(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 379 259**

(51) Int. CI.:
H04L 1/00 (2006.01)
H03M 13/05 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04008683 .7**
(96) Fecha de presentación: **10.04.2004**
(97) Número de publicación de la solicitud: **1469625**
(97) Fecha de publicación de la solicitud: **20.10.2004**

(54) Título: **Procedimiento y dispositivo para la transmisión orientada a paquetes de datos relevantes para la seguridad**

(30) Prioridad:
17.04.2003 DE 10318068

(45) Fecha de publicación de la mención BOPI:
24.04.2012

(45) Fecha de la publicación del folleto de la patente:
24.04.2012

(73) Titular/es:
PHOENIX CONTACT GMBH & CO.
FLACHSMARKTSTRASSE 8-28
32825 BLOMBERG, DE

(72) Inventor/es:
Schmidt, Jochaim

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Procedimiento y dispositivo para la transmisión orientada a paquetes de datos relevantes para la seguridad.

La invención concierne a un procedimiento y a dispositivos para la transmisión orientada a paquetes de datos relevantes para la seguridad.

Particularmente en la transmisión de datos relevantes para la seguridad por un medio no securizado, tal como, por ejemplo, por una red y/o un sistema de bus convencionales, se añade en general a tales datos una redundancia de alto valor de modo que casi todos los errores estadísticos y sistemáticos del sistema de transmisión total no tengan una repercusión negativa sobre la integridad de los datos y se satisfagan altos requisitos técnicos de seguridad en cuanto a la comunicación entre abonados de red y/o de bus individuales.

Usualmente, esto se realiza mediante una ampliación de los datos relevantes para la seguridad con un valor de securización de los datos que se genera basándose en datos relevantes para la seguridad y que, de conformidad con el respectivo protocolo, se anexan a los datos relevantes para la seguridad de un paquete de datos que se debe transmitir.

En la publicación de patente alemana DE 100 65 907 A1 se revela, por ejemplo, un procedimiento que se basa en el principio generalmente conocido de una "redundancia con comparación cruzada". En este caso, se tratan con información redundante en el lado del emisor unos datos relevantes para la seguridad puestos a disposición en un solo canal o en dos canales, según la clase de aplicación, efectuándose este tratamiento por duplicado, es decir, en dos paquetes de datos e independientemente uno de otro, y se transmiten estos datos a través de enlaces separados o bien se transmiten temporalmente uno tras otro a través de un enlace con el lado de recepción. Según la aplicación, el contenido de datos de uno de los dos paquetes de datos tratados dirigidos a la seguridad puede presentar también datos invertidos u otros entrelazamientos adicionales para reconocer también, por ejemplo, errores sistemáticos en los emisores, receptores y/u otras unidades de retransmisión de los datos. Además, se ha previsto según esta publicación comprobar de forma cruzada en el lado del emisor y/o en el lado del receptor el grado de corrección de los dos paquetes de datos tratados analizando para ello la respectiva redundancia agregada dentro de los paquetes de datos.

El mensaje completo dirigido a la seguridad según el estado de la técnica está estructurado entonces, por ejemplo, según la figura 3 adjunta, en donde el mensaje dirigido a la seguridad comprende consecuentemente dos paquetes de datos 3 y 3'. Según la figura 3, los datos relevantes para la seguridad, aparte de los datos útiles propiamente dichos, contienen también datos de control adicionales, comprendiendo cada uno de los paquetes de datos 3 y 3' estos datos con el mismo contenido de información, pero con codificación diferente. Además, cada paquete de datos 3 ó 3' contiene un bloque de información redundante CRC o $\overline{CRC}$ generado en base a los datos relevantes para la seguridad.

Sin embargo, una desventaja esencial de este procedimiento en sí conocido según el estado de la técnica reside especialmente en la mala relación de longitud de datos útiles a longitud de datos totales, la cual empeora cada vez más al disminuir el número de datos útiles a transmitir por cada paquete de datos, tal como éste se proporciona, por ejemplo, en el Interbus.

Se conoce por "A Hybrid ARQ Scheme with Parity Retransmission for Error Control of Satellite Channels", IEEE, Junio de 1982, páginas 1701-1719, un llamado sistema ARQ híbrido que representa una combinación de un esquema ARQ convencional y un esquema FEC y que es adecuado especialmente para control de errores en sistemas de comunicación de datos a alta velocidad con tiempos de circulación significativos, tal como en una transmisión por satélite. Por tanto, este procedimiento no es adecuado para una transmisión de datos relevantes para la seguridad, ya que aquí se tiene que reaccionar eventualmente con una extremada proximidad en el tiempo.

El documento US 2002/0133780 revela un procedimiento de transmisión de datos en el que se transmiten datos y una redundancia basada en estos en paquetes diferentes.

Por tanto, un problema de la invención consiste en proporcionar un modo de transmisión orientada a paquetes de datos relevantes para la seguridad, que sea nuevo y esté mejorado frente al estado de la técnica anteriormente indicado y con el cual, garantizando también una tasa de datos útiles sensiblemente mejorada, se asegure una protección de alta calidad frente a errores estadísticos y sistemáticos en un medio de transmisión no securizado.

La solución del problema según la invención viene dada ya de una manera sumamente sorprendente por un procedimiento con las características de la reivindicación 1, un dispositivo con las características de la reivindicación 10 y un sistema de transmisión con las características de la reivindicación 20.

Formas de realización o perfeccionamientos ventajosos y/o preferidos son objeto de las respectivas reivindicaciones

subordinadas.

Por tanto, según la invención, para la transmisión orientada a paquetes de datos relevantes para la seguridad, especialmente empleando al menos un sistema de transmisión que comprende una red y/o un sistema de bus en paralelo y/o en serie con al menos un abonado conectado a ellos, se ha previsto que se transmitan en paquetes diferentes los datos relevantes para la seguridad y una información redundante basada en dichos datos relevantes para la seguridad.

En consecuencia, es de importancia esencial que se garantice una protección de alta calidad frente a errores estadísticos y sistemáticos, especialmente en el caso de una transmisión a través de un medio no securizado, a una tasa de datos útiles sensiblemente mejorada.

Por tanto, la invención prevé de manera conveniente la habilitación de un dispositivo para la transmisión orientada a paquetes de datos relevantes para la seguridad entre al menos dos abonados de red y/o de bus, que presenta medios dispuestos en el lado del emisor para la incrustación orientada a paquetes de datos relevantes para la seguridad e información redundante asociada en diferentes paquetes y/o medios dispuestos en el lado de recepción que están concebidos para comprobar la transmisión exenta de errores de datos relevantes para la seguridad en base a datos relevantes para la seguridad incrustados en paquetes diferentes y a información redundante asociada.

Por tanto, la invención hace posible, además, que únicamente sean necesarios medios para generar, transmitir y comprobar una única unidad de información redundante para cada unidad de datos relevante para la seguridad, lo que conduce a una sensible simplificación en el procesamiento de datos, especialmente de equipos o abonados de entrada y/o salida, basados en la seguridad, de una red y/o un bus de transmisión.

Para garantizar que se reconozcan sustancialmente todos los errores estadísticos y sistemáticos en el sistema de transmisión se ha previsto de manera ventajosa un equipo de codificación con el cual se puede codificar correspondientemente la información redundante.

En un perfeccionamiento especialmente preferido la invención propone utilizar para la información redundante un valor de securización de datos que contenga una suma de verificación calculada en función de los datos relevantes para la seguridad.

Esta suma de verificación se puede elegir aquí, por ejemplo, empleando un polinomio para que, de una manera especialmente preferida, cada una de las sumas de verificación posibles se derive de justamente una de las posibles combinaciones de los datos relevantes para la seguridad.

Por tanto, la invención garantiza en conjunto una protección extraordinariamente buena frente a errores concentrados y frente a permutaciones de componentes individuales del mensaje dirigido a la seguridad que se debe transmitir.

Según un perfeccionamiento práctico, los medios de incrustación dispuestos en el lado del emisor llevan asociados unos medios del tipo de controladores para generar información redundante que presenta el mismo número de bits que el que presentan los datos relevantes para la seguridad que se deben transmitir. Por tanto, la invención puede utilizarse de una manera sustancialmente específica según la aplicación en sustancialmente todas las redes y/o sistemas de bus actualmente conocidos, como, por ejemplo, Interbus, Ethernet, Profibus o CAN.

Por tanto, en la transmisión según la invención de datos relevantes para la seguridad y de una redundancia asociada en paquetes separados se puede ajustar una distancia de Hamming grande.

En consecuencia, dado que, debido ya solamente a un bit variable, se puede asegurar también con la invención una alta dinámica incluso en el caso de un pequeño número de datos útiles, se puede garantizar también en la retransmisión de los datos un reconocimiento especialmente bueno de errores sistemáticos, especialmente de abonados de red y/o de bus no seguros, incluyendo interruptores, routers, amplificadores, pasarelas, acopladores de sistemas y/o un maestro.

La invención prevé también, según redes y/o sistemas de bus en serie y/o en paralelo, utilizados según la aplicación específica, que los datos relevantes para la seguridad, además de los datos útiles propiamente dichos, es decir, especialmente datos de entrada/salida y/u otros datos de proceso seguros, comprendan otros datos, especialmente datos de control y/o de mando.

Asimismo, se ha previsto que los paquetes con los datos relevantes para la seguridad y las informaciones redundantes asociados entre ellos se transmitan en paralelo o en serie y/o se transmitan varios paquetes dentro de una (sobre)trama predefinida, de modo que la invención pueda usarse en muy diferentes aplicaciones y/o campos de utilización. Particularmente en el caso últimamente citado, se propone también preferiblemente que, dentro de la estructura predefinida de una (sobre)trama se transmitan conjuntamente datos relevantes para la seguridad y las informaciones redundantes asociadas generadas en base a ellos para simplificar, especialmente en lo que respecta a la funcionalidad de asociación, la implementación para la habilitación en el lado de recepción de medios de lectura

y comprobación de los datos relevantes para la seguridad y de la información redundante asociada.

Por tanto, cuando los paquetes con datos relevantes para la seguridad e información redundante mutuamente asociados se transmiten por separado uno de otro, se ha previsto también en un perfeccionamiento preferido que los paquetes de datos a transmitir comprendan un bloque de direccionamiento y/o un indicativo de asociación lógica. En una realización práctica de medios del lado del emisor correspondientemente adaptados a la aplicación específica, este direccionamiento y/o este indicativo se incrustan de esta manera, basándose en el respectivo formato de transmisión utilizado, en los paquetes de datos a transmitir y son verificados, para comprobar una transmisión exenta de errores, por un medios de lectura configurados correspondientemente en el lado de recepción para efectuar una asociación lógica de paquetes de datos con contenidos mutuamente asociados.

Según el campo de aplicación de la invención, que reside, por ejemplo, en la técnica de gestión de edificios, la industria de procesos, la industria de fabricación, el transporte de personas y/o el funcionamiento de una instalación de automatización, así como basándose en la estructura individual de la respectiva red y/o sistema de bus, que presenta especialmente una estructura de forma anular, lineal, estrellada y/o arborescente, la invención hace posible de manera ventajosa la integración de los medios según la invención del lado del emisor y del lado del receptor, anteriormente relacionados, sustancialmente en cada equipo de abonado, es decir, especialmente en abonados de tipo maestro y/o esclavo.

A continuación, se describe la invención ayudándose de un ejemplo de realización preferido y haciendo referencia a los dibujos adjuntos.

Muestran en los dibujos:

La figura 1, una estructura según la invención de paquetes de datos para la transmisión orientada a paquetes de datos relevantes para la seguridad,

La figura 2, otra estructura según la invención para ilustrar el reconocimiento sensiblemente mejorado de errores sistemáticos y

La figura 3, la estructura de un mensaje dirigido a la seguridad según el estado de la técnica.

Haciendo referencia a la figura 1 se representa a título de ejemplo, para proporcionar una transmisión orientada a paquetes de datos relevantes para la seguridad, garantizando a la vez una alta tasa de datos útiles junto con una simultánea protección de alto valor frente a errores estadísticos y sistemáticos, un mensaje dirigido a la seguridad a transmitir según la invención que comprende dos paquetes de datos 1 y 2.

Según la invención, un mensaje dirigido a la seguridad de un juego de datos relevantes para la seguridad, como se representa en la figura 1, presenta básicamente al menos dos paquetes de datos separados 1 y 2, de los que un paquete de datos 1 comprende datos relevantes para la seguridad y otro paquete de datos 2 comprende información redundante asociada.

Basándose en esta estructura según la invención, se asegura que, también al transmitir datos relevantes para la seguridad a través de un medio no securizado, es decir, sustancialmente a través de un sistema de bus y/o de red que no satisface normas dirigidas a la seguridad y/o no comprende abonados de sistema seguros, se puedan reconocer sustancialmente todos los errores estadísticos y todos los errores sistemáticos.

Los errores estadísticos en una transmisión de datos se basan aquí especialmente en perturbaciones y/o influencias eléctricas actuantes desde fuera, mientras que los errores sistemáticos encuentran generalmente sus causas en errores basados en el software y/o el hardware de emisores, receptores y/u otros equipos de retransmisión de los datos, dispuestos en la vía de transmisión, como, por ejemplo, interruptores routers, amplificadores, pasarelas y/o acopladores de sistemas.

En consecuencia, tal como se describe seguidamente con más detalle, se pueden excluir de manera sustancialmente completa las repercusiones negativas de tales causas sobre la integridad de datos relevantes para la seguridad.

El paquete de datos 1 representado en la figura 1 comprende como datos relevantes para la seguridad un bloque de datos útiles 11 específico del protocolo y/o de la aplicación y, en el presente ejemplo, un bloque de datos de control 12.

Según la aplicación específica, tales datos útiles 11 son proporcionados en uno o dos canales en el lado del emisor, especialmente por sensores, actores y/o equipos de mando, y, basándose en la estructura total del sistema de transmisión, que puede presentar estructuras de red y/o de bus de forma anular, lineal, estrellada y/o arborescente, son transmitidos a un lado de recepción definido, por ejemplo a un actor o un servoaccionamiento de una rejilla de protección. En consecuencia, tales datos útiles 11 comprenden frecuentemente datos puros de entrada/salida. Por consiguiente, los campos de utilización de sistemas de transmisión en los que tales datos útiles 11 representan en

parte o en todo su volumen datos relevantes para la seguridad, se encuentran especialmente en el sector de la industria de fabricación, el transporte de personas, la técnica de combustión, la industria de procesos o el sector de la técnica de gestión de edificios.

Además de estos datos de entrada/salida puros 11, se generan frecuentemente para el mando de procesos unos datos de control 12 y/o unos datos seguros o no seguros adicionales, como por ejemplo, datos de mando, o, como se representa en la figura 2, un número correlativo 12b. Estos datos adicionales permiten que, por ejemplo, los abonados de comunicación comprueben sustancialmente el funcionamiento impecable de un abonado contrario, especialmente por control de la vía de transmisión a través de cadenas de pasos mediante el respectivo intercambio de bloques de datos de control 16.

El paquete de datos 2 que completa el mensaje dirigido a la seguridad comprende una información redundante 21 asociada al contenido de información del paquete de datos 1, es decir, un valor de securización de datos 21 basado en los datos útiles 11 y los datos de control 12.

El valor de securización de datos 21 contenido en el paquete de datos 2 es convenientemente una suma de verificación CRC calculada en función de los datos útiles 11 y el bloque de control 12, la cual se genera en el lado del emisor con medios adaptados de tipo controlador, especialmente un microprocesador o una disposición de circuito programable semejante, sobre la base de un algoritmo de comprobación de error, por ejemplo en forma de una "Cycle Redundancy Check" (verificación de redundancia de ciclo) en sí conocida.

En el lado de recepción o en un puesto de retransmisión definido los mensajes parciales 1 y 2 son leídos por abonados dispuestos según la aplicación específica, especialmente abonados esclavos y/o un abonado maestro, y son comprobados respecto de una transmisión exenta de errores por análisis de la información redundante 21 con respecto a los datos 11 y 12 relevantes para la seguridad antes de que los datos útiles 11 relevantes para la seguridad sean retransmitidos a los abonados de salida correspondientes, tal como, por ejemplo, un actor, para la activación de éste.

Por tanto, dado que los paquetes de datos a transmitir según un protocolo específico presentan básicamente siempre el mismo número de bits, se tiene que, como puede verse en la figura 1, el paquete de datos 1, que comprende los datos relevantes para la seguridad, es decir, en el presente ejemplo los datos útiles, y adicionalmente los datos de control 12, y el paquete de datos 2 que contiene la suma de verificación 21 poseen también en cada caso la misma longitud de bits n.

En consecuencia, la tasa de datos útiles, es decir, la relación de la longitud de datos útiles a la longitud de datos totales, de un mensaje dirigido a la seguridad constituido según la invención es sensiblemente más alta en comparación con un mensaje dirigido a la seguridad en el que, como se representa en la figura 3, cada paquete de datos 3 y 3', aún cuando está codificado de manera diferente, comprende los datos relevantes para la seguridad, es decir, especialmente los datos útiles, y también un valor de securización de datos basado en los datos relevantes para la seguridad.

En consecuencia, basándose en la incrustación de los datos 11, 12 relevantes para la seguridad y de la información redundante 21 en dos paquetes de datos diferentes 1 y 2 se tiene que realizar únicamente la generación de un valor de securización de datos 21 y, por tanto, la invención hace posible el ahorro de un valor de securización de datos frente a la transmisión de datos relevantes para la seguridad según el estado de la técnica (figura 3).

Sin embargo, para que, además de la tasa de datos útiles mejorada, especialmente también durante la transmisión de un juego de datos relevante para la seguridad que comprende únicamente un pequeño número de datos útiles 11, se garantice también una protección de alto valor frente a errores para una emisión y/o retransmisión de datos relevantes para la seguridad por abonados esclavos no seguros y/o por un maestro no seguro, el valor de securización de datos 21 consecuentemente incrementado en el número de bits es especialmente efectivo.

A este fin, se elige preferiblemente el valor de securización de datos 21, es decir, especialmente el polinomio CRC o el algoritmo de comprobación de error empleado para generar una suma de verificación, de modo que cada uno de los 2^n valores de securización de datos posibles se derive de justamente una de las 2^n combinaciones de datos relevantes para la seguridad. Por tanto, ambos paquetes de datos 1 y 2 del mensaje dirigido a la seguridad contienen sustancialmente las mismas informaciones, pero están codificados de maneras diferentes.

Por tanto, para el uso práctico se proporcionan, con una generación adecuada de la información redundante 21, una distancia de Hamming muy alta, así como una buena protección contra errores concentrados y contra permutación de componentes individuales de los datos del mensaje dirigido a la seguridad, y un buen reconocimiento de errores, especialmente también de errores sistemáticos por medio de los diferentes mensajes parciales 1 y 2, como se describe seguidamente con detalle haciendo referencia a la figura 2.

Haciendo referencia a la figura 2, en la que un mensaje dirigido a la seguridad está constituido por dos paquetes de datos 1b y 2b, cada uno de ellos comprendiendo 24 bits, se pone especialmente de manifiesto el reconocimiento

particularmente bueno de errores sistemáticos basándose en la invención. El paquete de datos 1b, que comprende los datos relevantes para la seguridad, comprende aquí dos zonas, una zona de datos útiles 11b que cuenta con 16 bits y una zona 12b que cuenta con 8 bits para la transmisión de un número correlativo.

Cuando, por ejemplo, no varían los datos de proceso o los datos de entrada/salida que se deben securizar, es decir, los datos útiles 11b que comprenden 16 bits, el número relativo se incrementa solamente en la zona de datos 12b', por ejemplo durante una aplicación. En consecuencia, cuando se la elegido adecuadamente el polinomio de comprobación 21b, se modifican siempre en la suma grande de verificación 21b, que comprende 24 bits, una serie completa de bits en posiciones muy diferentes. Por tanto, esta alta dinámica de los mensajes permite cubrir de manera especialmente sencilla y con garantía de máxima seguridad errores sistemáticos en los equipos que retransmiten los mensajes dirigidos a la seguridad.

Según la aplicación específica o basándose en la respectiva red y/o bus, la invención garantiza, además, que los dos mensajes parciales 1 y 2 que forman un mensaje dirigido a la seguridad se agrupen también y se transmitan conjuntamente dentro de una estructura de (sobre)trama predefinida.

Sin embargo, cabe consignar en principio que la transmisión de los dos mensajes parciales mutuamente asociados 1 y 2 puede efectuarse también por separado, por ejemplo a través de un enlace separado, o bien sucesivamente en el tiempo a través de un mismo enlace. Asimismo, la invención garantiza que los mensajes parciales mutuamente asociados 1 y 2 puedan también incrustarse y transmitirse dentro de diferentes estructuras de (sobre)trama predefinidas. A este fin, se ha previsto convenientemente que los distintos paquetes sean provistos de un bloque de direccionamiento y/o de un indicativo para la asociación lógica, de modo que la lectura, asociación y comprobación de la transmisión exenta de errores de datos recibidos en el lado del receptor pueda realizarse también independientemente de la transmisión temporal y/o de la naturaleza de la transmisión de los mensajes parciales mutuamente asociados 1 y 2.

Por tanto, la invención hace posible que se transmitan datos relevantes para la seguridad a una alta tasa de datos útiles a través de sustancialmente cualquier clase de medios inseguros, sin que se pierda la seguridad requerida. A título de ejemplo, cabe aludir en este punto al Interbus como medio de transmisión preferido para la aplicación de la invención, en el que se emiten y/o retransmiten datos seguros con un pequeño número de datos útiles desde abonados no seguros y/o desde el maestro no seguro.

REIVINDICACIONES

1. Procedimiento para la transmisión orientada a paquetes de datos (11, 11b, 12, 12b) relevantes para la seguridad en la técnica de gestión de edificios, la industria de procesos, la industria de fabricación, el transporte de personas y/o el funcionamiento de una instalación de automatización, en el que se tiene que, además de los datos (11, 11b, 12, 12b) de un respectivo paquete relevantes para la seguridad, se transmite cada vez únicamente una información redundante (21, 21b) basada en todos los datos de este paquete, en el que los datos (11, 11b, 12, 12b) relevantes para la seguridad y la respectiva información redundante (21, 21b) que se basa en estos datos se transmiten en respectivos paquetes diferentes (1, 1b, 2, 2b), en el que el paquete de datos (1, 1b) que comprende los datos relevantes para la seguridad comprende datos útiles (11, 11b) y datos de control (12, 12b) en calidad de datos relevantes para la seguridad, y en el que se comprueba por abonados de comunicación el funcionamiento impecable de un abonado contrario mediante el control de la vía de transmisión a través de cadenas de pasos y por efecto de un respectivo intercambio de bloques de datos de control.

2. Procedimiento según la reivindicación 1, **caracterizado** porque se codifica la información redundante (21, 21b).

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado** porque la información redundante (21, 21b) es una suma de verificación (CRC) calculada en función de los datos relevantes para la seguridad.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, **caracterizado** porque se transmiten varios paquetes (1, 1b, 2, 2b) dentro de una estructura de (sobre)trama predefinida.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, **caracterizado** porque algunos paquetes dentro de una estructura de (sobre)trama predefinida comprenden datos (11, 11b, 12, 12b) relevantes para la seguridad e información redundante (21, 21b) mutuamente asociados.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 5, **caracterizado** porque los paquetes (1, 1b, 2, 2b) con datos (11, 11b, 12, 12b) relevantes para la seguridad e información redundante (21, 21b) mutuamente asociados se transmiten en paralelo o en serie.

7. Procedimiento según cualquiera de las reivindicaciones 1 a 6, **caracterizado** porque los paquetes (1, 1b, 2, 2b) con datos relevantes para la seguridad e información redundante mutuamente asociados se transmiten yuxtapuestos o separados uno de otro.

8. Procedimiento según cualquiera de las reivindicaciones 1 a 7, **caracterizado** porque los paquetes (1, 1b, 2, 2b) comprenden un bloque de direccionamiento y/o un indicativo para la asociación lógica.

9. Procedimiento según cualquiera de las reivindicaciones 1 a 8 anteriores, que se ejecuta empleando al menos un sistema de transmisión que contiene una red y/o un sistema de bus en paralelo y/o en serie con al menos un abonado conectado a ellos.

10. Dispositivo para la transmisión orientada a paquetes de datos (11, 11b, 12, 12b) relevantes para la seguridad en la técnica de gestión de edificios, la industria de procesos, la industria de fabricación, el transporte de personas y/o el funcionamiento de una instalación de automatización, que comprende medios dispuestos en el lado del emisor para la incrustación orientada a paquetes de datos (11, 11b, 12, 12b) relevantes para la seguridad y de solamente una respectiva información redundante (21, 21b) asociada a los datos (11, 11b, 12, 12b) de un paquete relevantes para la seguridad y basada en todos estos datos, en donde los medios citados están concebidos para incrustar los datos relevantes para la seguridad y la respectiva información redundante asociada en diferentes paquetes (1, 1b, 2, 2b) y en donde el paquete de datos (1, 1b) que comprende los datos relevantes para la seguridad comprende, como datos relevantes para la seguridad, datos útiles (11, 11b) y datos de control (12, 12b) que permiten que los abonados de comunicación comprueben el funcionamiento impecable de un abonado contrario por control de la vía de transmisión a través de cadenas de pasos y mediante un respectivo intercambio de bloques de datos de control.

11. Dispositivo según la reivindicación 10, **caracterizado** por un equipo de codificación para codificar la información redundante (21, 21b).

12. Dispositivo según la reivindicación 10 u 11, **caracterizado** porque los medios de incrustación llevan asociados medios de generación de información redundante (21, 21b) con el mismo número de bits (n) que los datos (11, 11b, 12, 12b) relevantes para la seguridad que se deben transmitir.

13. Dispositivo según la reivindicación 10, 11 ó 12, **caracterizado** porque los medios de generación y/o incrustación están concebidos de tal manera que justamente una de las posibles combinaciones dentro del paquete (2, 2b) con información redundante asociada (21, 21b) se derive unívocamente de cada combinación posible de datos (11, 11b, 12, 12b) dirigidos a la seguridad de un paquete (1, 1b).

14. Dispositivo para la transmisión orientada a paquetes de datos (11, 11b, 12, 12b) relevantes para la seguridad, especialmente según cualquiera de las reivindicaciones 11 a 13, **caracterizado** por medios dispuestos en el lado de

recepción para comprobar una transmisión de datos exenta de errores basándose en datos (11, 11b, 12, 12b) relevantes para la seguridad e información redundante asociada (21, 21b), que están incrustados en diferentes paquetes (1, 1b, 2, 2b).

15. Dispositivo según la reivindicación 14, **caracterizado** porque los medios de comprobación llevan asociados medios de lectura y asociación de datos (11, 11b, 12, 12b) relevantes para la seguridad, recibidos con paquetes diferentes, e información redundante asociada (21, 21b).

16. Dispositivo según cualquiera de las reivindicaciones 11 a 15, **caracterizado** porque se pueden transmitir dentro de una estructura de (sobre)trama predefinida varios paquetes (1, 1b, 2, 2b) con datos (11, 11b, 12, 12b) relevantes para la seguridad y/o información redundante asociada (21, 21b).

17. Dispositivo según cualquiera de las reivindicaciones 11 a 16, **caracterizado** por medios de incrustación y lectura orientadas a paquetes de bloques de direccionamiento y/o indicativos para la asociación lógica entre paquetes individuales (1, 1b, 2, 2b) y/o sus contenidos (11, 11b, 12, 12b, 21, 21b).

18. Dispositivo según cualquiera de las reivindicaciones 11 a 17, **caracterizado** porque los medios llevan asociados equipos esclavos y/o un equipo maestro.

19. Dispositivo según cualquiera de las reivindicaciones 11 a 18 anteriores, adaptado para un sistema de transmisión con al menos una red y/o un sistema de bus en paralelo y/o en serie.

20. Sistema de transmisión con al menos una red y/o un sistema de bus en paralelo y/o en serie y con al menos un dispositivo según cualquiera de las reivindicaciones 11 a 19.

21. Sistema de transmisión según la reivindicación 20, que presenta al menos una red y/o un sistema de bus configurados en forma anular, lineal, estrellada y/o arborescente.

22. Sistema de transmisión según la reivindicación 20 ó 21, que comprende al menos un Interbus, una Ethernet, un Profibus y/o una CAN.

Fig. 1

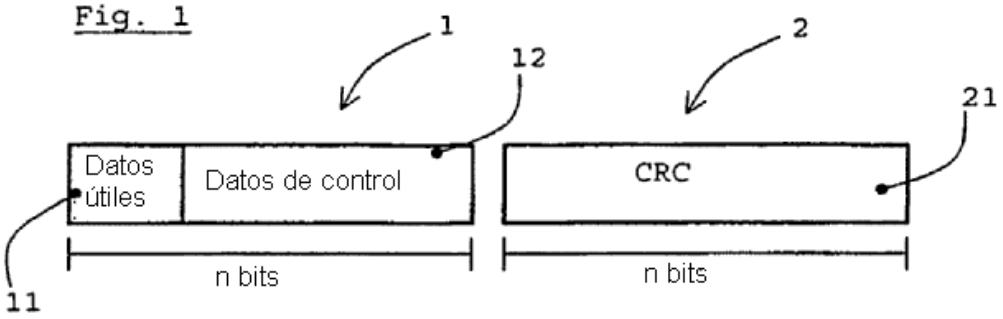

Fig. 2

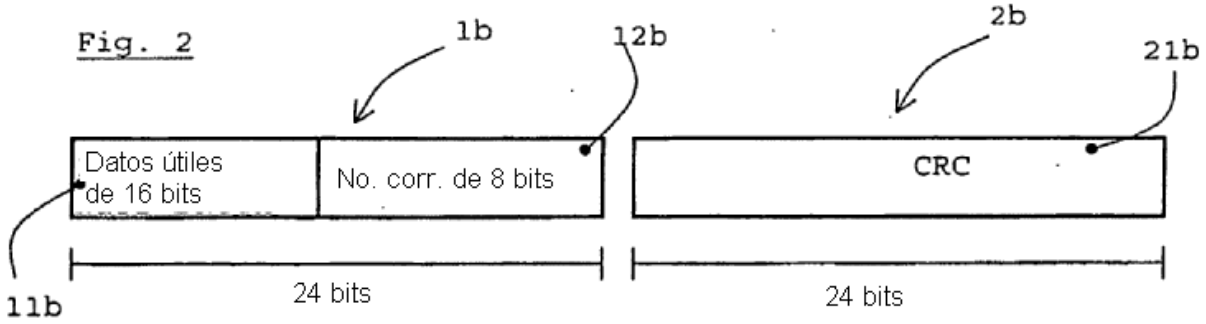

Fig. 3