(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 528 182**

(51) Int. CI.:

G06F 13/38 (2006.01)
H04L 12/46 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.02.2006 E 06003759 (5)**

(97) Fecha y número de publicación de la concesión europea: **12.11.2014 EP 1701270**

(54) Título: **Acoplamiento de sistemas de bus de campo seguros**

(30) Prioridad:

07.03.2005 DE 102005010820

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.02.2015

(73) Titular/es:

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

(72) Inventor/es:

ESCH, RAINER y
LANDWEHR, HEINZ-CARSTEN

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

ACOPLAMIENTO DE SISTEMAS DE BUS DE CAMPO SEGUROS

DESCRIPCIÓN

La invención se refiere a un procedimiento y a un equipo configurado para realizar el procedimiento para acoplar al menos sistemas de bus (de campo)/red con distintos mecanismos de seguridad para procesar datos relevantes o críticos para la seguridad.

En el marco de la invención se entienden bajo datos relevantes y críticos para la seguridad, denominados en la siguiente descripción y en las reivindicaciones en general datos de seguridad, datos que son relevantes y/o críticos para el control de procesos (parciales) relevantes o críticos para la seguridad, de los cuales se deriva, cuando se presenta una falta, un peligro no despreciable para las personas y/o también para bienes materiales, teniendo que conducirse por lo tanto el proceso, un proceso derivado acoplado con este proceso y/o un sistema que incluye este proceso a un estado seguro.

Ejemplos de tales procesos son procesos químicos en los que han de mantenerse parámetros críticos imprescindiblemente en una gama predeterminada, controles de máquina complejos, como por ejemplo en una prensa hidráulica o en una línea de fabricación, en los que por ejemplo la puesta en funcionamiento de una herramienta de prensa o cortadora puede significar un proceso parcial relevante para la seguridad. Otros ejemplos de procesos (parciales) relevantes para la seguridad son la vigilancia de rejas de protección, puertas de protección o barreras de luz, el control de interruptores a dos manos o también la reacción a interruptores de emergencia.

Así es imprescindible que los correspondientes datos de seguridad generados o captados y/o medidos se transporten con rapidez y sin falseamiento alguno.

Para responder a las exigencias de seguridad, ha habido en los últimos años numerosos acuerdos, que exigen un transporte de datos casi libre de errores cuando se utilizan sistemas de bus. Éstos se refieren en particular al propio transporte de datos, así como a una probabilidad de error residual admisible en función de la correspondiente aplicación o del correspondiente proceso. Como estándares vigentes citaremos aquí en particular el EN 61508 y el EN 954-1, así como el GS-ET-26 relativo a los principios para la prueba y certificación de "Sistemas de bus para la transmisión de mensajes relevantes para la seguridad" del organismo de prueba y certificación de las asociaciones profesionales industriales.

En función de estos acuerdos y normas se han desarrollado para distintos sistemas de bus/red en cada caso mecanismos de seguridad específicos para transmitir datos de seguridad con elevada redundancia. Los posibles errores se descubren a tiempo y puede prevenirse el peligro. Ejemplos de ello son entre otros el Safety Bus P, Profibus F, Interbus Safety, CAN Safety, entre otros.

Estos mecanismos de seguridad específicos desarrollados al respecto en particular en el marco de la técnica de control y automatización permiten así un reequipamiento sencillo y económico de los sistemas de bus (de campo)/red ya existentes en cada caso, utilizados entre unidades individuales que participan en un proceso para la comunicación de datos, para la transmisión de datos de seguridad, en particular entre sensores, actuadores y/o equipos de control.

El documento EP 1 188 096 B1 da a conocer por ejemplo un sistema de control para un proceso relevante para la seguridad con un bus de campo, mediante el cual están conectadas una unidad de control para controlar el proceso relevante para la seguridad y una unidad de señalización combinada mediante canales de entrada/salida con el proceso relevante para la seguridad. Para garantizar una comunicación segura frente a faltas entre las mismas, presentan estas unidades equipos orientados a la seguridad, mediante los cuales unidades que de por sí no son seguras deben transformarse en unidades seguras. En detalle está prevista una estructura de procesamiento multicanal realizada mediante ordenador, mediante la que puede detectarse y dado el caso corregirse un error en un canal de procesamiento en base a un resultado que se desvía del de otro canal de procesamiento redundante.

Bajo el concepto de ordenador ha de entenderse a continuación esencialmente cualquier tipo de equipos de procesamiento de datos, como microcomputadores, microprocesadores, microcontroladores o también PCs.

También el documento WO 01/15385 A2 se refiere al control de procesos relevantes para la seguridad utilizando un sistema de bus (de campo) basado en un mecanismo de seguridad, en el que las unidades que participan en el control del proceso relevante para la seguridad presentan a su vez por lo general canales de procesamiento constituidos redundantes. Cada uno de los canales redundantes incluye un ordenador, controlándose los mismos entre sí. Esta estructura multicanal se transforma mediante otro ordenador unido con el bus de campo en una estructura monocanal.

Del documento WO 01/15391 A1 y del documento de publicación DE 199 39 567 A1 pueden tomarse otros ejemplos de usuarios de bus seguros. Se prevé un mecanismo de seguridad con canales de procesamiento que se controlan entre sí en cuanto a la realización de un protocolo seguro, realizados

redundantes, y/u ordenadores y una transición a continuación de la bicanalidad a la monocanalidad mediante otro ordenador acoplado al bus, conectado a un chip del protocolo o que ha integrado el mismo.

La memoria de patente DE 195 32 639 C2 relativa a otro equipo para la transmisión monocanal de datos formados mediante dos ordenadores redundantes integra, para reducir el coste de los circuitos, la función del acoplamiento del bus en uno de ambos ordenadores realizados redundantes.

Además describe el documento DE 100 65 907 A1 un mecanismo de seguridad basado en el principio de una "redundancia con comparación cruzada" para el transporte de datos asegurado relativo a la transmisión de datos en redes o buses en paralelo o en serie, utilizándose un registro intermedio con dos zonas de datos idénticas lógicamente para la transición de la bicanalidad a la monocanalidad.

Basándose en la transición de la multicanalidad a la monocanalidad, se refiere la solicitud alemana con el número de expediente DE 10 2004 039932.8 entregada por el solicitante de la presente invención el 17 de agosto de 2004 a otra vía para un acoplamiento de bus seguro de procesos relevantes para la seguridad, quedando asegurada la ausencia de retroactividad y la independencia en la confección de un protocolo relativo a la seguridad. La solicitud con el número de expediente DE 10 2004 039932.8 prevé al respecto, para el acoplamiento de bus monocanal de un proceso crítico para la seguridad, un procedimiento en el que se procesa un bloque de datos relevante para el proceso crítico para la seguridad mediante al menos dos canales de procesamiento redundantes según normas idénticas para llegar en cada caso a un protocolo orientado a la seguridad y los protocolos redundantes orientados a la seguridad se reúnen para el acoplamiento de bus monocanal de nuevo para formar un protocolo común orientado a la seguridad, precisamente accediendo cada canal de procesamiento a un registro intermedio común, otorgándose para cada lugar del registro una autorización de escritura sólo una vez, tal que el protocolo común orientado a la seguridad, es decir, el telegrama de seguridad a transmitir, se componga por partes mediante certificación en cada caso de partes distintas de los correspondientes protocolos orientados a la seguridad.

Una tarea de la presente invención consiste en proporcionar una vía para acoplar los más diversos sistemas de bus de campo o de red con respectivos mecanismos de aseguramiento propios tal que la transmisión de datos de seguridad entre al menos dos sistemas de bus/red quede garantizado con distintos mecanismos de aseguramiento.

Marcos M. y colab. describen 1997 en la serie PROCEEDINGS IEEE (actas IEEE) bajo el número XP-000995489 en las páginas 349 a 353 en el artículo “On the Design and Development of a Gateway between MAP-MMS and PROFIBUS/FMS” (En el diseño y desarrollo de una pasarela entre MAP-MMS y PROFIBUS/FMS) un procedimiento que hace posible el acoplamiento entre dos sistemas propietarios diferentes de bus de campo/red SINEC H1 y SINEC L2, así como la transmisión transparente de datos entre ambos sistemas de bus de campo/red, utilizando tanto SINEC HI como también SINEC L2, inclusive a partir de la quinta capa del modelo de referencia OSI los mismos protocolos propietarios SINEC AP (Automation Protocol, protocolo de automatización) y SINEC TF (Technological Functions, funciones tecnológicas). Puesto que la forma de funcionamiento de una pasarela descrita en este estado de la técnica para realizar el procedimiento se basa en esta base común de ambos sistemas de bus de campo/red, especialmente en el protocolo SINEC TF con su biblioteca de funciones y en el concepto del Virtual Manufactoring Device (VMD, aparato de fabricación virtual), no puede utilizarse la pasarela para acoplar otros sistemas de bus de campo/red distintos con mecanismos/protocolos de transmisión en cada caso diferentes, en particular en cada caso propietarios, no pudiéndose deducir además del estado de la técnica ninguna indicación sobre que la pasarela también transmita con seguridad datos de seguridad entre el sistema de red SINEC H1 y el sistema de bus de campo SINEC L2 y por lo tanto utilice cualquier mecanismo de seguridad. Basándose en ello se indica además en este estado de la técnica que el objetivo actual es el desarrollo de una pasarela para acoplar los dos sistemas de bus de campo/red propietarios diferentes SINEC HI-MAP/MMS y Profibus/SINEC L2-FMS. Ciertamente no se describe ninguna implementación de este tipo de una pasarela, pero estaría configurada una tal implementación de pasarela, al igual que la implementación de pasarela descrita para SINEC H1-TF y SINEC L2-TF para una conversión directa del tipo que sea entre dos sistemas de bus de campo y/o red especiales. La solución correspondiente a la invención resulta ya de manera extremadamente sorprendente mediante un objeto con las características de una de las reivindicaciones independientes anexas.

Ventajosas y/o preferentes formas de ejecución y perfeccionamientos son objeto de las correspondientes reivindicaciones dependientes.

Así, está previsto en el marco de la invención, para el acoplamiento de al menos dos sistemas de bus (de campo)/red con respectivos distintos mecanismos de seguridad, en particular respectivos mecanismos de seguridad propietarios, procesar datos de seguridad a transmitir entre los distintos mecanismos de seguridad basados en el sistema utilizando adicionalmente una estructura de datos segura definida, pero independiente del sistema.

Un dispositivo correspondiente a la invención para acoplar al menos dos sistemas de bus (de campo)/red, que presenta respectivos distintos mecanismos de seguridad, en particular respectivos mecanismos de seguridad propietarios, para convertir datos de seguridad en una estructura de datos segura dependiente del sistema y/o a la inversa, incluye para ello al menos un primer y un segundo módulo de procesamiento de datos orientado a la seguridad para procesar datos de seguridad a transmitir entre los distintos mecanismos de seguridad basados en el sistema, utilizando una estructura de datos segura definida, pero independiente del sistema.

Una ventaja esencial de la invención ha de considerarse en consecuencia que es que de manera sencilla puede establecerse una relación de comunicación segura independiente de cualquier sistema de bus (de campo)/red y con ello esencialmente local entre los más diversos sistemas de bus (de campo)/red y se evita una conversión directa entre dos mecanismos de seguridad diferentes de diversos sistemas de bus (de campo)/red con los mecanismos de conversión seguros a adaptar de manera diferente que son necesarios para ello en cada caso. De esta manera pueden acoplarse por primera vez también sistemas de bus (de campo)/red con mecanismos de seguridad propietarios diferentes en cada caso.

Como "propietario" en el sentido de la invención se denomina al respecto, así como a continuación y en las reivindicaciones en general, un hardware o un software que sólo puede utilizarse en un sistema y no es compatible con otro hardware o software afín.

De manera conveniente está previsto para ello que cada uno de los módulos de procesamiento de datos esté acoplado con uno de los mecanismos de aseguramiento basados en el sistema, estando configurado al menos un módulo de procesamiento de datos para convertir datos de seguridad existentes a transmitir en monocanal o multicanal a la estructura de datos segura definida, pero independiente del sistema y al menos otro módulo de procesamiento de datos está configurado para la evaluación orientada a la seguridad de la estructura de datos segura independiente del sistema para proporcionar datos de seguridad existentes en monocanal o multicanal.

Preferiblemente está configurado cada módulo de procesamiento de datos para la conversión en ambos sentidos de acoplamiento y pueden, de manera extremadamente flexible y utilizable de forma polivalente, convertir datos de seguridad a transmitir entre los sistemas antes de su transmisión en la estructura de datos segura definida, pero independiente del sistema, a partir de una estructura de datos segura existente en multicanal o monocanal y dependiente del sistema y/o convertir los datos de seguridad a transmitir, tras su transmisión en la estructura de datos segura, definida pero independiente del sistema, en una estructura de datos segura, dependiente del sistema, multicanal o monocanal.

En particular prevé la invención que una estructura de datos a convertir en cada caso de una estructura de datos segura en otra estructura de datos segura, se evalúe ventajosamente primeramente de forma orientada a la seguridad y se convierta un bloque de datos existente tras la evaluación en mono o multicanal y que contiene “datos primarios” evaluados en la correspondiente otra estructura de datos segura. Los módulos de procesamiento de datos seguros están así esencialmente desligados de cualquier exigencia de seguridad dependiente del sistema.

En una ejecución especialmente preferente se transmiten los datos de seguridad procesados utilizando adicionalmente una estructura de datos segura definida, pero independiente del sistema dentro de una unidad que participa en un proceso a controlar, entre un equipo de la unidad orientado a la seguridad y que procesa datos de seguridad relevantes para este proceso y al menos una conexión de bus (de campo)/red de la unidad. Para ello están integrados los módulos de procesamiento de datos de manera conveniente en la unidad que participa en el proceso a controlar tal que al menos uno de los módulos de procesamiento de datos, de los que al menos hay dos, esté integrado en el equipo orientado a la seguridad y al menos otro de los módulos de procesamiento de datos con la conexión de bus (de campo)/red.

Una forma de ejecución especialmente preferente prevé que un bloque de datos de entrada/salida existente en monocanal o en multicanal del proceso a controlar se convierta en una estructura de datos definida, pero segura e independiente del sistema o bien se obtenga a partir de ésta mediante evaluación de la estructura de datos definida, segura pero independiente del sistema. Para ello está configurado de manera conveniente al menos un módulo de procesamiento de datos integrado en el equipo orientado a la seguridad para convertir datos de seguridad del proceso a controlar que incluyen un bloque de datos de entrada/salida existentes en monocanal o multicanal en una estructura de datos segura definida pero independiente del sistema y/o para evaluar la estructura de datos segura definida, pero independiente del sistema para aportar en mono o en multicanal un bloque de datos de seguridad que incluye datos de entrada/salida.

La unidad puede ser para ello una unidad de usuario que incluye al menos una entrada y/o salida mono o multicanal para la conexión de un proceso a controlar, con lo que también pueden integrarse entradas/salidas seguras de un proceso relevante para la seguridad utilizando la invención. Cuando se integran mediante el equipo orientado a la seguridad entradas/salidas seguras, pueden existir estos datos

de entrada de seguridad ya como “datos primarios”. No obstante, la unidad puede ser también una unidad de control que genera por ejemplo datos de seguridad a procesar. Así en consecuencia es ventajoso además que quede garantizada la integración tanto de datos de seguridad basados en bus/red como también basados en entradas/salidas locales en el acoplamiento correspondiente a la invención de distintos mecanismos de aseguramiento.

Esencialmente cada unidad de usuario de bus o unidad de control de bus existente puede adaptarse así ya mediante una ligera modificación para el acoplamiento correspondiente a la invención, extremadamente flexible, de distintos sistemas y puede así aportarse también con funcionalidad de pasarela integrada. Tales unidades configuradas según la invención para realizar el procedimiento incluyen unidades configuradas específicamente para la aplicación, también modulares, por ejemplo INLINE y la conexión de bus/red puede integrarse en consecuencia también en una estación INLINE incluida en la unidad.

Mediante el desplazamiento del correspondiente sistema de comunicación propietario para la transmisión de datos segura desde el equipo orientado a la seguridad, resulta la ventaja adicional de unas prestaciones esencialmente mayores, ya que el equipo referido a la seguridad no queda cargado, o sólo ligeramente, con estas tareas de comunicación, lo cual repercute por ejemplo además positivamente en los tiempos de recorrido para la pila TCP/IP o Profinet.

La conversión en las estructuras de datos seguras independientemente del sistema se realiza preferiblemente de forma asegurada para una transmisión monocanal, preferiblemente según la funcionalidad de aseguramiento publicada en el documento DE 10 2004 039932.8, utilizándose así para la transmisión de tales estructuras de datos aseguradas independientemente del sistema entre los correspondientes módulos de procesamiento de datos, de manera conveniente y económica, también esencialmente cualesquiera estructuras de hardware, por ejemplo microprocesadores como USC4, buses serie como I^2C o SPI y/o varias memorias de acoplamiento o registros intermedios por ejemplo en forma de DPM (Dual Port Memory, memoria de puerto dual), dentro de la unidad.

Para el aseguramiento de las estructuras de datos seguras independientemente del sistema incluyen los módulos de procesamiento de datos en consecuencia preferentemente al menos dos unidades de módulo redundantes, que interactúan, estando acopladas las unidades modulares por el lado de salida con un componente de acoplamiento no seguro para la transferencia de una estructura de datos asegurada común independientemente del sistema a este componente de acoplamiento y/o por el lado de entrada con un componente de acoplamiento no seguro para la lectura orientada la seguridad de una estructura de datos asegurada independientemente del sistema a partir de este componente de acoplamiento.

Para cumplir las exigencias de aseguramiento, se asegura la conexión de comunicación interna mediante un componente no seguro que se encuentra en otra configuración preferente en monocanal en un sistema de control seguro de una unidad que participa en un proceso crítico para la seguridad y las unidades situadas a continuación mediante mecanismos de aseguramiento listados en IEC 61508 para zonas de memoria variables e interfaces de comunicación según SIL 3, es decir, en particular mediante CRC, expectativas en el tiempo o bien mecanismos time-out (de tiempo de cierre).

La invención hace así posible de manera sencilla una integración basada en la seguridad de equipos específicos referidos a la seguridad, por ejemplo un control Interbus seguro también en unidades con otras interfaces de bus (de campo)/red. También la aportación de una unidad configurada según la invención con funcionalidad de pasarela segura integrada hacia diversos sistemas de red se encuentra en el marco de la invención.

Los módulos de procesamiento de datos pueden incluir hardware o software específicamente para cada aplicación, con lo que los mismos pueden integrarse en unidades basadas en los sistemas más diversos ya con sólo una ligera modificación del firmware de comunicación ya utilizado y esencialmente sin modificación de estructuras de hardware.

La invención hace posible así en general el acoplamiento de unidades con un determinado equipo referido a la seguridad a otros sistemas de comunicación referidos a la seguridad, pudiendo recurrirse también de manera efectiva, con la correspondiente modificación, a técnicas y procedimientos acreditados, con lo que queda asegurado un elevado grado de reutilización y una gran modularidad. Así puede acoplarse entre otros por ejemplo una unidad con un equipo referido a la seguridad basado en el INTERBUS, por ejemplo un sistema de control seguro integrado como placa insertable o en la configuración del conjunto (layout) de una unidad que participa en un proceso crítico para la seguridad, a otros sistemas de comunicación referidos a la seguridad, como por ejemplo CAN SAFETY, PROFISAFE, entre otros.

La invención incluye por lo tanto además un medio legible por ordenador con informaciones allí memorizadas que, leídas por un ordenador, en particular por un ordenador de una unidad de bus o de red que participa en un proceso a controlar, para realizar el procedimiento correspondiente a la invención, interactúan con el mismo.

La invención se describirá a continuación más en detalle en base a ejemplos de ejecución preferentes, con referencia a los dibujos adjuntos. En los dibujos muestran:

figuras 1a y 1b dos esquemas funcionales de circuitos muy simplificados, en cada caso de una adaptación directa de una estructura de hardware de 2 canales de un equipo referido a la seguridad de una unidad que participa en un proceso a controlar a una conexión de bus de campo para un bus de campo con otro mecanismo orientado a la seguridad según la invención,

figura 2 un esquema funcional de circuitos muy simplificado de una realización a modo de ejemplo de una pasarela entre dos sistemas de bus de campo seguros distintos según la invención, y

figuras 3a y 3b dos esquemas funcionales de circuitos muy simplificados de un ejemplo de un flujo de datos correspondiente a la invención entre una IB Safety (Interbus de seguridad) y una estructura de datos segura independiente del sistema o bien entre la estructura de datos segura independiente del sistema y la IB Safety, basándose en el esquema funcional de circuitos de la figura 2.

El acoplamiento correspondiente a la invención se describirá a continuación a modo de ejemplo en base a un equipo referido a la seguridad de una unidad que participa en un proceso a controlar con un bus/red con mecanismo de aseguramiento propietario, en particular con referencia a un bus con mecanismo de aseguramiento basado en CAN y un equipo referido a la seguridad basado en INTERBUS para procesar datos de seguridad para el control de una unidad que participa en un proceso crítico para la seguridad.

Primeramente nos referiremos a las figuras 1a y 1b, que muestran dos esquemas funcionales de circuitos muy simplificados de unidades de usuario de bus configuradas según la invención, que proporcionan la correspondiente adaptación directa de una estructura de hardware de 2 canales de un equipo integrado referido a la seguridad a otra conexión de bus de campo orientada a la seguridad según la invención.

En general se dibuja esquemáticamente en la figura 1a una forma de ejecución en la que dos nodos de bus de campo o bien chips de protocolo actúan sobre un bus del campo 401 con mecanismo de aseguramiento propietario de forma redundante, como por ejemplo en diversas soluciones CAN. En esta forma de ejecución representada, tal como se muestra con las referencias 301 y 302, integran microprocesadores µC1 y µC2 acoplados al bus 401 el correspondiente chip de protocolo, mediante el cual se acoplan al bus 401 o bien se desacoplan del bus 401 datos (BS) basados en la seguridad 321 y 322 formados con el mecanismo de aseguramiento propietario. En la figura 1b actúa sobre el bus 402 un sistema con mecanismo de aseguramiento propietario y por lo tanto para el acoplamiento o desacoplamiento de datos 331 y 332 formados mediante un mecanismo de aseguramiento propietario sólo está conectado un nodo de bus de campo o bien chip de protocolo 313 a los dos microprocesadores µC1 y µC2, 311 y 312 respectivamente, con lo que aquí por lo tanto resulta una transición entre una bicanalidad y una monocanalidad, como por ejemplo en Profisafe. Tanto en la figura 1a como también en la figura 1b resulta así para el acoplamiento a bus un mecanismo de aseguramiento propietario con dos ordenadores o canales de procesamiento que funcionan de forma redundante para confeccionar un protocolo seguro para el acoplamiento a bus y para la evaluación del protocolo seguro para el acoplamiento a bus.

La secuencia descrita a continuación según la figura 1a se refiere al acoplamiento a bus de datos de seguridad, que se obtienen mediante dos canales de aseguramiento SK1 y SK2 del equipo referido a la seguridad señalados con las referencias 101 y 102 que procesan datos de entrada/salida. Los canales de aseguramiento 101 y 102 incluyen aquí en realización práctica respectivas CPU con los componentes periféricos necesarios. Un watchdog (perro guardián) 105 asociado vigila y garantiza la funcionalidad.

En el caso de una unidad de usuario de bus según la figura 1a está conectado cada uno de los canales de aseguramiento 101 y 102 que procesan datos de seguridad con las unidades de entrada y/o salida no representadas asociadas al proceso crítico para la seguridad a acoplar, como por ejemplo sensores y/o actuadores. A una unidad de usuario de bus con aplicación del lado del sensor se le proporcionan así datos de entrada relevantes para el proceso crítico para la seguridad, preferiblemente idénticos, a los canales de aseguramiento 101 y 102 y se memorizan primeramente de forma conveniente. En particular en el caso de una unidad de control de bus se encuentran los datos de entrada a asegurar por ejemplo en las correspondientes memorias.

Los datos de entrada redundantes se procesan a continuación mediante unidades modulares LSL integradas, señaladas con 10, de los canales de aseguramiento 101 y 102 para formar datos comunes con una estructura de datos asegurada localmente, es decir, asegurada independientemente del sistema de bus (de campo)/red. Esta estructura de datos o de protocolo asegurada independientemente del sistema de bus (de campo)/red se denominará a continuación LSL (Local Safety Layer, capa de seguridad local).

Utilizando preferentemente un mecanismo de seguridad dado a conocer mediante la solicitud DE 10 2004 039932.8 a la que hacemos referencia, se procesan los datos de entrada presentes como datos primarios básicamente de forma redundante utilizando las mismas normas para formar en cada caso un protocolo orientado a la seguridad que, siempre que en el cálculo no se haya presentado ningún error o fallo, son idénticas y cumplen las exigencias de la norma relativa a una transmisión orientada a la seguridad. A continuación se procesa a partir de los protocolos de redundantes orientados a la seguridad una LSL común, con lo que pueden transferirse a continuación los datos LSL señalados con 215 en monocanal, por ejemplo basándose en una unión punto a punto con la conexión de bus de campo/red con anchura de datos variable para el sistema propietario a acoplar.

Los datos LSL 215 asegurados mediante la LSL pueden transmitirse así a través de estructuras de hardware no seguras y se forman utilizando el mecanismo de seguridad dado a conocer en la solicitud DE 10 2004 039932.8 mediante una composición proporcional de datos de los protocolos redundantes orientados a la seguridad en una memoria intermedia o registro intermedio señalado con la referencia 200, por ejemplo la DPM mostrada.

La consideración de seguridad de la arquitectura redundante puede finalizar con referencia a las unidades modulares LSL 10 así como básicamente archivando los datos LSL 215 en la memoria no segura 200. A partir de aquí interviene el mecanismo de seguridad de la LSL, ya que a partir de aquí se tienen en cuenta como hasta ahora posibles errores para la transmisión siguiente y deben dominarse. Un error a considerar al respecto procedente del principio básico para la prueba y certificación de "sistemas de bus para la transmisión de mensajes relevantes para la seguridad", es un falseamiento del mensaje.

En la correspondiente conexión del bus de campo de la unidad de usuario del bus, se evalúan no obstante de manera orientada a la seguridad los datos LSL 215 en función de la definición LSL a su vez mediante unidades modulares LSL 10. Esta evaluación tiene lugar según las figuras 1a y 1b preferiblemente con una redundancia de 2 canales con o sin diversidad. Los datos evaluados se introducen a continuación a su vez como datos primarios en el protocolo de bus-red propietario orientado a la seguridad propiamente dicha. Rigen entonces los mecanismos de aseguramiento propietarios del correspondiente sistema seguro acoplado según los cuales se generan los correspondientes datos seguros SB (orientados a la seguridad) 321 y 322 según la figura 1a o bien 331 y 332 según la figura 1b a partir de los datos primarios y se acoplan al bus 401 y 402 respectivamente.

La vía de comunicación opuesta, igualmente incluida en la invención, de datos BS seguros 321 y 322 a desacoplar del bus 401 ó 402 según la figura 1a o bien 331 y 332 según la figura 1b en dirección a los canales de seguridad 101 y 102 hacia unidades de salida asociadas, se proporciona no obstante viceversa de forma esencialmente igual. Las estructuras de datos seguras dependientes del sistema se evalúan así primeramente de forma orientada a la seguridad mediante los respectivos mecanismos de seguridad propietarios y los "datos primarios" evaluados se convierten a continuación de manera orientada a la seguridad para la transmisión entre la correspondiente conexión de bus de campo y el equipo orientado a la seguridad mediante las unidades modulares LSL 10 integradas en el mismo en la estructura de datos LSL segura independiente del sistema.

Así se prevé para la composición proporcional del protocolo específico de la aplicación, existente de forma redundante y orientado a la seguridad, o dado el caso específico de la aplicación para la composición proporcional de los datos primarios existentes de forma redundante para formar la LSL a transmitir en monocanal utilizando el mecanismo de seguridad dado a conocer en la solicitud DE 10 2004 039932.8, preferiblemente una regla de acceso definida o que puede definirse, que ciertamente otorga a las unidades modulares LSL 10 plenos derechos de lectura sobre la memoria intermedia 200, pero controla los derechos de escritura sobre la memoria intermedia 200. La regla de acceso determina al respecto que de cada una de las unidades modulares LSL redundantes 10 sólo pueden escribirse las partes del correspondiente protocolo calculado orientado a la seguridad para formar la LSL en los correspondientes lugares de memoria de la memoria intermedia 200 para los que las correspondientes unidades modulares LSL 10 tengan el correspondiente derecho de escritura. Para cada lugar de la memoria o del registro se define por lo tanto en el marco de la invención para un sentido de comunicación preferentemente sólo en cada caso un derecho de escritura.

Así por un lado están ambas unidades modulares LSL 10 en condiciones de calcular los datos LSL completos, lo cual repercute positivamente en la longitud necesaria para la estructura de datos, ya que todos los bits de datos con los distintos mecanismos de seguridad se conocen ya previamente en las unidades modulares LSL 10 redundantes y no tiene que transmitirse ningún tipo de datos adicional que permita en el lado receptor la conclusión de que el cálculo es correcto. Además queda asegurado que una unidad modular LSL 10 por sí sola no está en condiciones de enviar un LSL, representando el control sobre el derecho de escritura, que en cada caso sólo puede otorgarse una vez, de datos en un lugar del registro, una posibilidad fácil de implementar y muy eficiente para que independientemente de la LSL y del sistema utilizado quede garantizada una seguridad mucho mayor con poco coste.

El acceso completo a la lectura de la memoria intermedia 200 posibilita una comparación sencilla de todos los datos, ya que por un lado puede comprobarse de manera sencilla si la LSL formada conjuntamente, que por ejemplo cumple las exigencias de seguridad para una transmisión sencilla según SIL 3 IEC 61508, está libre de errores, precisamente mediante la correspondiente verificación respecto al protocolo propio orientado a la seguridad formado antes separadamente. Además permite el acceso a lectura en toda su extensión para cada una de las unidades modulares LSL 10 la comprobación que puede realizarse de manera conveniente ya al principio del control/vigilancia/regulación de un proceso crítico para la seguridad relativo a si la regla de acceso en general se cumple sin errores. Para ello se comprueba en particular si los datos calculados de la correspondiente unidad modular 10 de los canales de procesamiento redundantes se escriben exclusivamente, pero con garantía, en las direcciones de memoria asignadas en cada caso de la memoria intermedia 200.

Además posibilita el acceso de lectura completo a la memoria intermedia 200 la evaluación de datos LSL 210 mediante cada unidad modular LSL 10 con comparación mutua subsiguiente en cuanto a si son correctos.

En cuanto a otras explicaciones adicionales al respecto, remitimos de nuevo a la publicación de la solicitud DE 10 2004 039932.8.

Mediante la aplicación de la invención queda garantizada así una estructura flexible, independiente del bus, modular, orientada a la seguridad de comunicación y de hardware en una unidad de usuario de bus/control de bus. En particular en el caso de un equipo orientado a la seguridad integrado o que puede integrarse en una tal unidad de usuario de bus/control de bus con superficie de programación, queda además asegurado un elevado valor de reutilización como plataforma.

La invención hace posible en consecuencia un acoplamiento rápido a sistemas existentes o futuros de bus de campo/red, manteniéndose las elevadas prestaciones del equipo orientado a la seguridad de la unidad de bus, ya que la comunicación se desplaza con el sistema de bus (de campo)/red a acoplar.

Además pueden realizarse de manera sencilla mediante la aplicación de la invención funciones de pasarela entre los más diversos sistemas de bus (de campo)/red propietarios orientados a la seguridad, tal como se describirá a continuación más en detalle en base al ejemplo de una CAN Safety Application (aplicación de seguridad CAN) junto a una comunicación INTERBUS Safety (de seguridad).

Primeramente nos referimos al respecto a la figura 2, designando las mismas referencias componentes iguales o de igual funcionalidad. Tal como puede verse en la figura 2, integra el equipo orientado a la seguridad de una unidad de usuario de bus correspondientemente adaptada unidades modulares LSL 10 redundantes adicionalmente a unidades modulares IB-Safety 30 redundantes construidas sobre un protocolo INTERBUS Safety con los canales de aseguramiento redundantes 101 y 102.

Una primera DPM no segura está acoplada como memoria de acoplamiento 201 para alojar/transferir los datos LSL 215 asegurados mediante la LSL y los datos IB-Safety 366 asegurados mediante el protocolo INTERBUS Safety con las unidades modulares 10, 30 referidas a la seguridad. La memoria de acoplamiento 201 está conectada con una unidad de control específica del INTERBUS o CPU 360 con chip de protocolo 361 integrado o externo, con lo que se proporciona un primer nodo de bus de campo basado en INTERBUS para un INTERBUS Safety Bus 403. Los datos de seguridad a acoplar o desacoplar desde o en el bus 403 mediante el chip del protocolo 361, se basan en el protocolo INTERBUS Safety y se encuentran presentes correspondientemente como datos IB-Safety 366. Adicionalmente pueden acoplarse y desacoplarse datos estándar no asegurados 365 mediante el chip del protocolo 361.

A esta unidad de control específica de INTERBUS o CPU 360 está conectada otra DPM como memoria de acoplamiento adicional 202, en la que está montada una conexión de bus CAN orientada a la seguridad. No obstante el acoplamiento puede también realizarse mediante otros medios, como por ejemplo mediante SPI, Wireless (inalámbrico), Multi Port Memory (memoria multi-puerto), PCI express.

La conexión de bus CAN orientada a la seguridad está constituida esencialmente tal como se describió respecto a la figura 1a, pudiendo acoplarse y desacoplarse también datos estándar no asegurados 305 mediante el µC1 con chip de protocolo 361 integrado. En la transición de la memoria de acoplamiento 202 a la estructura de 2 canales de la conexión de bus CAN pueden utilizarse correspondientemente de nuevo los mecanismos de seguridad antes descritos.

Opcionalmente puede estar conectada a la unidad de control específica de INTERBUS o CPU360 otra memoria de acoplamiento 371, en la que por ejemplo está previsto otro sistema de control opcional (seguro) 372.

En base a las figuras 3a y 3b se describirá a continuación a modo de ejemplo un flujo de datos basado en el esquema funcional de circuitos de la figura 2 entre una estructura de datos IB Safety y la estructura de

datos específica de otro sistema con mecanismo de aseguramiento propietario o bien entre la estructura de datos específica del otro sistema con mecanismo de aseguramiento propietario y la estructura de datos IB Safety, señalándose la zona que incluye estructuras de hardware no seguras con “NS” y la zona segura con “S”.

En la figura 3a se llevan a través de la conexión de bus de campo 360, 361 basada en INTERBUS datos IB-Safety desacoplados, asegurados en el marco de una funcionalidad de pasarela primeramente a la memoria de acoplamiento 201 para la transferencia posterior, por ejemplo mediante un microprocesador no representado. Desde la memoria de acoplamiento 201 se leen los datos IB-Safety 366 de las unidades modulares IB-Safety 30 redundantes del equipo referido a la seguridad y se evalúan para formar “datos primarios”. Estos “datos primarios” existentes de forma redundante se procesan a continuación mediante las unidades modulares LSL redundantes 10 del equipo referido a la seguridad para formar datos LSL asegurados localmente 215 y se llevan de nuevo a la memoria de acoplamiento 201 reunidos para la siguiente transferencia monocanal. Desde allí se llevan los datos LSL asegurados localmente 215, por ejemplo mediante un microprocesador no representado, a la memoria de acoplamiento 202, para la transferencia posterior. Desde la memoria de acoplamiento 202 se leen y evalúan los datos LSL 215 mediante las unidades modulares LSL redundantes 10 de la conexión de bus de campo para el sistema con mecanismo de seguridad propietario, por ejemplo para un CAN-Bus. En una ejecución alternativa, específica de la aplicación, se leen y a continuación evalúan datos LSL 215 después de la transferencia en al menos otro equipo de acoplamiento o directamente desde la memoria de acoplamiento 201 mediante las unidades modulares redundantes 10 de la conexión de bus de campo para el sistema con mecanismo de seguridad propietario. Los “datos primarios” evaluados existentes de forma redundante en la transición de la estructura monocanal a la estructura multicanal, se alojan a continuación mediante los microprocesadores redundantes, acoplados al sistema de bus (de campo)/red propietario con chip de protocolo 301 y 302 integrado en cada caso en el protocolo propietario orientado a la seguridad y se acoplan al sistema como datos SB 321 y 322 formados con el mecanismo de aseguramiento propietario.

En la figura 3b se representa la comunicación opuesta. Correspondientemente se desacoplan los datos SB asegurados mediante la conexión de bus de campo basada en el mecanismo de seguridad propietario y se llevan mediante las unidades modulares LSL orientadas a la seguridad los datos LSL correspondientemente asegurados localmente a la memoria de acoplamiento 202 para la transferencia posterior. Después de la transferencia posterior a la memoria de acoplamiento 201, se leen los datos LSL desde la misma mediante las unidades modulares LSL redundantes 10 del equipo referido a la seguridad y se evalúan para formar “datos primarios” 20. Estos “datos primarios” existentes de forma redundante se procesan a continuación mediante las unidades modulares IB-Safety redundantes 30 del equipo referido a la seguridad para formar datos IB-Safety y se conducen de nuevo reunidos a la memoria de acoplamiento 201 para la transferencia monocanal a continuación. Desde allí se transfieren los datos IB-Safety a la conexión de bus de campo basada en INTERBUS, para el acoplamiento al bus.

La memoria de acoplamiento 201 sirve así para la transferencia monocanal de datos asegurados específicamente para el sistema y asegurados localmente.

Tal como se ha descrito antes, pueden estar conectadas también mediante los canales de aseguramiento 101 y 102 entradas/salidas locales y pueden integrarse así también datos de seguridad de entrada y/o salida en la vía de comunicación correspondiente a la invención dentro de la unidad constituida dado el caso también modularmente.

REIVINDICACIONES

1. Procedimiento para acoplar al menos dos sistemas de bus de campo o de red con en cada caso distintos mecanismos de seguridad, configurados para convertir datos de seguridad a transmitir en una estructura de datos segura dependiente del sistema y/o para convertir datos de seguridad a transmitir desde una estructura de datos segura dependiente del sistema,
en el que el procedimiento **se caracteriza porque** los datos de seguridad a transmitir entre los distintos mecanismos de seguridad basados en el sistema, se procesan (10, 200, 201, 202, 215) utilizando adicionalmente una estructura de datos definida segura pero independiente del sistema (215), evaluándose, al convertir los datos de seguridad desde una estructura de datos segura, dicha estructura de forma orientada a la seguridad.

2. Procedimiento según la reivindicación precedente,
en el que al menos uno de los distintos mecanismos de seguridad de los sistemas de bus de campo o de red a acoplar correspondientes es un mecanismo de seguridad propietario.

3. Procedimiento según una de las reivindicaciones precedentes,
caracterizado además **porque** los datos de seguridad a transmitir entre los sistemas, antes de su transmisión, se convierten en la estructura de datos definida segura, pero independiente del sistema a partir de una estructura de datos segura dependiente del sistema (321, 322, 366), existente en multicanal o monocanal.

4. Procedimiento según una de las reivindicaciones precedentes,
caracterizado además **porque** los datos de seguridad a transmitir entre los sistemas, después de su transmisión en la estructura de datos definida segura, pero independiente del sistema, se convierten en una estructura de datos segura dependiente del sistema (321, 322, 366) multicanal o monocanal.

5. Procedimiento según una de las reivindicaciones precedentes,
caracterizado además **porque** una estructura de datos a convertir en cada caso de una estructura de datos segura en otra estructura de datos segura, se evalúa de forma orientada a la seguridad (10, 20, 301, 302, 311, 312) y se convierte (10, 20, 301, 302, 311, 312) un bloque de datos (20) existente tras la evaluación en mono o multicanal en la correspondiente otra estructura de datos segura.

6. Procedimiento según una de las reivindicaciones precedentes,
caracterizado además **porque** se transmiten los datos de seguridad procesados utilizando adicionalmente una estructura de datos segura definida, pero independiente del sistema (215), dentro de una unidad que participa en un proceso a controlar de uno de los sistemas a acoplar, precisamente entre un equipo referido a la seguridad y que procesa datos de seguridad relevantes para este proceso y al menos una conexión de bus (de campo)/red de la unidad.

7. Procedimiento según la reivindicación precedente,
caracterizado además **porque** un bloque existente en monocanal o en multicanal de datos de seguridad que contiene datos de entrada/salida del proceso a controlar, se convierte en una estructura de datos definida, pero segura e independiente del sistema o bien mediante evaluación de la estructura de datos definida, segura pero independiente del sistema, se obtiene a partir de ésta.

8. Procedimiento según una de las reivindicaciones precedentes,
caracterizado además **porque** la estructura de datos segura e independiente del sistema, se asegura para una transmisión monocanal.

9. Procedimiento según la reivindicación precedente,
caracterizado además **porque** el aseguramiento de la estructura de datos se realiza utilizando mecanismos de seguridad según IEC 61508 y SIL 3.

10. Procedimiento según una de ambas reivindicaciones precedentes,
caracterizado además **porque** la transmisión se realiza utilizando componentes no seguros (200, 201, 202).

11. Dispositivo para el acoplamiento de al menos dos sistemas de bus de campo o de red que presentan en cada caso distintos mecanismos de seguridad para convertir datos de seguridad a transmitir en una estructura de datos segura dependiente del sistema y/o a la inversa, incluyendo al menos un primer y un segundo módulo de procesamiento de datos (10) para procesar datos de seguridad a transmitir entre los distintos mecanismos de seguridad basados en el sistema, utilizando una estructura de datos segura definida (215), pero independiente del sistema, estando configurado al menos uno de los módulos de procesamiento de datos para la evaluación orientada a la seguridad de la estructura de datos segura independiente del sistema para proporcionar datos de seguridad.

12. Dispositivo según la reivindicación precedente,
en el que al menos uno de los correspondientes mecanismos de seguridad distintos de los sistemas de bus de campo o de red a acoplar, es un mecanismo de seguridad propietario.

13. Dispositivo según una de las reivindicaciones precedentes 11 ó 12,
caracterizado además **porque** cada uno de los módulos de procesamiento de datos (10) está acoplado con un mecanismo de aseguramiento (30, 301, 302, 311, 312) basado en el sistema, estando configurado al menos el primer módulo de procesamiento de datos, de los que al menos hay uno, para convertir datos de seguridad a transmitir existentes en monocanal o multicanal en la estructura de datos segura definida, pero independiente del sistema y al menos un segundo módulo de procesamiento de datos, de los que al menos hay uno, está configurado para la evaluación orientada a la seguridad de la estructura de datos segura independiente del sistema para proporcionar datos de seguridad existentes en monocanal o multicanal.

14. Dispositivo según una de las reivindicaciones precedentes 11 a 13,
caracterizado además **porque** los módulos de procesamiento de datos (10) están integrados en una unidad que participa en un proceso a controlar de uno de los sistemas a acoplar, estando al menos uno de los módulos de procesamiento de datos, de los que al menos hay dos, integrado en un equipo orientado a la seguridad que procesa datos de seguridad relevantes para este proceso y al menos otro de los módulos de procesamiento de datos, de los que al menos hay dos, con una conexión de bus de campo o de red de la unidad.

15. Procedimiento según la reivindicación precedente,
caracterizado además **por** al menos un módulo de procesamiento de datos integrado en el equipo referido a la seguridad para convertir datos de seguridad que incluyen un bloque existente en monocanal o multicanal de datos de entrada/salida del proceso a controlar en la estructura de datos segura definida, pero independiente del sistema y/o para la evaluación orientada a la seguridad de la estructura de datos segura definida pero independiente del sistema para proporcionar datos de seguridad que incluyen un bloque de datos de entrada/salida en monocanal o multicanal.

16. Dispositivo según una de ambas reivindicaciones precedentes,
caracterizado además **porque** la unidad es una unidad constituida modularmente.

17. Procedimiento según una de las tres reivindicaciones precedentes,
caracterizado además **porque** la unidad es una unidad de usuario de bus o una unidad de control de bus.

18. Procedimiento según una de las cuatro reivindicaciones precedentes,
caracterizado además **porque** la unidad está configurada como una unidad con funcionalidad de pasarela.

19. Procedimiento según una de las reivindicaciones precedentes 11 a 18,
caracterizado además **porque** los módulos de procesamiento de datos (10) están configurados para procesar una estructura de datos asegurada independiente del sistema para una transmisión monocanal entre en cada caso al menos dos módulos de procesamiento de datos.

20. Dispositivo según la reivindicación precedente,
caracterizado además **por** al menos un componente de acoplamiento no seguro (200, 201, 202) en la vía de transmisión para la transmisión monocanal entre los correspondientes módulos de procesamiento de datos.

21. Procedimiento según una de las reivindicaciones precedentes 11 a 20,
caracterizado además **porque** un módulo de procesamiento de datos incluye al menos dos unidades de módulo redundantes (10), que funcionan conjuntamente, estando acopladas las unidades modulares por el lado de salida con un componente de acoplamiento no seguro (200, 201, 202) para transferir una estructura de datos asegurada común independientemente del sistema a este componente de acoplamiento y/o estando acopladas por el lado de entrada con un componente de acoplamiento no seguro (200, 201, 202) para la lectura orientada la seguridad de una estructura de datos asegurada independientemente del sistema de este componente de acoplamiento.

22. Dispositivo según una de ambas reivindicaciones precedentes,
caracterizado porque un componente de acoplamiento no seguro incluye al menos un microprocesador, bus serie y/o memoria de acoplamiento (200, 201, 202), en particular en forma de una DPM.

23. Dispositivo según una de las reivindicaciones precedentes 11 a 22,
caracterizado porque los módulos de procesamiento de datos (10) incluyen hardware y/o software.

24. Medio legible por ordenador con informaciones allí memorizadas que, leídas por un ordenador, interactúan con el ordenador para realizar todas las etapas de procedimiento correspondientes al procedimiento según una de las reivindicaciones precedentes 1 a 10.

25. Medio legible por ordenador con informaciones allí memorizadas que, leídas por un ordenador de una unidad de bus o de red que participa en un proceso a controlar, dentro de un dispositivo según una de las reivindicaciones 11 a 23, interactúan con el ordenador para realizar todas las etapas del procedimiento según una de las reivindicaciones precedentes 1 a 10.

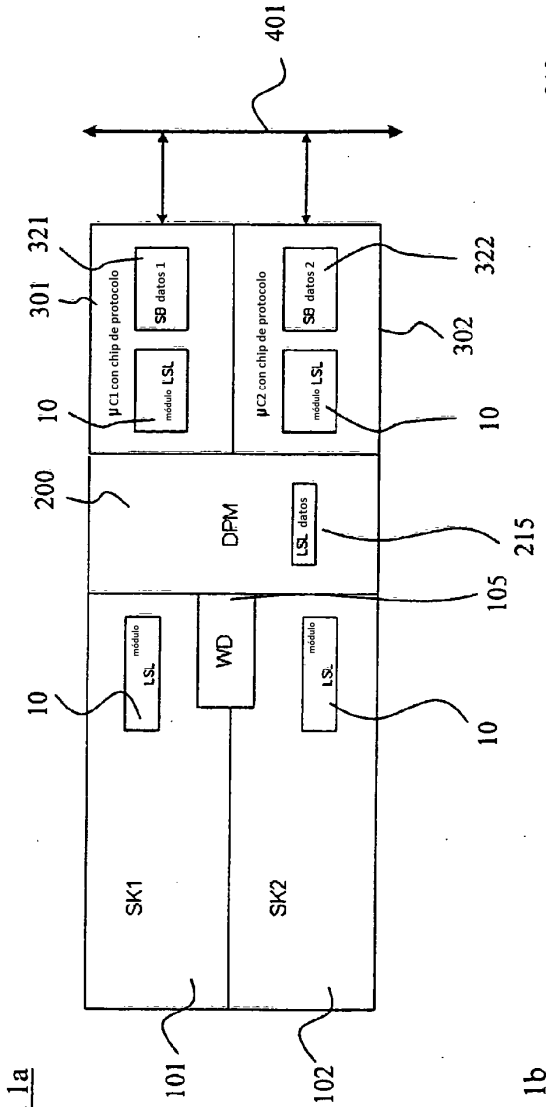
401
321
301
322
302
µC1 con chip de protocolo
SB datos 1
módulo LSL
µC2 con chip de protocolo
SB datos 2
módulo LSL
10
200
DPM
LSL datos
215
105
WD
SK1
SK2
101
102

Fig. 1a

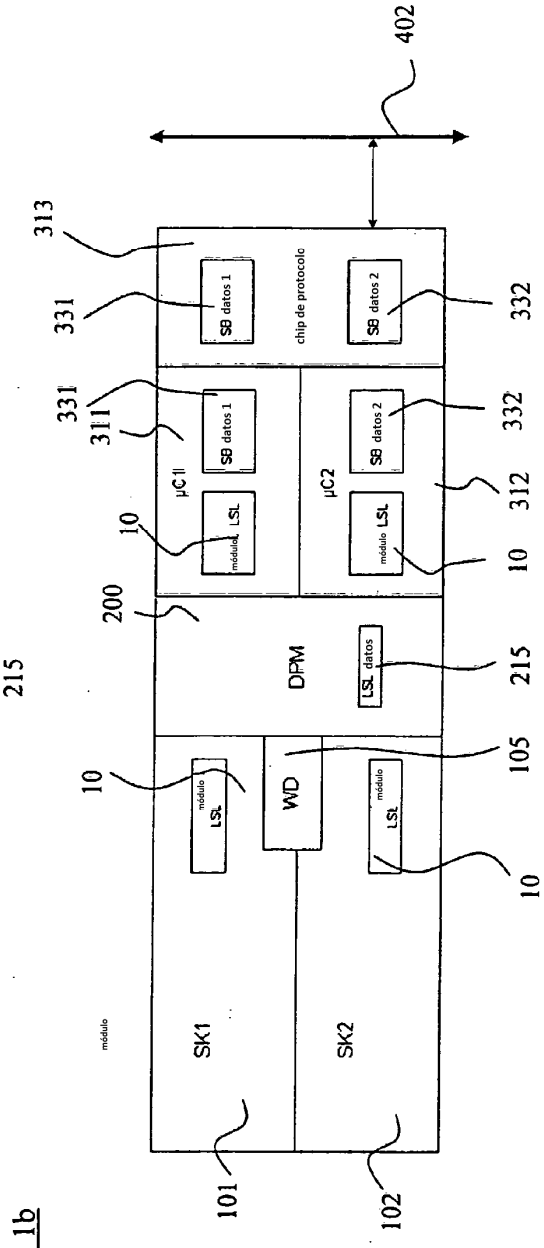
402
313
331
332
SB datos 1
chip de protocolo
SB datos 2
311
µC1
µC2
312
módulo LSL
10
200
DPM
LSL datos
215
105
WD
SK1
SK2
101
102

Fig. 1b

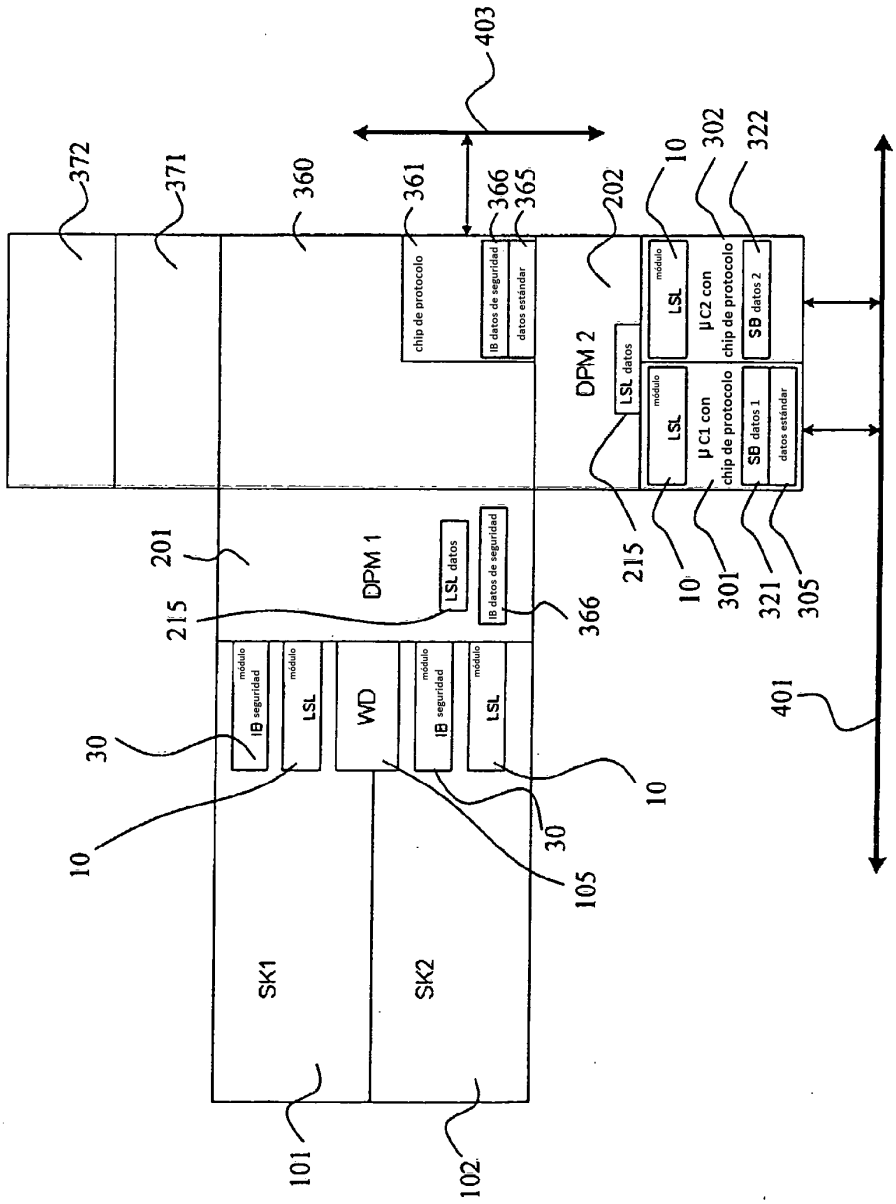
403
372
371
360
361
366
365
202
10
302
322
chip de protocolo
IB datos de seguridad
datos estándar
DPM 2
LSL datos
módulo
LSL
µC2 con chip de protocolo
SB datos 2
µC1 con chip de protocolo
SB datos 1
datos estándar
215
10
301
321
305
201
DPM 1
LSL datos
IB datos de seguridad
366
módulo
IB seguridad
LSL
WD
30
10
105
401
SK1
SK2
101
102

Fig. 2

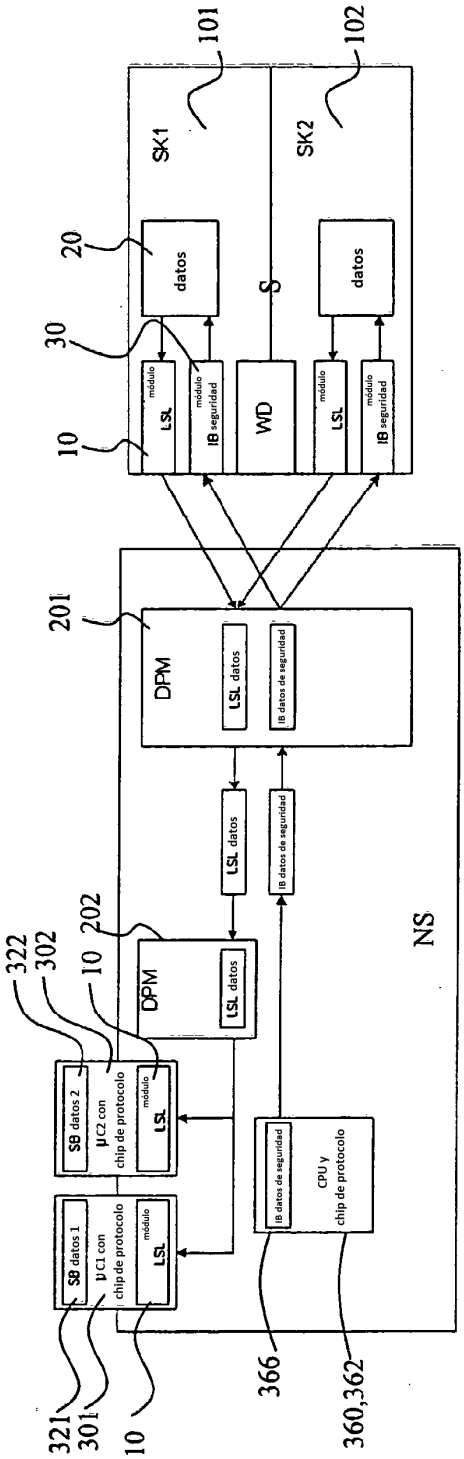
101
102
SK1
SK2
20
datos
30
módulo LSL
módulo IB seguridad
WD
S
10
201
DPM
LSL datos
IB datos de seguridad
NS
202
322
302
SB datos 2
µC2 con chip de protocolo
SB datos 1
µC1 con chip de protocolo
CPU y chip de protocolo
321
301
366
360,362

Fig. 3a

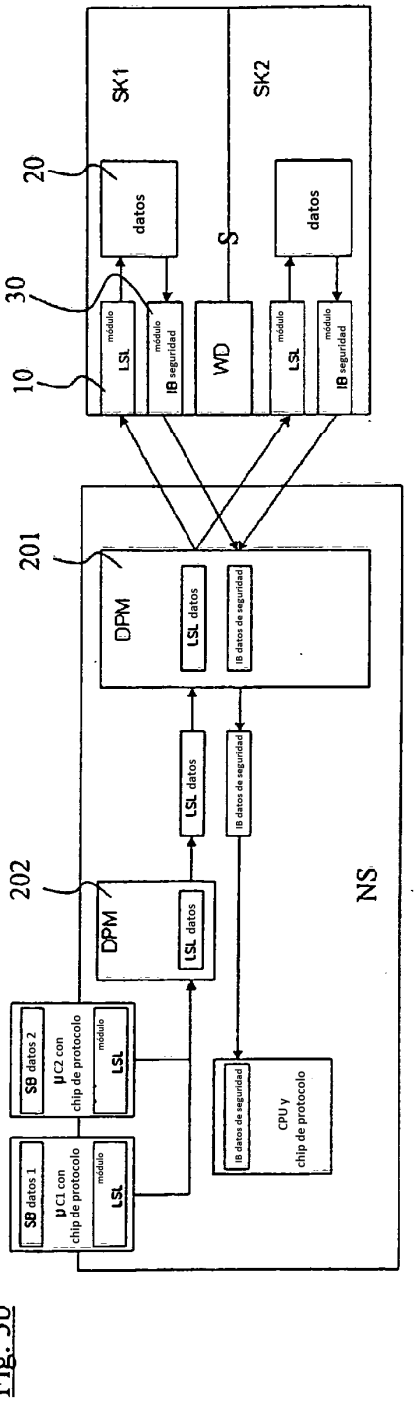
SK1
SK2
20
datos
30
módulo LSL
módulo IB seguridad
WD
S
10
201
DPM
LSL datos
IB datos de seguridad
NS
202
SB datos 2
µC2 con chip de protocolo
SB datos 1
µC1 con chip de protocolo
CPU y chip de protocolo

Fig. 3b