

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 377 186**

51 Int. Cl.:
H04L 12/403 (2006.01)
H04L 12/46 (2006.01)
G05B 19/00 (2006.01)
H04L 12/56 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **10009765 .8**
- 96 Fecha de presentación: **17.09.2010**
- 97 Número de publicación de la solicitud: **2302841**
- 97 Fecha de publicación de la solicitud: **30.03.2011**

54 Título: **Procedimiento y dispositivo para una comunicación orientada a la seguridad en la red de comunicaciones de una instalación de automatización**

30 Prioridad:
23.09.2009 DE 102009042354

45 Fecha de publicación de la mención BOPI:
23.03.2012

45 Fecha de la publicación del folleto de la patente:
23.03.2012

73 Titular/es:
Phoenix Contact GmbH & Co. KG
Flachmarktstrasse 8 - 28
32825 Blomberg, DE

72 Inventor/es:
Schmidt, Jochen y
Horn, Steffen

74 Agente/Representante:
Carvajal y Urquijo, Isabel

ES 2 377 186 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y dispositivo para una comunicación orientada a la seguridad en la red de comunicaciones de una instalación de automatización.

5 La invención se refiere en general a instalaciones de automatización y a sus sistemas de bus de automatización. En especial la invención se refiere a la comunicación entre módulos orientados a la seguridad en la red de comunicaciones de una instalación de automatización de este tipo.

10 Para reducir el riesgo para las personas o el medio ambiente es necesario con frecuencia prever funciones de seguridad en sistemas de bus de automatización, respectivamente en los abonados conectados a los mismos. Un ejemplo es la desconexión de una máquina conectada al sistema de bus de automatización después del accionamiento de un interruptor de desconexión de emergencia. Con esta finalidad se usan cada vez con más frecuencia sistemas de automatización a prueba de errores. Por lo general estos sistemas de automatización a prueba de errores materializan por un lado la verdadera función de seguridad, como por ejemplo conmutación bimanual, amortiguación de ruidos, interruptor selector de formas de funcionamiento, etc. y, por otro lado, también medidas de reconocimiento de errores y de control de errores, como las que están establecidas en las normas IEC 15 61508 e ISO1384.

20 En los sistemas de automatización actuales se utilizan, en función del grado de automatización y de la extensión de las instalaciones, sistemas de comunicación que unen aparatos de entrada/salida (aparatos E/A) descentralizados y controles. Para el transporte de datos de técnica de seguridad es con ello conocido apoyar la red mediante protocolos de red seguros. El flujo de señales utilizado se basa hasta ahora en una técnica de seguridad central, en la que las señales de entrada seguras se transportan hasta un control seguro, allí se tratan y después se transportan hasta los actuadores correspondientes. El tratamiento seguro recibe también el nombre de aplicación segura.

La solicitud de patente europea EP1533673 publica un sistema de control para controlar procesos críticos para la seguridad, con una comunicación a través de un bus de campo.

25 Los errores en la comunicación pueden estar presentes o producirse en el hardware y en el firmware de los aparatos de automatización, en los componentes de la infraestructura de las redes, por ejemplo componentes de bus de campo o Ethernet, y durante la transmisión de datos a causa de influencias externas. Las influencias externas pueden ser por ejemplo perturbaciones de la transmisión de datos a causa de campos electromagnéticos.

30 En la técnica de automatización pueden reconocerse actualmente dos tendencias. Por un lado existe la tendencia a descentralizar las funciones de control. Asimismo existe interés en la integración de la técnica de seguridad en la técnica de control y de redes.

En el caso de la descentralización se traslada la función de control cada vez más al plano de salida. De este modo puede integrarse por ejemplo la función de control, en un volumen limitado, en accionamientos.

35 Con la integración de la técnica de seguridad en controles y redes se crean evidentemente fuertes dependencias en el proceso de aplicación. Estas dependencias conducen a una planificación y programación más complejas de los sistemas. Esto está de algún modo en contradicción con el deseo de una sencillez en la manipulación de la técnica de seguridad. La complejidad en la planificación de aplicaciones orientadas a la seguridad es hasta ahora uno de los motivos esenciales para que la transición desde una técnica de seguridad convencional con cableado fijo, en especial sobre la base de relés de seguridad, sólo encuentre una aceptación lenta. En el caso de los actuales sistemas de bus de automatización seguros también puede llegarse, a causa de las dificultades antes citadas, a un uso defectuoso y una falta de disponibilidad de la instalación controlada a causa de las llamadas activaciones fallidas.

La invención se ha impuesto por tanto la tarea de simplificar la instalación y la planificación de módulos orientados a la seguridad en una red de automatización.

45 Una idea básica de la invención para resolver esta tarea consiste en dividir las funciones de seguridad de una instalación en pequeños grupos modulares, supervisables, limitables localmente y fácilmente verificables. Los grupos de módulos, que están previstos para ejecutar una acción orientada a la seguridad, representan de este modo islas más o menos autárquicas dentro de toda la red de comunicaciones.

50 Esta arquitectura se corresponde con la forma de pensar de las personas expertas en la técnica de seguridad, en el caso de automatización de instalaciones. Además de esto son posibles de este modo de forma más sencilla modificaciones y ampliaciones de la instalación, sin que las partes de instalación ya verificadas tengan que verificarse posteriormente de nuevo. Además de esto favorecen en un grado máximo la modularización y la separación de la función de seguridad de funciones estándar los requisitos de las normas de seguridad actuales, como las normas citadas anteriormente IEC 61508 e ISO 13849.

55 Otra ventaja para el usuario se obtiene de la posibilidad de configurar los módulos de seguridad descentralizados, dado el caso con independencia de la red y del control. Por medio de esto se obtiene también una independencia

respecto al ofertante del control. Esto significa también que, en el caso de un cambio del control estándar o de la red, por ejemplo a causa de unos requisitos no relevantes para la seguridad, sea posible mantenerse en la técnica de seguridad usada y en los módulos de seguridad verificados.

5 Conforme a la invención, los módulos de seguridad descentralizados para asegurar la función de seguridad conjunta unos con otros deben poder comunicarse entre sí a prueba de errores, al menos en un volumen limitado. Para hacer esto posible con independencia del medio físico planteado, se transfiere al abonado receptor la comprobación de la transmisión conforme con los requisitos de seguridad. De este modo puede prescindirse de un maestro de seguridad, previsto en algunos sistemas conocidos.

10 Para la comunicación de los módulos de una isla, respectivamente de un grupo de módulos para ejecutar una acción orientada a la seguridad, se envían los telegramas a un maestro de comunicación y allí se enrutan hacia el receptor. El enrutamiento automático del flujo de datos se materializa por medio de que los protocolos de comunicación a prueba de errores y/o los abonados de comunicación a prueba de errores ponen a disposición informaciones o medios, que pueden valorarse mediante las capas de enrutamiento. Valorar quiere decir aquí que la tabla de copiado o enrutamiento puede estructurarse automáticamente en una fase de inicialización, sin que el usuario tenga que predefinir las direcciones del abonado de comunicación mediante una configuración de red. Los medios o informaciones pueden ponerse a disposición y valorarse con ello, tanto una vez durante una fase de inicialización como para la duración del sistema.

La invención contempla en especial, para solucionar la tarea antes citada, una instalación de automatización con un maestro de comunicación en especial no seguro y varios módulos descentralizados, en donde

- 20 - los módulos descentralizados están configurados como abonados de red y
- están encadenados al maestro de comunicación mediante una red de comunicaciones, en donde
- la comunicación entre los módulos descentralizados en la red de comunicaciones se materializa a través de telegramas, en donde
- 25 - al menos dos de los módulos son módulos de seguridad, entre los cuales se transmiten datos orientados a la seguridad y
- forman un grupo lógico de módulos para ejecutar una función orientada a la seguridad, y en donde
- el maestro de comunicación de forma preferida no seguro mantiene una tabla de comunicación, en la que están archivadas conexiones lógicas entre los módulos de seguridad descentralizados de forma correspondiente a la función orientada a la seguridad, en donde
- 30 - el maestro de comunicación está diseñado para, controlado con base en la tabla de enrutamiento, llevar a cabo un enrutamiento automático de los datos entre el módulo de seguridad emisor y el módulo de seguridad receptor,
- de tal modo que se produce una comunicación entre los módulos de seguridad pertenecientes a un grupo lógico en cada caso a través de dos conexiones punto a punto, precisamente entre el módulo de seguridad emisor y el maestro de comunicación y, además, entre el maestro de comunicación y el módulo de seguridad receptor,
- 35 - en donde el módulo de seguridad receptor está diseñado para ejecutar una acción orientada a la seguridad de forma correspondiente a los datos recibidos, y en donde la red de comunicación presenta una instalación para consultar a los módulos de seguridad informaciones para la creación de una tabla de enrutamiento y, con base en esta información, crear la tabla de enrutamiento.

40 La instalación para la creación de la tabla de enrutamiento está implementada de forma preferida en el propio maestro de comunicación. Sin embargo, también es concebible que la tabla de enrutamiento sea creada por una instalación exterior, por ejemplo un módulo adicional conectado a la red, y después se transmita al maestro de comunicación.

Con estas particularidades de una instalación de automatización se hace posible después de forma correspondiente un procedimiento para vigilar funciones de seguridad en la instalación, con un maestro de comunicación en especial no seguro y varios módulos descentralizados, en donde

- 45 - los módulos descentralizados están configurados como abonados de red y
- están encadenados al maestro de comunicación mediante una red de comunicaciones, en donde
- la comunicación entre los módulos descentralizados en la red de comunicaciones se materializa a través de telegramas, en donde
- al menos dos de los módulos son módulos de seguridad, entre los cuales se transmiten datos orientados a la seguridad y
- 50

- forman un grupo lógico de módulos para ejecutar una función orientada a la seguridad, y en donde
 - el maestro de comunicación de forma preferida no seguro mantiene una tabla de comunicación, en la que están archivadas conexiones lógicas entre los módulos de seguridad descentralizados de forma correspondiente a la función orientada a la seguridad, en donde
- 5 - el maestro de comunicación lleva a cabo, con base en la tabla de enrutado, un enrutado automático de los datos entre el módulo de seguridad emisor y el módulo de seguridad receptor,
- de tal modo que se lleva a cabo una comunicación entre los módulos de seguridad pertenecientes a un grupo lógico en cada caso a través de dos conexiones punto a punto, precisamente entre el módulo de seguridad emisor y el maestro de comunicación y, además, entre el maestro de comunicación y el módulo de seguridad receptor,
- 10 - en donde el módulo de seguridad receptor ejecuta una acción orientada a la seguridad de forma correspondiente a los datos recibidos, y en donde una instalación de la red de comunicaciones, de forma preferida el maestro de comunicación, consulta a los módulos de seguridad informaciones para la creación de una tabla de enrutado y se crea, con base en esta información, la tabla de enrutado.

15 El término de tabla de enrutado no se refiere a una asociación estricta en forma tabular. Más bien debe entenderse en el sentido de la invención, bajo este término, una norma de asociación disponible en cualquier forma, en la que los módulos de seguridad, respectivamente sus direcciones, se enlazan de forma correspondiente a las conexiones lógicas a estructurar.

20 Una tabla de enrutado puede presentarse conforme a una forma de ejecución de la invención en forma de una lista de copiado. El copiado puede realizarse en especial en forma de un copiado de telegramas enteros o de sus datos dentro del programa de usuario o de un firmware de comunicación del maestro de comunicación.

La particularidad de un maestro de comunicación no seguro significa que el maestro de comunicación no necesita estar configurado en sí mismo para una comunicación a prueba de errores, y/o tiene que presentar un hardware redundante especial.

25 Una gran ventaja de la invención consiste entre otras cosas en que puede prescindirse por completo de una herramienta de configuración central, con la que se configuran los módulos de seguridad y sus acciones orientadas a la seguridad.

30 En el caso de una comunicación orientada a la seguridad se exige una transmisión rápida de los datos. Aquí parece ser en principio engorroso el procedimiento conforme a la invención con un enrutado a través de un maestro de comunicación no seguro, ya que cada telegrama tiene que transportarse a través de dos conexiones punto a punto y con ello también tiene que enrutarse todavía. Sin embargo, ha quedado demostrado que la velocidad de comunicación es comparable con la de otros sistemas con una comunicación a través del bus, de tal modo que se cumple el requisito de un corto tiempo de reacción.

35 Como base para el tráfico de datos en la red de comunicaciones puede utilizarse comunicación de red estándar. Aquí pueden citarse entre otros los sistemas INTERBUS, PROFIBUS, PROFINET, DeviceNet y Ethernet IP. Para una comunicación segura entre los módulos de seguridad pueden utilizarse los correspondientes protocolos de red seguros INTERBUS-Safety, PROFIsafe o CIP-Safety. Estos protocolos de red a prueba de errores funcionan según el principio de "Black-Channel", en el que el telegrama a prueba de errores se incrusta en un telegrama estándar. Un abonado de comunicación asume con ello el papel del maestro de comunicación seguro, por ejemplo mediante una capa maestro-esclavo, o en forma de un F-Host.

40 A continuación se explica la invención con más detalle, en base a los dibujos adjuntos. Con ello los símbolos de referencia iguales hacen referencia a elementos iguales o correspondientes. Aquí muestran:

la figura 1: un esquema de conexiones esquemático de una red de automatización de una instalación de fabricación automatizada,

la figura 2: un ejemplo de ejecución de una tabla de enrutado para la red de automatización mostrada en la figura 1,

45 la figura 3 un ejemplo de ejecución con módulos de introducción y edición de datos.

En la figura 1 se ha representado un esquema de conexiones en bloques de la red de comunicaciones de una instalación de automatización 1, de forma preferida de una instalación de fabricación automatizada.

50 Una instalación de automatización 1 conforme a la invención comprende un maestro de comunicación, por ejemplo formando parte de un control central y varios módulos descentralizados. En el ejemplo de la figura 1 está previsto un maestro de comunicación 3 como control central o formando parte del mismo. A la red de comunicaciones 2 están conectados módulos descentralizados 70, 80, 81, 82, 83, 90, 91.

Los módulos descentralizados 70, 80, 81, 82, 83, 90 91 están configurados como abonados de red y acoplados al maestro de comunicación 3 mediante la red de comunicaciones 2. La comunicación entre los módulos descentralizados 70, 80, 81, 82, 83, 90, 91 en la red de comunicaciones 2 se materializa a través de telegramas. La red de comunicaciones 2 puede presentar por ejemplo una red Ethernet como capa física y la comunicación puede materializarse, de forma correspondiente, con telegramas Ethernet.

Asimismo al menos dos de los módulos son módulos de seguridad, entre los cuales se transmiten datos orientados a la seguridad. En el ejemplo de la figura 1 en especial los módulos 80, 81, 82, 83,90, 91 están configurados como módulos de seguridad. Los módulos de seguridad forman uno o varios grupos lógicos de módulos, para ejecutar una función orientada a la seguridad.

El maestro de comunicación 3 mantiene una tabla de enrutado, en la que están archivadas conexiones lógicas entre los módulos de seguridad descentralizados 80, 81, 82, 83, 90, 91 de forma correspondiente a la función orientada a la seguridad. El maestro de comunicación 3 está diseñado para, controlado con base en la tabla de enrutado, llevar a cabo un enrutado automático de los datos desde el respectivo módulo de seguridad emisor hasta el módulo de seguridad receptor. El módulo de seguridad receptor está diseñado para ejecutar una acción orientada a la seguridad de forma correspondiente a los datos receptores.

El maestro de comunicación 3 no tiene que ser seguro, en especial por sí mismo, en el sentido de las normas antes citadas. Más bien el control central puede representar un control estándar.

En el ejemplo citado en la figura 1 existen conexiones punto a punto10, 11, 12, 13, 14, 15 entre el maestro de comunicación 3 y los módulos de seguridad 80, 81, 82, 83, 90, 91. En la tabla de enrutado están archivadas asimismo las conexiones lógicas 16, 17,18, 19 utilizadas para llevar a cabo las diferentes funciones orientadas a la seguridad. Mediante esta tabla de enrutado el maestro de comunicación 3 enruta los datos, que se envían desde los módulos de seguridad en cada caso emisores, automáticamente hacia los módulos de seguridad receptores asociados. Los módulos de seguridad enlazados con una conexión lógica forman en cada caso un grupo lógico de módulos para ejecutar una función orientada a la seguridad. En el ejemplo mostrado en la figura 1 se forma conforme a esto un grupo lógico con los módulos de seguridad 80, 81, 82, 83, en el que mediante las conexiones lógicas 16, 17, 18 los módulos de seguridad 81, 82, 83 están enlazados en cada caso con el módulo de seguridad 80. Asimismo se enlaza un grupo lógico de los módulos de seguridad 90, 91 a través de la conexión lógica 19.

Por ejemplo uno de los módulos de seguridad puede valorar los datos de una barrera óptica. Después puede estar previsto, por ejemplo, que se desconecte un dispositivo cuyo acceso se vigila con la barrera óptica. Después se acciona una instalación de desconexión correspondiente desde otro módulo de seguridad, mediante la reacción ante un telegrama enviado por el módulo de seguridad, al que está conectada la barrera óptica, y enrutado desde el maestro de comunicación 3 hacia el otro módulo de seguridad.

Las conexiones lógicas se dividen de este modo en cada caso en dos conexiones punto a punto desde y hacia el maestro de comunicación 3. Por ejemplo se materializa la conexión lógica 16 del ejemplo de ejecución mostrado en la figura 1 mediante las conexiones punto a punto 10 y 11. Para la comunicación planteada puede utilizarse de este modo cualquier protocolo punto a punto. Una base preferida es una red Ethernet.

La transmisión de los datos orientados a la seguridad en telegramas puede realizarse en especial a través de un canal no seguro, a través de la red de telecomunicaciones. En otras palabras, se utiliza el mismo medio de comunicación que para los datos estándar para controlar el proceso. Esto es especialmente ventajoso para reducir la complejidad de hardware y simplificar en instalaciones de automatización existentes. Para conseguir aquí una fiabilidad elevada en la transmisión de los datos orientados a la seguridad, se utiliza un principio de "Black-Channel". De este modo se transfiere el reconocimiento de errores de telegrama por completo al módulo de seguridad receptor. Conforme a esto, en este perfeccionamiento de la invención para la transmisión a prueba de errores de los datos orientados a la seguridad, el módulo de seguridad receptor está configurado para reconocer errores con respecto a una permutación, falsificación, un error de encaminamiento o una destrucción de telegramas.

Para esto el módulo de seguridad receptor puede comprobar, en el caso de un telegrama recibido, al menos una de las siguientes particularidades, de forma preferida todas las particularidades siguientes:

- el cronofechador,
- redundancia,
- una suma de comprobación,
- un número de telegrama correlativo,
- una identificación de emisor,
- una identificación de receptor.

Con base en la identificación de emisor y receptor de los telegramas puede determinarse, en especial mediante el módulo de seguridad receptor, si la asociación de fuente y destino del telegrama es correcta y clara.

5 El principio del "Black Channel" se basa en cualquier tipo de error, como permutación, destrucción y falsificación de telegramas en la red de comunicaciones 2. Las medidas de reconocimiento de errores del protocolo de comunicación a prueba de errores, utilizado para la comunicación entre los módulos de seguridad, no tienen en cuenta con ello en especial las medidas de reconocimiento de errores dado el caso también existentes en el tráfico estándar.

En la figura 2 se ha representado una tabla de enrutado 20 a modo de ejemplo para las conexiones lógicas mostradas en la figura 1.

10 En la primera columna están archivadas las conexiones lógicas. La segunda columna ubica la dirección maestra y la tercera columna la dirección esclava. Como direcciones maestra y esclava se designan aquí las respectivas direcciones del respectivo módulo de edición e introducción de datos. De forma preferida se utiliza un módulo de edición como maestro, pero también es posible una configuración inversa. La división en módulos de seguridad maestros y esclavos se refiere con ello en especial a la comunicación a prueba de fallos. De este modo el maestro puede estar por ejemplo diseñado para comprobar los números correlativos de los telegramas y, con base en ellos, determinar si los módulos esclavos y la comunicación de estos módulos funciona apropiadamente con el módulo de seguridad maestro.

20 Debido a que en el ejemplo mostrado en la figura 1 existen varias conexiones lógicas con el módulo de seguridad 80, se asocian a este módulo de seguridad también varias direcciones en forma de puertos. En especial están asociadas la dirección 80:0 con el puerto 0 para la conexión lógica 16 al módulo de seguridad 82, la dirección 80:1 con el puerto 1 para la conexión lógica 17 al módulo de seguridad 83, y la dirección 80:2 con el puerto 2 para la conexión lógica 18 al módulo de seguridad 83.

25 Para reducir la complejidad a la hora de inicializar o planificar las funciones de seguridad, es asimismo conveniente que el control central esté diseñado para consultar a los módulos de seguridad informaciones para la creación de una tabla de enrutado y crear la tabla de enrutado con base en esta información. De forma correspondiente también están con ello diseñados los módulos de seguridad para poner a disposición la información necesaria.

30 La comunicación orientada a la seguridad se realiza conforme a la invención, por lo tanto, en cada caso a través del maestro de comunicación, en donde los módulos de seguridad emisores, en el ejemplo de la figura 1 por lo tanto los módulos de seguridad 80 y 90, envían siempre al maestro de comunicación 3, respectivamente al control central, y desde éste se envían telegramas con la información obtenida después al módulo de seguridad con la dirección de destino definida en la tabla de enrutado. Esto ofrece la ventaja de que ni los módulos de seguridad emisores ni los receptores necesitan informaciones, cuyo otro módulo de seguridad está asociado a éste para llevar a cabo una función orientada a la seguridad dentro de un grupo lógico.

35 Una forma de ejecución de la inicialización del control central no seguro, con relación a la creación de la tabla de enrutado, es como sigue:

- En primer lugar se establece la configuración de red conectada.
- Después se realiza un establecimiento de las direcciones, respectivamente, más en general de información de identificación del módulo de seguridad conectado.
- Dado el caso se lleva a cabo una comprobación de plausibilidad.
- 40 - Con base en la información procedente de los dos primeros pasos se lleva a cabo una lista de instrucciones o copiado para el enrutado de telegramas en el funcionamiento cíclico.

Como información de identificación del módulo de seguridad, para la creación automática de la tabla de enrutado o lista de copiado, puede utilizarse en especial:

- un código de identificación,
- 45 - una ID de aparato,
- un nombre de aparato,
- una dirección de seguridad, que puede ser ajustable también mediante interruptores por ejemplo en el módulo de seguridad.

50 En general la inicialización puede desarrollarse de este modo, mediante un algoritmo implementado en el maestro de comunicación, de la forma siguiente: primero el algoritmo reconoce en la red los módulos de seguridad, por ejemplo por su código ID, y lee después en estos módulos las direcciones de seguridad. A continuación puede reconocerse, con base en las direcciones de seguridad, que debe realizarse un enrutado automático dentro de las

islas o de los grupos lógicos, es decir, en el ejemplo según la figura 1 entre los módulos 80 – 83 por un lado y los módulos 90, 91 por otro lado. Se establecen referencias o solicitudes de copiado de forma correspondiente a las conexiones lógicas 16 a 18, dentro de la primera isla, y una referencia o solicitud de copiado conforme a la conexión lógica 19 de la segunda isla.

5 Una asociación de los módulos de seguridad puede realizarse también, conforme a otra forma de ejecución de la invención, a través del ajuste de una información de dirección del maestro de comunicación a los módulos de seguridad. Esto es favorable cuando existen varios maestros de comunicación 3 en la red de comunicaciones y se pretende asociar a cada maestro de comunicación 3 una isla, respectivamente un grupo lógico de módulos de seguridad.

10 Transferido al ejemplo mostrado en la figura 3, en este caso el maestro de comunicación 3 tiene por ejemplo el número 8 o una dirección correspondiente. Éste se ajusta en los interruptores selectores de dirección 21 de los módulos de seguridad 80, 81. El maestro de comunicación 3 consulta después en la fase de inicialización los números ajustados a los módulos de seguridad, respectivamente las direcciones correspondientes y reconoce, de este modo, que los módulos 80, 81 le están asociados y deben formar un grupo lógico para ejecutar una función de seguridad.

15 La lista de instrucciones o copiado representa con ello una posible forma de tabla de enrutado. La transmisión de la información al módulo de seguridad receptor puede realizarse, conforme a una forma de ejecución de la invención, mediante copiado de los telegramas completos en el programa de usuario o dentro del firmware de comunicación del maestro de comunicación 3. Para esto pueden estructurarse listas de copiado (tablas, etc.), que después se elaboran en el funcionamiento cíclico.

A través del módulo de seguridad recibido en cada caso, mediante el protocolo de red a prueba de errores, puede establecerse también si la tabla de enrutado mantenida en el maestro de comunicación es correcta y con ello, también, si las informaciones se enrutan hacia los abonados correctos.

20 Las listas de copiado contienen para las solicitudes de copiado siempre una dirección fuente (indicador fuente), una dirección de destino (indicador de destino) y la longitud de los datos a copiar.

25 Para la creación automática de la tabla de enrutado, como se ha representado a modo de ejemplo en la figura 2, es importante que no se introduzca ninguna conexión innecesaria o incluso incorrecta, respectivamente que sólo se introduzcan conexiones correctas. Conexiones incorrectas serían por ejemplo aquellas entre módulos de seguridad de diferentes grupos lógicos. Esto podría conducir a que se desconecte una señal de un interruptor de desconexión de emergencia para una máquina de otra máquina.

30 Para encontrar la asociación correcta de las conexiones pertenecientes a un grupo lógico de módulos de seguridad, a la hora de estructurar la tabla de enrutado, el maestro de comunicación 3 está diseñado, en un perfeccionamiento de la invención, para consultar informaciones a los módulos de seguridad conectados a la red de comunicaciones y, con base en la información consultada, determinar cuáles de los módulos de seguridad pertenecen a un grupo lógico y llevar a cabo en la tabla de enrutado las conexiones de forma correspondiente a la asociación de los módulos de seguridad.

35 Para esto existen varias posibilidades. Una posibilidad sencilla consiste en valorar la información de dirección de los módulos de seguridad. Para ello las direcciones de los módulos de seguridad pueden configurarse de tal modo que éstas reflejen ya, respectivamente representen, en cada caso la pertenencia a un grupo lógico. Una posibilidad para esto consiste en que el maestro de comunicación asocie grupos lógicos en cada caso a determinados espacios de dirección. Otra posibilidad consiste en que los módulos de seguridad estén diseñados para, a través de la red de comunicaciones y bajo solicitud, proporcionar una información que marque la pertenencia a un determinado grupo lógico. Esta información puede tomarse también como componente de la dirección.

40 En el ejemplo representado en la figura 1 los módulos de seguridad pueden presentar por ejemplo direcciones correspondientes a los símbolos de referencia asociados. De este modo, el maestro de comunicación puede estar diseñado para reproducir en la tabla de enrutado, mediante registros de conexiones correspondientes, grupos lógicos correspondientes a los espacios de dirección 50-59, 60-69, 70-79, 80-89, 90-99, etc.

45 Como puede verse con base en la figura 1, los módulos de uno de los grupos lógicos presentan por ejemplo todos una dirección en el espacio de dirección 80 a 89, y los módulos de seguridad de los otros grupos lógicos direcciones en el espacio de dirección 90 – 99. De forma correspondiente se registran después conexiones entre los módulos 80, 81, 82, 83, por un lado, y una conexión entre los módulos 90 y 91, por otro lado.

50 Para materializar muchas funciones de seguridad, como por ejemplo la emisión de una señal de desconexión ante la respuesta a una señal de entrada, es conveniente que de los módulos de seguridad de un grupo al menos un módulo de seguridad comprenda un módulo de introducción de datos y al menos un módulo de seguridad un módulo de edición. El módulo de introducción de datos envía después, a través de una conexión lógica a las dos conexiones punto a punto, con la participación del maestro de comunicación, un telegrama al módulo de edición que después, ante la respuesta al telegrama, activa una acción orientada a la seguridad.

Para a continuación, por ejemplo a la hora de instalar la instalación de automatización, marcar los módulos de seguridad pertenecientes a un grupo lógico, los módulos de seguridad pueden estar dotados de un interruptor selector de dirección. Son por ejemplo adecuados interruptores Dip aplicados a la carcasa.

5 La dirección así ajustada o determinada de otro modo para la comunicación segura no tiene que ser idéntica a la dirección de red general. Más bien puede tratarse aquí de una dirección de seguridad especial. Como se explica a modo de ejemplo más adelante con base en la figura 3, la adjudicación de la dirección de seguridad o también de otra información de dirección individual puede realizarse de tal modo que un algoritmo, implementado en el maestro de comunicación, reconozca la pertenencia de módulos de seguridad a un grupo lógico y estructure la tabla de enrutado de forma correspondiente mediante el registro de una conexión de estos módulos de seguridad. Para esto, 10 la figura 3 muestra un ejemplo de ejecución con módulos de seguridad en forma de módulos de introducción y edición de datos.

Del grupo lógico de los módulos de seguridad 80, 81, 82 y 83 del ejemplo mostrado en la figura 1 sólo se han representado, para mayor sencillez, los módulos de seguridad 80 y 81. El módulo de seguridad 80 es un módulo de edición y recibe informaciones del módulo de seguridad 81 emisor, que está configurado como módulo de 15 introducción de datos.

Ambos módulos de seguridad 80, 81 presentan una conexión 23 para conectarse a sensores, respectivamente actuadores. El módulo de seguridad 81 como módulo de introducción de datos está conectado con ello a un sensor 27 y el módulo de seguridad 80 como módulo de edición a un actuador 29, en cada caso a través de un cable 26. En el ejemplo mostrado en la figura 3, el sensor 27 es el sensor de una barrera óptica 30. El actuador 29 es en este 20 ejemplo un relé de seguridad, el cual desconecta una máquina 31 controlada por la red de automatización, por ejemplo de un torno.

La acción orientada a la seguridad es en este ejemplo, conforme a esto, la desconexión automática de la máquina 31 en el caso de que se interrumpa la barrera óptica 30. De este modo se quiere asegurar que ninguna persona pueda acercarse a la máquina 31 en marcha y ponerse en riesgo.

25 Si se produce una interrupción de la barrera óptica 30, accionado mediante la señal del sensor 27 desde el módulo de seguridad 81, se envía después un telegrama al maestro de comunicación 3. Éste determina, con base en su tabla de enrutado, que el telegrama se transmita al módulo de seguridad 80 y enruta el telegrama de forma correspondiente. El módulo de seguridad receptor 80 activa ante la respuesta a la información contenida en el telegrama, a través del accionamiento de la barrera óptica y a través de la conexión 23, el actuador 29, respectivamente aquí en especial un actuador 29 en forma de un relé que, ante la respuesta a una señal, se conecta 30 a la conexión 23 y con ello transfiere la máquina 31 a un estado seguro.

A continuación se quiere evitar una configuración complicada de la acción orientada a la seguridad durante la instalación de la instalación. En especial se quiere hacer posible, de forma sencilla, acoplar con sus funciones los diferentes módulos de seguridad pertenecientes a un grupo lógico. En la técnica de seguridad tradicional esto se 35 produce mediante el cableado de los diferentes módulos.

Para llevar a cabo la configuración para una instalación de automatización conforme a la invención, los módulos de seguridad pueden presentar en cada caso un interruptor de dirección 21. La pertenencia de los módulos de seguridad a un grupo lógico puede realizarse después, de forma sencilla, mediante una adjudicación de dirección según un esquema predeterminado. En el ejemplo conforme a la figura 3 con los interruptores de dirección 21 40 pueden seleccionarse en cada caso espacios de dirección, en donde la asociación a un grupo lógico se consigue mediante la selección del mismo espacio de dirección. Con los interruptores selectores de dirección 21 pueden seleccionarse en el ejemplo mostrado los espacios de dirección 40-49 (posición de interruptor 4), 50-59 (posición de interruptor 5), 60-69, 70-79, 80-89 y 90-99. Para acoplar ambos módulos de seguridad 80 y 81 lógicamente a un grupo, en el ejemplo representado se han seleccionado los dos módulos de seguridad del espacio de dirección 80 – 45 89, mediante el ajuste del interruptor selector de dirección 21 al número “8”.

En una fase de inicialización se consultan las direcciones de los módulos de seguridad conectados a la red de comunicaciones. Estos reenvían después la información de dirección. Con base en la asociación reconocida de los módulos de seguridad a un grupo lógico, el maestro de comunicación puede estructurar después la tabla de enrutado con los enlaces correspondientes.

50 La información de dirección no es necesario que sea completa. Los dos módulos de seguridad 80, 81 pueden comunicar por ejemplo al maestro de comunicación el espacio de dirección 80 – 89 asignado a los mismos. Éste puede asignar después, en un segundo paso, una dirección completa a los módulos de seguridad 80, 81. De forma preferida se consultan evidentemente direcciones de seguridad completas, en donde la dirección ajustada para cada interruptor selector de dirección 21 se adjudica adicionalmente a la dirección de seguridad completa o forma parte de 55 la dirección completa.

De forma similar a la adjudicación de dirección descrita, puede realizarse también por ejemplo el ajuste del puerto utilizado por el módulo de seguridad receptor 80. Para esto pueden preverse interruptores selectores correspondientes, con los que se ajustan entre sí los puertos para la comunicación de los módulos de seguridad.

Siempre que la asociación de un puerto determinado a un módulo de introducción de datos determinado no sea necesaria para el reconocimiento y la ejecución de la acción orientada a la seguridad, la adjudicación de las direcciones de puerto puede realizarse también en la fase de inicialización.

REIVINDICACIONES

1. Instalación de automatización con un maestro de comunicación (3) en especial no seguro y varios módulos descentralizados (70, 80 – 83, 90, 91), en donde
- los módulos descentralizados (70, 80 – 83, 90, 91) están configurados como abonados de red y
- 5
- están encadenados al maestro de comunicación (3) mediante una red de comunicaciones, en donde
 - la comunicación entre los módulos descentralizados en la red de comunicaciones se materializa a través de telegramas, en donde
 - al menos dos de los módulos son módulos de seguridad, entre los cuales se transmiten datos orientados a la seguridad y
- 10
- forman un grupo lógico de módulos para ejecutar una función orientada a la seguridad, caracterizada porque
 - el maestro de comunicación (3) de forma preferida no seguro mantiene una tabla de comunicación, en la que están archivadas conexiones lógicas entre los módulos de seguridad descentralizados de forma correspondiente a la función orientada a la seguridad, en donde
- 15
- el maestro de comunicación está diseñado para, controlado con base en la tabla de enrutado, llevar a cabo un enrutado automático de los datos entre el módulo de seguridad emisor y el módulo de seguridad receptor,
 - de tal modo que se produce una comunicación entre los módulos de seguridad pertenecientes a un grupo lógico en cada caso a través de dos conexiones punto a punto, precisamente entre el módulo de seguridad emisor y el maestro de comunicación (3) y, además, entre el maestro de comunicación (3) y el módulo de seguridad receptor,
- 20
- en donde el módulo de seguridad receptor está diseñado para ejecutar una acción orientada a la seguridad de forma correspondiente a los datos recibidos, y
 - en donde la red de comunicación presenta una instalación para consultar a los módulos de seguridad informaciones para la creación de una tabla de enrutado y, con base en esta información, crear la tabla de enrutado.
- 25
2. Instalación de automatización conforme a la reivindicación anterior, en donde el maestro de comunicación está diseñado para, con objeto de inicializar la tabla de enrutado, llevar a cabo los pasos siguientes:
- establecimiento de la configuración de red conectada,
 - establecimiento de información de identificación de los módulos de seguridad conectados,
 - dado el caso, ejecución de una comprobación de plausibilidad,
 - con base en la información procedente de los pasos a) y b), creación de una lista de instrucciones o copiado para
- 30
- el enrutado de telegramas en el funcionamiento cíclico.
- 35
3. Instalación de automatización conforme a una de las reivindicaciones anteriores, en la que el maestro de comunicación (3) está diseñado para consultar informaciones a los módulos de seguridad conectados a la red de comunicaciones y, con base en la información consultada, determinar cuáles de los módulos de seguridad pertenecen a un grupo lógico y llevar a cabo en la tabla de enrutado las conexiones de forma correspondiente a la asociación de los módulos de seguridad.
- 40
4. Instalación de automatización conforme a una de las reivindicaciones anteriores, caracterizada porque las direcciones de los módulos de seguridad están configuradas de tal modo, que éstas reflejan en cada caso la pertenencia a un grupo lógico.
- 45
5. Instalación de automatización conforme a una de las reivindicaciones anteriores, en donde la transmisión de los datos orientados a la seguridad se realiza en telegramas, a través de un canal no seguro y, para la transmisión a prueba de errores de los datos orientados a la seguridad, el módulo de seguridad receptor está configurado para reconocer errores con respecto a una permutación, falsificación, un error de encaminamiento o una destrucción de telegramas.
6. Instalación de automatización conforme a la reivindicación anterior, caracterizada porque el módulo de seguridad receptor comprueba, en el caso de un telegrama recibido, al menos una de las siguientes particularidades, de forma preferida todas las particularidades siguientes:
- el cronofechador,

- redundancia,
 - una suma de comprobación,
 - un número de telegrama correlativo,
 - una identificación de emisor,
 - 5 - una identificación de receptor.
7. Instalación de automatización conforme a la reivindicación anterior, caracterizada porque el maestro de comunicación (3) está diseñado para asociar grupos lógicos en cada caso a determinados espacios de dirección.
8. Instalación de automatización conforme a una de las reivindicaciones anteriores, en donde de los módulos de seguridad de un grupo lógico al menos un módulo de seguridad comprende un módulo de introducción de datos y al menos un módulo de seguridad un módulo de edición, en donde el módulo de edición está diseñado para, ante la respuesta a un telegrama de un módulo de introducción de datos, activar una función de seguridad.
- 10
9. Procedimiento para vigilar funciones de seguridad en una instalación de automatización, con un maestro de comunicación (3) en especial no seguro y varios módulos descentralizados, en donde
- los módulos descentralizados están configurados como abonados de red y
- 15
- están encadenados al maestro de comunicación mediante una red de comunicaciones, en donde
 - la comunicación entre los módulos descentralizados en la red de comunicaciones se materializa a través de telegramas, en donde
 - al menos dos de los módulos son módulos de seguridad, entre los cuales se transmiten datos orientados a la seguridad y
- 20
- forman un grupo lógico de módulos para ejecutar una función orientada a la seguridad, caracterizado porque
 - el maestro de comunicación (3) de forma preferida no seguro mantiene una tabla de comunicación, en la que están archivadas conexiones lógicas entre los módulos de seguridad descentralizados de forma correspondiente a la función orientada a la seguridad, en donde
- 25
- el maestro de comunicación lleva a cabo, con base en la tabla de enrutado, un enrutado automático de los datos entre el módulo de seguridad emisor y el módulo de seguridad receptor,
 - de tal modo que se lleva a cabo una comunicación entre los módulos de seguridad pertenecientes a un grupo lógico en cada caso a través de dos conexiones punto a punto, precisamente entre el módulo de seguridad emisor y el maestro de comunicación (3) y, además, entre el maestro de comunicación (3) y el módulo de seguridad receptor,
- 30
- en donde el módulo de seguridad receptor ejecuta una acción orientada a la seguridad de forma correspondiente a los datos recibidos, y en donde
 - una instalación de la red de comunicaciones, de forma preferida el maestro de comunicación, consulta a los módulos de seguridad informaciones para la creación de una tabla de enrutado y se crea, con base en esta información, la tabla de enrutado.

Fig. 1

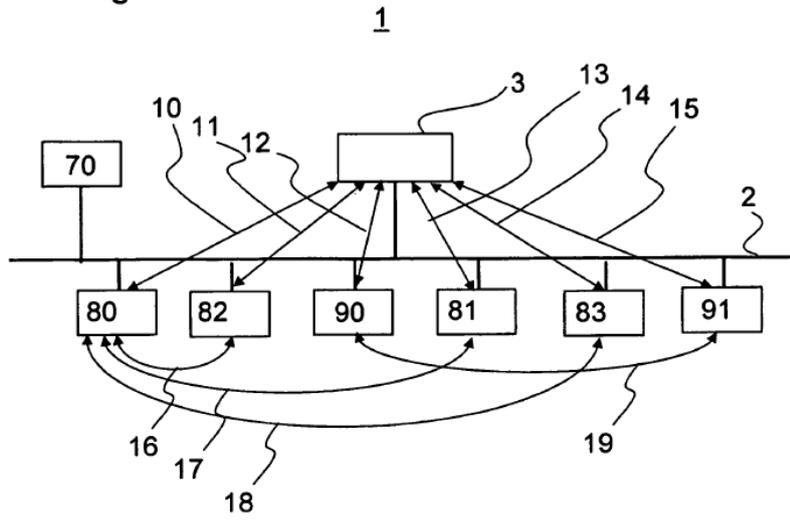


Fig. 2

Conexión	Dirección Maestra	Dirección esclava
16	80:0	81
17	80:1	82
18	80:2	83
Conexión	90:0	91

Fig. 3

