y el cero lógico como señal definida por ejemplo del equipo de control y evaluación 382 o de la interfaz de comunicación 381 en los subcampos 453_1 y 453_2. Señalemos que también la unidad de señales no segura 400 escribe en el campo de datos 454 los datos del sensor recibidos a través de la entrada 402 procedentes del proceso no crítico para la seguridad. Una vez que la trama sumatoria ha recorrido todas las unidades de señal, se transmite la misma al equipo central 320. El equipo central 320 y con preferencia el master de bus 324 están configurados solamente para leer y evaluar el segundo subcampo de los campos de datos 451, 452 y 453, que contiene la correspondiente señal definida. Puesto que se ha supuesto que el equipo central 320 funciona sin fallos, se sobreescribe el cero lógico, que según una implementación ventajosa se interpreta como señal de conexión por las unidades de señales seguras, por un uno lógico en cada segundo subcampo. Esta tarea puede ejecutarla el master de bus 320. En lugar del master de bus 324, podría estar previsto un equipo separado que evalúa y sobreescribe los segundos subcampos. Un 1 lógico impide que las unidades de señales seguras 340, 360 y 380 desconecten el proceso completo o subprocesos asociados. Adicionalmente puede escribir el equipo central 320 en el tercer subcampo de los campos de datos 451 a 453 datos dinámicos, que por ejemplo en cada ciclo de comunicación se incrementan en el valor 1.

El equipo de control de orden superior 320 transmite ahora la trama sumatoria mostrada en la figura 4b a través del bus de campo 330 a las unidades de señales. La evaluación de un campo de datos se describirá de nuevo en cuanto a la unidad de señales segura 380. Según una implementación ventajosa de la unidad de señales segura 380, transfiere la interfaz de comunicación 381 el campo de datos 453 al equipo de control y evaluación 382. El equipo de control y evaluación 382 detecta en el subcampo 453_2 un uno lógico. Como reacción al uno lógico, no aporta el equipo de control y evaluación 382 ninguna señal de desconexión a la salida 384 y transfiere los datos

relativos a la seguridad al equipo de seguridad 383. El equipo de seguridad detecta que no existe ningún fallo o peligro y no aporta correspondientemente ninguna señal de salida en la salida 386. También detectan todas las demás unidades de señales un funcionamiento sin fallos y el proceso completo sigue corriendo.

Según un segundo escenario, supongamos que el equipo de control y evaluación 382 de la unidad de señales segura 380 tiene un fallo y por lo tanto escribe en el subcampo 453_2 un uno lógico, en lugar de la señal definida previamente ajustada, que en el presente ejemplo es un cero lógico. Todas las demás unidades de señales y el proceso completo 430 corren sin fallos. En el siguiente ciclo de comunicación recibe el equipo central 320 ahora la correspondiente trama sumatoria. El equipo central 320, que a su vez evalúa sólo los segundos subcampos, detecta en el subcampo 453_2 un uno lógico. En función de la configuración del sistema puede ocuparse el equipo central 320 de que al menos a una unidad de señales segura predeterminada se transmita una orden central de desconexión. En el presente caso escribe el equipo central 320 en el segundo subcampo de los campos de datos 451 a 453, que están asociados a las unidades de señales seguras 340, 360 y 380, en cada caso un uno lógico. Además escribe el mismo en el campo de datos 454 datos de salida, que contienen igualmente una orden de desconexión. A continuación envía el equipo central 320 la trama sumatoria a las unidades de señales. Los equipos de control y evaluación 342, 362 y 382 de las unidades de señales 340, 360 y 380 respectivamente generan en cada caso, en reacción al cero lógico recibido, una señal de desconexión, que se emite a través de la salida 344, 364 y 384 respectivamente. Las señales de desconexión controlan con preferencia contactores, que desconectan inmediatamente el correspondiente proceso crítico para la seguridad, es decir, los procesos 432, 434 y 436 y lo hacen independientemente de la información que contienen los datos relativos a la seguridad de los primeros subcampos. Por lo tanto puede denominarse el cero lógico transmitido en el segundo subcampo también orden central de desconexión rápida.

Con preferencia están constituidos los equipos de control y evaluación 342, 362 y 382 para dar lugar cuando reciben un cero lógico a que el correspondiente equipo de seguridad 343, 363 y 383 respectivamente no evalúen ni procese los datos relativos a la seguridad recibidos en el primer subcampo.

La unidad de señales no segura 400 retransmite los datos de salida recibidos en el campo de datos 454 a través de la salida 411 por ejemplo a un contactor, que al reaccionar a los datos de salida desconecta el subproceso no crítico para la seguridad 438. De esta manera se desconecta también el subproceso 438 y con ello el proceso completo 430.

Señalemos aquí que la señal definida que puede aportar cada unidad de señales segura también puede ser una señal relativa a la seguridad que puede generarse y evaluarse en el correspondiente equipo de seguridad 343, 363 y 383. Las líneas discontinuas entre los equipos de seguridad 343, 363 y 383 y las salidas 344, 364 y 384 respectivamente indican que una señal definida relativa la seguridad, que puede transmitirse como la señal definida no relativa a la seguridad en el segundo subcampo, puede ser evaluada por el correspondiente equipo de seguridad y a continuación emitida como orden de desconexión rápida a través de la correspondiente salida.

Según un tercer escenario, supongamos que solamente el equipo central 320 está afectado por un fallo y no sobreescribe los segundos subcampos con un uno lógico. Todas las unidades de señales y el proceso completo 430 corren sin fallo.

En un ciclo de comunicación recibe ahora el equipo central 320 la correspondiente trama sumatoria y evalúa a su vez sólo los segundos subcampos. Desde luego el mismo no sobreescribe, al estar defectuoso, los segundos subcampos, con lo que para cada unidad de señales segura se transmite en el segundo subcampo un cero lógico. El equipo de control y evaluación 342, 362 y 382 de las unidades de señales 340, 360 y 380 respectivamente generan en consecuencia, como reacción a los respectivos ceros lógicos recibidos, una señal de desconexión, que se emite a través de la salida 344, 364 y 384 respectivamente. Las señales de desconexión controlan preferentemente contactores, que desconectan inmediatamente el correspondiente proceso crítico para la seguridad, es decir, los procesos 432, 434 y 436.

En base a este comportamiento del sistema se detecta que un cero lógico transmitido en el segundo subcampo, que representa una orden de desconexión rápida, se ejecutará con preferencia por las unidades de señales seguras frente a los datos relativos a la seguridad que se transmiten en los respectivos subcampos de los campos de datos 451, 452 y 253.

Supongamos ahora ventajosamente que el equipo central 320 o 420 está configurado para, como reacción a un evento predeterminado, no modificar las señales definidas recibidas de las unidades de señales seguras 340, 360, 380, cuando no hay fallo con preferencia un cero lógico. Un tal evento predeterminado puede ser activado por ejemplo por un operario o por el sistema de control y transmisión de datos 310. Supongamos que el equipo central 320 ha recibido de un operario la comunicación de que el proceso completo 430 debe desconectarse inmediatamente.

En consecuencia se ocupa el equipo central 320 de que cada segundo subcampo contenga un cero lógico. Además escribe el mismo en el campo de datos 454 una orden de desconexión para la unidad de señales no segura 400 y transmite la trama sumatoria a las unidades de señales.

Tal como ya se ha descrito, generan los equipos de control y evaluación 342, 362 y 382, como reacción a un cero lógico recibido, en cada caso una señal de desconexión, que a través de la salida 344, 364 y 384 respectivamente desconecta el correspondiente subproceso crítico para la seguridad 432, 434 y 436 respectivamente. También la unidad de señales no segura 400 emite a través de su salida 403 una orden de desconexión para desconectar el subproceso no crítico para la seguridad 438. De esta manera puede desconectarse inmediatamente el proceso completo 430 centralmente mediante el equipo central 320 sin utilizar los datos relativos a la seguridad.

Esto puede lograrse, tal como se ha explicado antes, estando configurados los equipos de control y evaluación 342, 362 y 382 con preferencia para provocar, al recibir un cero lógico el correspondiente equipo de seguridad 343, 363 y 383 respectivamente, que no se evalúen ni se procesen los datos relativos a la seguridad recibidos.

Tal como ya se ha mencionado, puede estar previsto que el equipo central 320 esté configurado para generar datos dinámicos, como por ejemplo números consecutivos, que cuentan los ciclos de comunicación y transmitir los mismos en cada caso en los terceros subcampos de los campos de datos 451, 452 y 453 a las unidades de señales seguras 340, 360 y 380. Las unidades de señales seguras 340, 360 y 380 pueden entonces detectar en base a los datos dinámicos recibidos en el tercer subcampo si los segundos datos relativos a la seguridad recibidos en el segundo subcampo proceden del equipo de control de orden superior 320 y se han retransmitido correctamente.

Supongamos ahora que en lugar de una trama sumatoria basada en Interbus, se transmiten telegramas individuales entre el equipo central 320 y las unidades de señales a través del medio de comunicación 330, que por ejemplo es un sistema de comunicación basado en Ethernet. Las interfaces de comunicación 322, 341, 361, 381 y 401 están configuradas correspondientemente y pueden enviar y recibir un telegrama representado sólo esquemáticamente en la figura 4a.

El telegrama mostrado en la figura 4a contiene un campo de direcciones 441, en el que pueden encontrarse direcciones de destino y/o de origen y/o direcciones de radiodifusión y/o de grupo. En un campo de datos 442 pueden transmitirse datos relativos a la seguridad desde y hacía los correspondientes equipos de seguridad 343, 363 y 383. Un campo de datos 443 sirve para transmitir las señales definidas generadas por una unidad de señales segura. Además puede estar previsto un campo de datos 444, en el que, tal como antes se ha descrito, pueden transmitirse datos dinámicos.

Supongamos ahora que la unidad de señales segura 380 desea transmitir datos recibidos a través de la entrada 385, que contienen por ejemplo la velocidad de giro de una máquina del subproceso crítico para la seguridad 436, a través del equipo central 320 a la unidad de señales segura 340. El equipo de seguridad 383 genera a partir de los datos recibidos a través de la entrada 385, de manera de por sí conocida, datos relativos a la seguridad y transfiere estos datos a la interfaz de comunicación 381. Supongamos en el presente ejemplo que el equipo de control y evaluación 382 funciona incorrectamente y por lo tanto transmite un uno lógico en lugar del cero previamente ajustado al equipo de comunicación 381. En función de la implementación puede escribir el equipo de comunicación 381 la dirección del equipo central 320, la dirección de la unidad de señales segura 380 y la dirección de destino del equipo de señales seguro 360 en el campo de direcciones 441. Además escribe el mismo los datos relativos a la seguridad en el campo de datos 442 y un uno lógico en el campo de datos 443 y transmite el telegrama de datos al equipo central 320. El equipo central 320 está configurado a su vez para evaluar el campo de datos 443, pero no el campo de datos 442. El mismo detecta que en lugar de un cero lógico se ha transmitido un uno lógico desde la unidad de señales segura 380. En función de la configuración del sistema sabe el equipo central 320 por ejemplo que al recibir un uno lógico de la unidad de señales segura 380 tienen que desconectarse todos los procesos críticos para la seguridad 432, 434 y 436. En consecuencia puede estar configurado el equipo central 320 para generar un único telegrama de datos, en el que se describe una dirección de radiodifusión o de grupo en el campo de datos 441, que direcciona las unidades de señales seguras 340, 360 y 380. En el campo de datos 442 se tienen sin modificar los datos relativos a la seguridad, mientras que en el campo de datos 443 se escribe un cero lógico como orden de desconexión central. En el campo de datos 444 puede escribirse un número progresivo. El telegrama de datos se transmite ahora a través del medio de comunicación 330 a las unidades de señales seguras 340, 360 y 380. Los equipos de control y evaluación 342, 362 y 382 evalúan el campo de datos 443 del telegrama de datos recibido y generan en cada caso como reacción al cero lógico una señal de desconexión para las salidas 344, 364 y 384. Las señales de desconexión provocan que los procesos críticos para la seguridad 432, 434 y 436 se desconecten inmediatamente. Los datos relativos a la seguridad recibidos no se evalúan ni se procesan en las correspondientes unidades de señales seguras 340, 360 y 380. En consecuencia puede interpretarse el cero lógico también como orden de desconexión rápida.

Señalemos que en un funcionamiento libre de fallos de las unidades de señales seguras y del equipo central 320, el equipo central 320 sustituye cualquier cero lógico en el campo de datos 443 de un telegrama de datos recibido por un uno lógico y lo transmite a las unidades de señales seguras 340, 360 y 380. Esto significa que los equipos de control y evaluación 342, 362 y 382 no generan ninguna señal de desconexión y retransmiten los datos relativos a la seguridad a los correspondientes equipos de seguridad 343, 363 y 383 respectivamente. Los equipos de seguridad evalúan a continuación los datos relativos a la seguridad retransmitidos sin variación desde el equipo

central de manera de por sí conocida y proporcionan funciones en la salida 346, 366 y 386 respectivamente las correspondientes señales de control para ejecutar funciones de seguridad.

También puede pensarse en que por ejemplo la salida 344 de la unidad de señales segura 340 esté conectada con un contactor, con cuya ayuda puede desconectarse el proceso completo 430. En este caso puede estar configurado el equipo central 320 para transmitir un telegrama de datos en cuyo campo de datos 443 se escribe un cero lógico, selectivamente sólo a la unidad de señales segura 340. La unidad de control y evaluación 342 aporta entonces una señal de desconexión en la salida 344, que provoca una desconexión rápida del proceso completo 430.

Generalizando, ilustra la figura 3 un sistema de control y transmisión de datos 310 para transmitir datos relativos a la seguridad a través de un medio de comunicación 330. El mismo presenta varias unidades de señales seguras 340, 360 y 380, que están conectadas mediante respectivas salidas 341, 346, 361, 366 o bien 381, 386 y/o al menos respectivas entradas 345, 365 y 385 con un proceso crítico para la seguridad o un respectivo subproceso 432, 434 y 436. A un medio de comunicación 330 están conectadas las unidades de señales seguras 340, 360, 380 y un equipo central 320, 420. Las unidades de señales seguras 340, 360 y 380 presentan respectivos equipos de seguridad 343, 363 y 383 y están configuradas para proporcionar datos relativos a la seguridad y transmitir esos datos a través del medio de comunicación 330. Con preferencia está configurada cada unidad de señales segura 340, 360, 380 para proporcionar una señal definida y transmitir tanto la señal definida como también los datos relativos a la seguridad al equipo central 320, 420. El equipo central 320, 420 está configurado para evaluar sólo la señal definida y en función de la señal definida evaluada, generar una orden de control central y transmitir la orden de control central junto con los datos relativos a la seguridad a al menos una unidad de señales segura predeterminada de las varias unidades de señales seguras 340, 360, 380. La unidad de señales segura 340, 360, 380, de las que al menos hay una, está configurada para evaluar los datos relativos a la seguridad y la orden de control central, para controlar al menos una parte del proceso crítico para la seguridad 430, con preferencia en cada caso un subproceso 432, 434, 436.

El equipo central 320 puede ser un equipo de control de orden superior, configurado para controlar la comunicación sobre el medio de comunicación 330 y la unidad de señales no segura 400.

La señal definida puede ser una orden de desconexión en forma de un cero lógico.

Los equipos de seguridad 343, 363 y 383 están configurados con preferencia para no evaluar y/o no procesar datos relativos a la seguridad cuando la orden de control central recibida sea una orden de desconexión. Esto puede lograrse estando configurados los equipos de control y evaluación 342, 362 y 382 con preferencia para provocar al recibirse un cero lógico que el correspondiente equipo de seguridad 343, 363 y 383 respectivamente no evalúe y/o no procese los datos relativos a la seguridad recibidos.

El equipo central 320, 420 puede estar configurado para al recibir una señal definida no falsificada, generar una orden de control central que no active ninguna desconexión del proceso crítico para la seguridad 432, 434, 436 o de una parte del proceso crítico para la seguridad, pudiendo estar configurado el equipo central 320, 420 además para al recibir una señal definida falsificada, generar una orden de control central que active una desconexión del proceso crítico para la seguridad o de una parte del proceso crítico para la seguridad.

El equipo central 320, 420 puede además estar configurado para, como reacción a un evento predeterminado, no modificar la señal definida recibida.

El equipo central 320, 420 puede además estar configurado para transmitir la orden de control central utilizando una dirección de grupo a un determinado grupo de las unidades de señales seguras o a todas las unidades de señales seguras 340, 360, 380 y/o dado el caso a una o varias unidades de señales no seguras 400.

Cada una de las unidades de señales seguras 340, 360, 380 puede estar configurada para generar a partir de la señal definida una señal definida relativa a la seguridad.

Para que las unidades de señales seguras 340, 360 y 380 puedan detectar que los segundos datos relativos a la seguridad proceden del equipo central 320, 420 y se han transmitido correctamente, puede estar configurado el equipo central 320, 420 para proporcionar datos dinámicos de una manera definida y transmitirlos a la unidad de señales segura, de las que al menos hay una. La unidad de señales segura, de las que al menos hay una, está configurada al respecto correspondientemente para evaluar los datos dinámicos. Los datos dinámicos pueden ser informaciones alternantes o bien un número correlativo.

Alternativamente puede estar configurada la unidad señales segura, de las que al menos hay una, para generar datos dinámicos y transmitirlos al equipo central 320, 420. El equipo central 320, 420 puede estar configurado al respecto correspondientemente para modificar los datos dinámicos recibidos selectivamente, es decir, de forma definida y transmitirlos a la unidad de señales segura, de las que al menos hay una.

La unidad de señales segura, de las que al menos hay una, puede estar configurada para, como reacción a datos dinámicos modificados de manera indefinida, desconectar inmediatamente el correspondiente proceso crítico para la seguridad o bien llevar el mismo a un estado seguro definido.

El medio de comunicación 330 puede ser un bus de campo, en particular un bus de campo basado en Interbus y/o un sistema Ethernet.

La señal definida, previamente ajustada, puede ser una palabra de un solo bit, en particular un cero lógico y la orden de control central igualmente una palabra de un solo bit.

REIVINDICACIONES

1. Sistema de control y transmisión de datos (310) para transmitir datos relativos a la seguridad a través de un medio de comunicación (330), que presenta:
   - varias unidades de señales seguras (340, 360, 380), cada una de las cuales está conectada mediante al menos una salida (341, 346; 361, 366; 381, 386) y/o al menos una entrada (345; 365; 385) con un proceso crítico para la seguridad (432, 434; 436),
   - un medio de comunicación (330), al que están conectadas las unidades de señales seguras (340, 360, 380) y
   - un equipo central (320; 420), que está conectado al medio de comunicación (330), presentando las unidades de señales seguras (340, 360, 380) respectivos equipos de seguridad (343; 363; 383) y estando configurada cada una para proporcionar datos relativos a la seguridad y transmitir estos datos en un primer subcampo (442; 453_1) del correspondiente telegrama o trama sumatoria a través del medio de comunicación (330),

   caracterizado porque cada unidad de señales segura (340, 360, 380) está configurada para proporcionar una señal definida, que indica que el sistema de control y transmisión de datos (310) no tiene fallos o indica que no se ha activado ninguna función de seguridad y para escribir la señal definida en un segundo subcampo (443; 453_2) del correspondiente telegrama o trama sumatoria y para transmitir tanto la señal definida como también los datos relativos a la seguridad al equipo central (320; 420),

   porque el equipo central (320; 420) está configurado para leer y evaluar sólo el segundo subcampo del correspondiente telegrama o trama sumatoria y en función de la señal definida evaluada, generar una orden de control central y transmitir la orden de control central junto con los datos relativos a la seguridad a al menos una unidad de señales segura predeterminada de las varias unidades de señales seguras (340, 360, 380) y

   porque la unidad de señales segura (340, 360, 380), de las que al menos hay una, está configurada para evaluar los datos relativos a la seguridad y la orden de control central, para controlar al menos una parte del proceso crítico para la seguridad (432, 434, 436).

2. Sistema de control y transmisión de datos según la reivindicación 1,
   caracterizado porque el equipo central (320) es un equipo de control de orden superior, que está configurado para controlar la comunicación sobre el medio de comunicación (330).

3. Sistema de control y transmisión de datos según una de las reivindicaciones 1 a 2,
   caracterizado porque el equipo central (320; 420) está configurado para al recibir una señal definida no falsificada, generar una orden de control central que no activa ninguna desconexión del proceso crítico para la seguridad (432, 434, 436) o de una parte del proceso crítico para la seguridad y en el que el equipo central (320; 420) está configurado además para, al recibir una señal definida falsificada, generar una orden de control central que activa una desconexión del proceso crítico para la seguridad (432, 434, 436) o de una parte del proceso crítico para la seguridad.

4. Sistema de control y transmisión de datos según la reivindicación 3,
   caracterizado porque el equipo central (320; 420) está configurado para como reacción a un evento previamente determinado, no modificar la señal definida recibida.

5. Sistema de control y transmisión de datos según una de las reivindicaciones 3 ó 4,
   caracterizado porque los equipos de seguridad (343, 363, 383) están configurados para no evaluar y/o no procesar datos relativos a la seguridad cuando la orden de control central recibida es una orden de desconexión.

6. Sistema de control y transmisión de datos según una de las reivindicaciones 1 a 5,
   caracterizado porque el equipo central (320; 420) está configurado para transmitir la orden de control central utilizando una dirección de grupo a un grupo predeterminado de las unidades de señales seguras o a todas las unidades de señales seguras (340, 360, 380).

7. Sistema de control y transmisión de datos según una de las reivindicaciones 1 a 6,
   caracterizado por una unidad de señales no segura (400), que está conectada al medio de comunicación (330) y que está conectada con un proceso no crítico para la seguridad (438) o subproceso no crítico para la seguridad, en el que
   el equipo central (320; 420) está configurado para transmitir la orden de control central utilizando una dirección de grupo a todas las unidades de señales seguras (340, 360, 380) y a la unidad de señales no segura (400).

8. Sistema de control y transmisión de datos según una de las reivindicaciones 1 a 7,
   caracterizado porque cada una de las unidades de señales seguras (340, 360, 380) está configurada para generar a partir de la señal definida una señal definida relativa a la seguridad.

9. Sistema de control y transmisión de datos según una de las reivindicaciones 1 a 8,
   caracterizado porque el equipo central (320, 420) está configurado para proporcionar datos dinámicos y transmitirlos a al menos una unidad de señales segura (340, 360, 380) y porque la unidad de señales segura (340, 360, 380), de las que al menos hay una, está configurada para evaluar los datos dinámicos.

10. Sistema de control y transmisión de datos según una de las reivindicaciones 1 a 9,

caracterizado porque el medio de comunicación (330) es un bus de campo, en particular un bus de campo basado en Interbus y/o un sistema de Ethernet.

11. Sistema de control y transmisión de datos según una de las reivindicaciones 1 a 10,
caracterizado porque la señal definida es una palabra de un solo bit, en particular un cero lógico y porque el equipo central (320; 420) está configurado para al recibir una señal definida no falsificada, generar una orden de control central, que es una palabra de un solo bit, en particular un uno lógico.

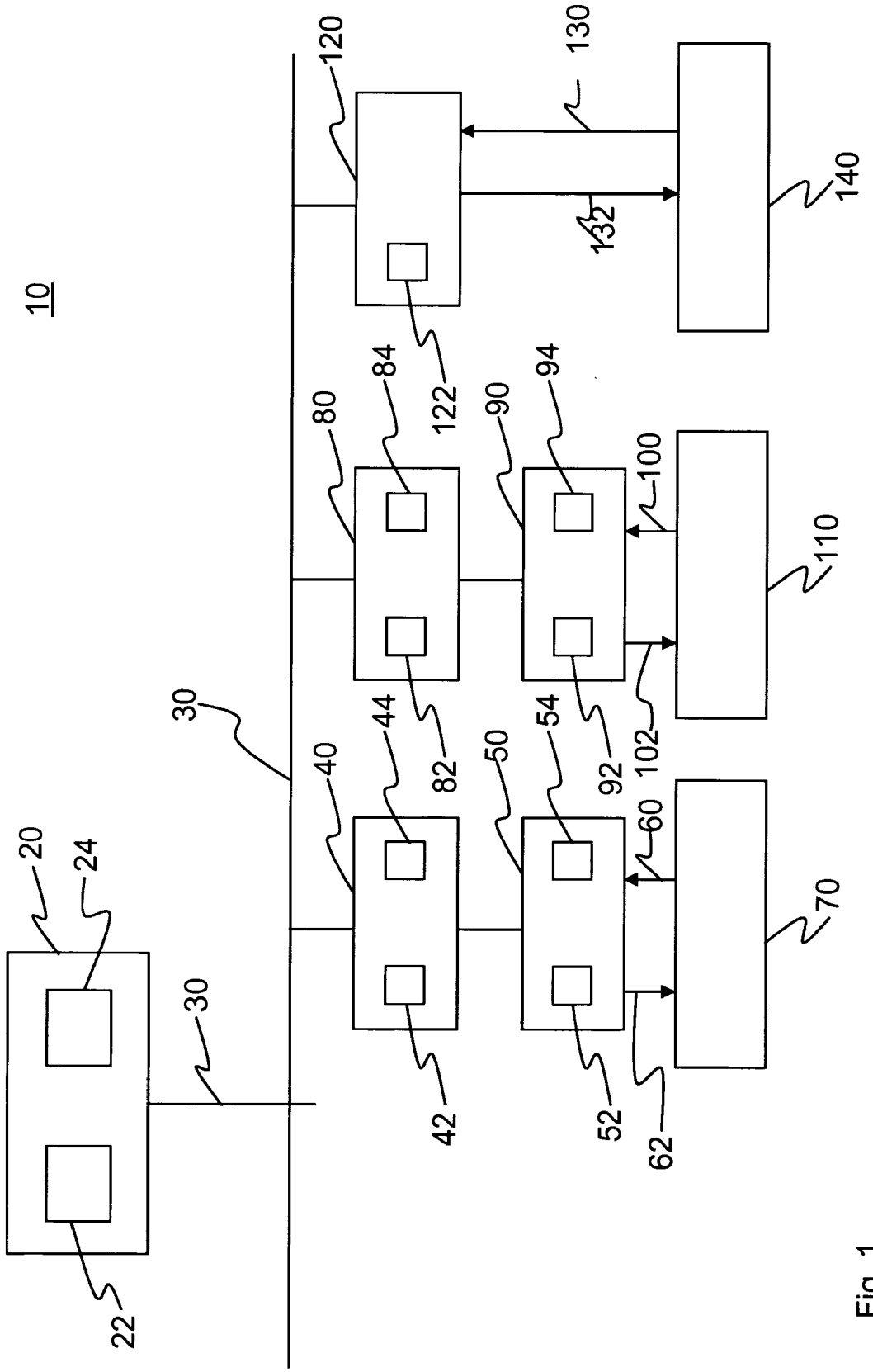
10
120
130
140
132
122
84
80
90
94
100
110
30
44
40
50
54
102
82
92
60
70
20
24
30
42
52
62
22

Fig. 1

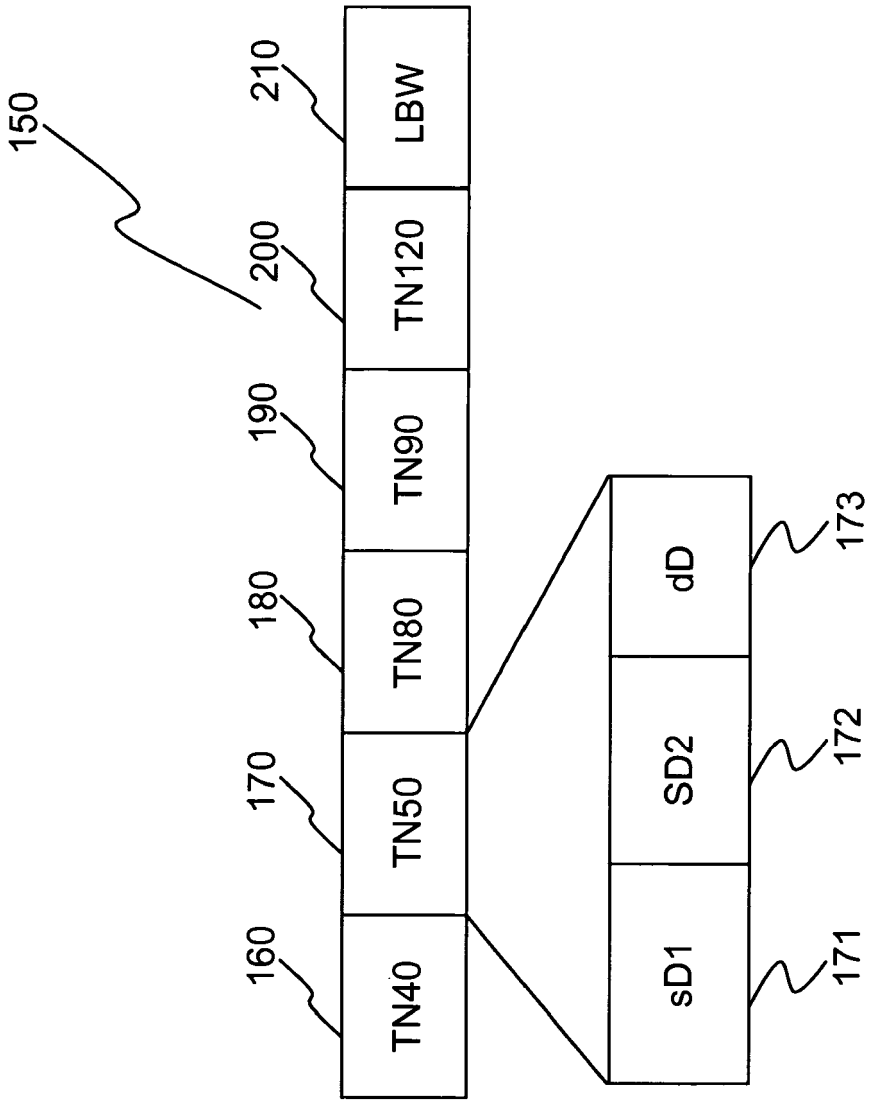
150
210
LBW
200
TN120
190
TN90
180
TN80
170
TN50
160
TN40
dD
173
SD2
172
sD1
171

Fig. 2

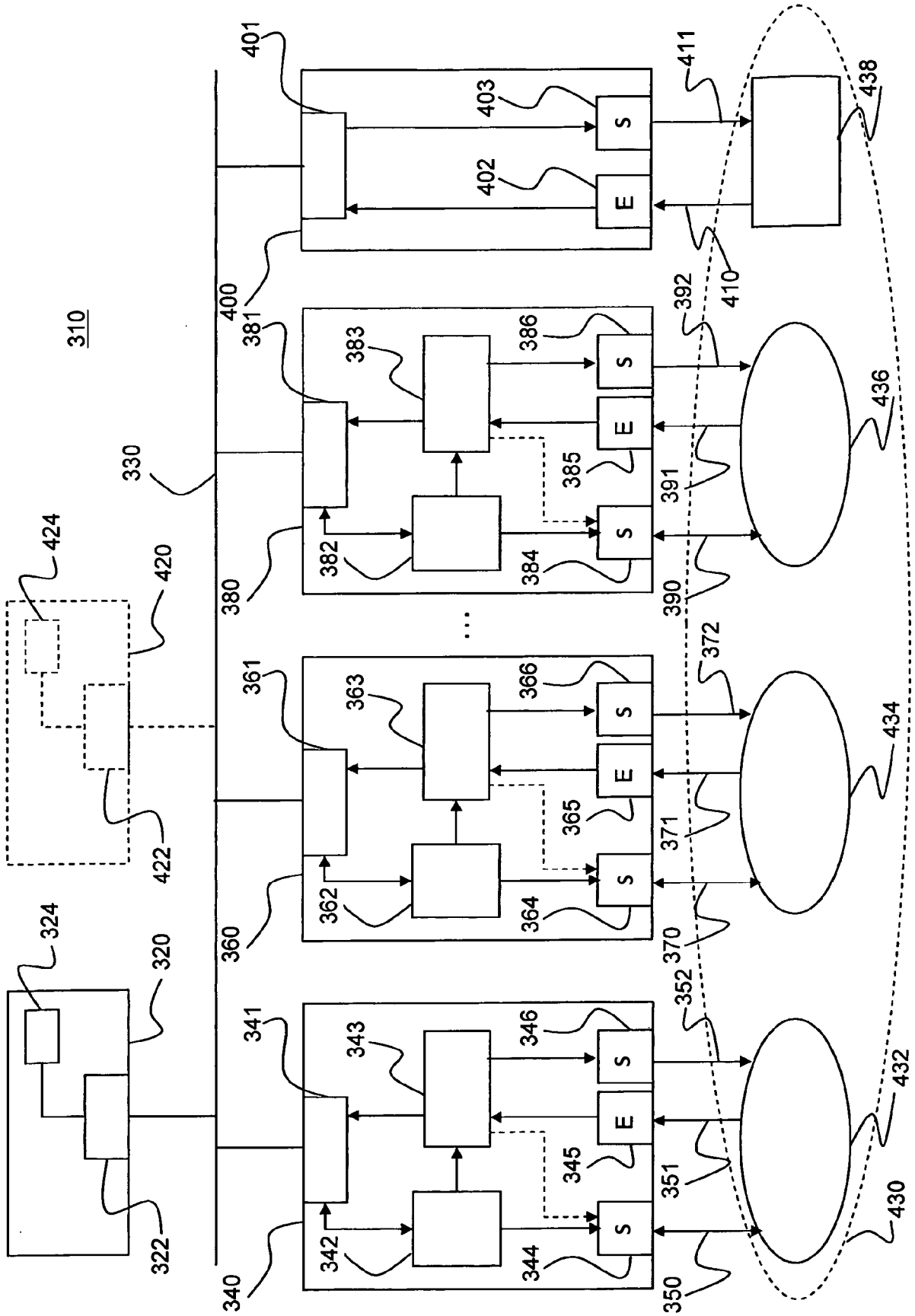
310
320
322
324
330
340
341
342
343
344
345
346
350
351
352
360
361
362
363
364
365
366
370
371
372
380
381
382
383
384
385
386
390
391
392
400
401
402
403
410
411
420
422
424
430
432
434
436
438
E
S

Fig. 3

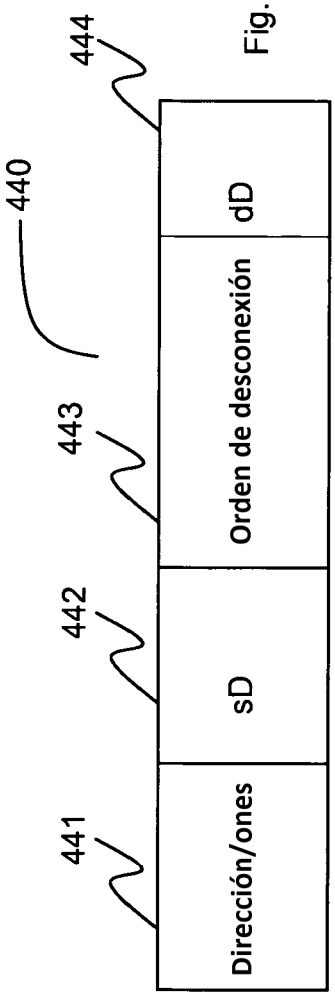
440
441
442
443
444
Dirección/ones
sD
Orden de desconexión
dD

Fig. 4a

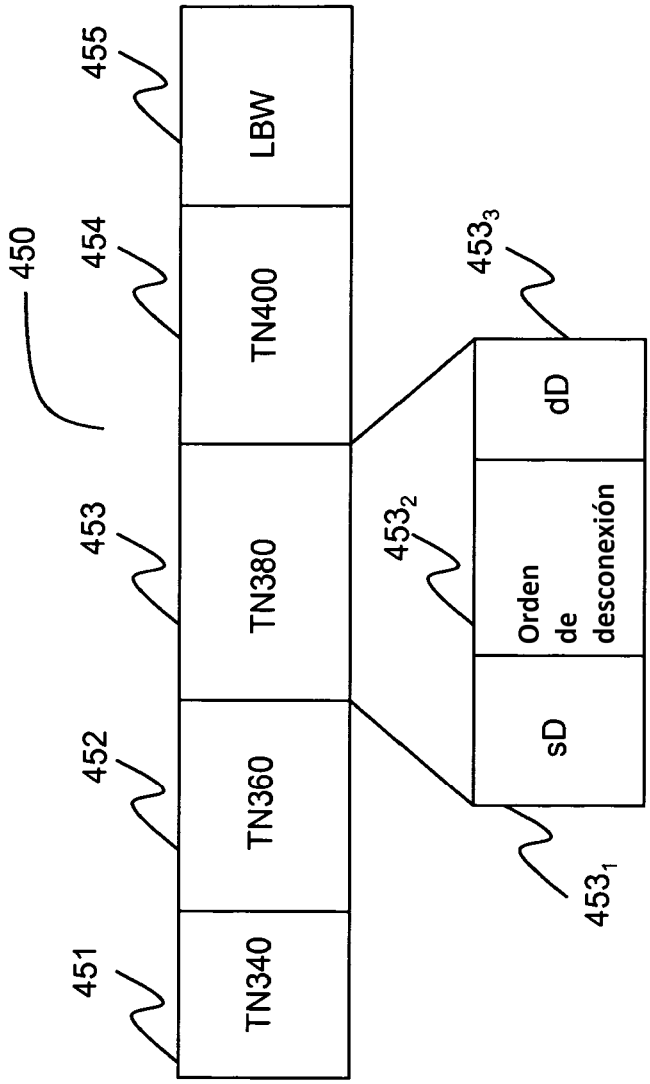
450
451
452
453
454
455
TN340
TN360
TN380
TN400
LBW
453_1
453_2
453_3
sD
Orden de desconexión
dD

Fig. 4b