



(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 335 788**

(51) Int. Cl.:
G05B 19/042 (2006.01)
H04L 1/00 (2006.01)

(12)

TRADUCCIÓN DE PATENTE EUROPEA

T3

(96) Número de solicitud europea: **05785677 .5**
(96) Fecha de presentación : **16.09.2005**
(97) Número de publicación de la solicitud: **1789857**
(97) Fecha de publicación de la solicitud: **30.05.2007**

(54) Título: **Procedimiento para la transmisión de datos y sistema de automatización para el empleo de un procedimiento de transmisión de datos de este tipo.**

(30) Prioridad: **16.09.2004 DE 10 2004 044 764**
01.03.2005 DE 10 2005 009 224

(45) Fecha de publicación de la mención BOPI:
05.04.2010

(45) Fecha de la publicación del folleto de la patente:
05.04.2010

(73) Titular/es: **Beckhoff Automation GmbH**
Eiserstrasse 5
33415 Verl, DE

(72) Inventor/es: **Buttner, Holger y**
Sachs, Jens

(74) Agente: **Carpintero López, Mario**

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 para la transmisión de datos y sistema de automatización para el empleo de un procedimiento de transmisión de datos de este tipo.

La invención se refiere a un procedimiento para la transmisión de paquetes de datos en un tramo de transmisión de datos entre dos participantes en la comunicación, y a un sistema de automatización con dos participantes en la comunicación conectados a través de un tramo de transmisión de datos que presentan una unidad de conexión en cada caso.

En los sistemas de automatización para el control de máquinas, debe quedar garantizado que incluso cuando falle el sistema de automatización no existe ningún riesgo para las personas y el medio ambiente. Por tanto, los sistemas de automatización normalmente trabajan según el denominado “principio Fail-Safe”, según el cual, en caso de fallo de componentes importantes, el sistema de automatización pasa a un estado seguro. En este sentido, requisitos fundamentales que debe cumplir el sistema de automatización durante la implementación de funciones de control pertinentes para la seguridad según el principio Fail-Safe son el que los datos de proceso de los sensores de las máquinas durante la implementación de las funciones de control de seguridad se procesen de forma actualizada y sin falsearlos y el que siempre se muestre a los actores de las máquinas un estado de proceso seguro.

Sin embargo, en los sistemas de automatización, el número de funciones de control pertinentes para la seguridad normalmente es fundamentalmente menor que el número de funciones de control no pertinentes para la seguridad que sirven para mantener el funcionamiento normal en el sistema de automatización. Para garantizar que la funcionalidad de las funciones de control pertinentes para la seguridad no se ve afectada por funciones de control no pertinentes para la seguridad en el sistema de automatización, las funciones pertinentes para la seguridad se agrupan tradicionalmente en un programa de seguridad independiente, aislado frente a las funciones de control no pertinentes para la seguridad.

Una completa separación de funciones de control pertinentes y no pertinentes para la seguridad se consigue si el programa de seguridad se implementa en un ordenador de automatización independiente, que a menudo también está conectado con un cableado propio con los interruptores de desconexión de emergencia, barreras de luz y otros componentes que garantizan la seguridad de las máquinas. Para reducir este gasto de hardware adicional por un ordenador de automatización adicional en el sistema de automatización, se conocen ya sistemas de automatización en los que un programa de seguridad y un programa de control no pertinente para la seguridad se implementan en los mismos componentes de hardware mediante la ampliación del programa de control no pertinente para la seguridad con una denominada “capa de seguridad”.

Los modernos sistemas de automatización normalmente están diseñados de forma descentralizada, comunicándose la periferia de procesos, es decir, el nivel de sensores o actores, con los ordenadores de control a través de redes locales, preferiblemente un sistema de bus de campo. Para el control de las máquinas, los ordenadores de control leen las señales de entrada de los programas de control a través del bus de campo de la periferia de procesos y, tras el procesamiento en tiempo real por el ordenador de control, se emiten las señales de salida, a través del bus de campo, a la periferia de procesos. Para poder transmitir al mismo tiempo a través del bus de campo del sistema de automatización también señales de procesos de un programa de seguridad, el sistema de bus de campo se amplía con una denominada “capa de seguridad”, que minimiza a un valor mínimo permitido la probabilidad de que, debido a un fallo, se falsee la transmisión de los datos entre la periferia de procesos y los ordenadores de control de forma que esta falsificación ya no se detecte, de modo que el bus de campo también puede utilizarse para la transmisión de datos pertinentes para la seguridad.

Este tipo de capas de seguridad adicionales en los sistemas de bus de campo incluyen normalmente una relación de direcciones adicional entre los dos participantes en la comunicación en el bus de campo para permitir una asignación inequívoca. Además, el paquete de datos pertinente para la seguridad transmitido entre los participantes en la comunicación está dotado de un carácter de comprobación adicional que se calcula a partir de las direcciones o datos de procesos transmitidos para poder detectar de forma fiable una falsificación de los datos. Para poder comprobar la secuencia correcta de los datos de procesos pertinentes para la seguridad que deben transmitirse y su llegada en el momento adecuado a los participantes en la comunicación, normalmente el paquete de datos pertinente para la seguridad está dotado además con un número de secuencia continuo. En este caso, el número de secuencia normalmente se extrae de un bloque de números predeterminado que se reinicializa nuevamente una vez realizado un ciclo completo.

Un sistema de automatización conocido en el que el programa de control y el programa de seguridad pueden implementarse en los mismos componentes de hardware es el sistema Simatic de la empresa Siemens. Como sistema de bus de campo se emplea en este caso el sistema Profibus, que está ampliado con un denominado “protocolo Profisafe” para la transmisión de paquetes de datos pertinentes para la seguridad. Sin embargo, la ampliación del sistema de automatización con el programa de seguridad sólo es posible en el marco de este entorno de procesamiento de datos y configuración fijo.

No obstante, en los sistemas de automatización, además de los conocidos protocolos de bus de campo propietarios, se utiliza cada vez más el protocolo Ethernet para la transmisión de señales de procesos. El protocolo Ethernet representa, en la comunicación entre oficinas, la tecnología más ampliamente difundida, con la que, en las redes de

comunicación locales, se transmiten datos con gran velocidad. Debido a las ventajas del concepto de Ethernet en cuanto al uso de componentes de hardware y software estándar así como a la posibilidad de conseguir con una tecnología de conexión sencilla altas velocidades de transmisión de datos, se emplean cada vez más sistemas de bus de campo Ethernet también en la fabricación industrial para el intercambio de datos entre el nivel de actores y sensores y los ordenadores de control.

Por tanto, sería deseable poder equipar también los sistemas de bus de campo de Ethernet con una capa de seguridad para así, además de programas de control convencionales, poder implementar también programas de seguridad en el bus de campo de Ethernet. Sin embargo, las redes de Ethernet normalmente se estructuran con ayuda de los denominados "switchs" para evitar las colisiones de datos en la red. Los switchs son nodos de comunicación de paquetes de datos con varias entradas y salidas, conmutándose el paquete de datos que llega a una entrada exclusivamente a la salida que conoce la estación receptora. Sin embargo, en la transmisión de paquetes de datos a través de switchs en una red Ethernet se producen retrasos temporales dado que el paquete de datos recibido por el switch en una entrada se almacena temporalmente y sólo entonces se conmuta a la salida deseada.

No obstante, debido a la transmisión retrasada de los paquetes de datos en las redes Ethernet equipadas con switchs, en las capas de seguridad convencionales, tales como el protocolo Profisafe, existe el peligro de que se produzca un estado de procesos erróneo. Dado que los paquetes de datos de seguridad están dotados de un número de secuencia continuo procedente de un bloque de números con una cantidad predeterminada de números, mediante el almacenamiento temporal de los paquetes de datos en el switch puede excederse el número de secuencia, lo que puede conducir entonces a que se transmitan datos de seguridad erróneos. En el protocolo Profisafe, por ejemplo, se transmiten los paquetes de datos de seguridad con un número de secuencia de 8 bits, es decir, un paquete de datos en el que los datos de proceso no varían se repite cada 255 ciclos durante la transmisión de datos en el sistema de automatización dado que entonces se excede el número de secuencia, siendo 0 un número de secuencia no permitido. En consecuencia, puede, por ejemplo, no detectarse en el debido momento una desconexión de emergencia o no desconectarse en el debido momento una protección para las máquinas y, con ello, no puede garantizarse un estado de procesos seguro en el sistema de automatización.

Del documento WO 99/49373 se conoce además un procedimiento para la operación de un sistema de automatización en el que se intercambia información segura frente a fallos de forma cíclica con un protocolo de seguridad. Para sólo tener que transmitir una vez datos que permanecen sin cambios en múltiples transmisiones, los paquetes de datos se dividen en una parte estática y una parte dinámica, transmitiéndose la parte estática del paquete de datos sólo en una fase de inicialización entre los participantes en la comunicación en el sistema de bus de campo. La parte estática del paquete de datos forma en este caso el valor inicial para el cálculo del carácter de comprobación de la parte dinámica del paquete de datos. La no presencia de un nuevo paquete de datos en un intervalo de tiempo de tolerancia predeterminado se valora en este sentido como situación de fallo. Al utilizar una capa de seguridad de este tipo con transmisión cíclica de paquetes de datos en una red Ethernet con switchs, existe además el riesgo de un estado de procesos erróneo debido a la transmisión retrasada de los paquetes de datos por motivo del switch. Asimismo, debe tenerse en cuenta un cumplimiento preciso de las condiciones temporales.

El objetivo de la presente invención es proporcionar un procedimiento para la transmisión de paquetes de datos en un tramo de transmisión de datos entre dos participantes en la comunicación, y un sistema de automatización correspondiente que garantice que las señales de procesos para la implementación de funciones de control pertinentes para la seguridad se procesan de forma actualizada y no falseada y que siempre se muestra a los actores del sistema de automatización un estado de procesos seguro.

Este objetivo se consigue según la invención con un procedimiento según la reivindicación 1 y un sistema de automatización según la reivindicación 15. En las reivindicaciones dependientes se muestran variantes preferidas.

Según la invención, para la transmisión de paquetes de datos en un tramo de transmisión de datos entre dos participantes en la comunicación en un sistema de comunicación se dota a cada uno de los paquetes de datos con un carácter de comprobación que se calcula a partir de los otros datos del paquete de datos, utilizándose como valor inicial para el cálculo del carácter de comprobación para un paquete de datos que ha de enviarse a otro participante en la comunicación el carácter de comprobación del último paquete de datos recibido del otro participante en la comunicación.

Con la forma de proceder según la invención, también en sistemas de automatización cuya transmisión de datos se realiza mediante un bus de campo Ethernet que puede contener además switchs como nodos de transmisión de paquetes de datos, existe la posibilidad de ampliar los programas de control con una capa de seguridad que garantiza la transmisión de datos pertinentes para la seguridad. Al tomar el carácter de comprobación que se incluye en el último paquete de datos recibido como valor inicial para el cálculo del carácter de comprobación del siguiente paquete de datos que ha de enviarse, se evita que, al igual que en el protocolo Profi-Safe, en una secuencia de paquetes de datos puedan repetirse de forma idéntica los paquetes de datos. Con ello, no existe el riesgo de que, cuando en la transmisión de datos los paquetes de datos, por ejemplo, se almacenen temporalmente en la red Ethernet mediante switchs, los paquetes de datos no puedan identificarse correctamente debido a que se producen confusiones. Gracias a la generación dinámica continua según la invención de los caracteres de comprobación, en una secuencia de paquetes de datos no se presentan paquetes de datos idénticos.

Según una primera forma de realización preferida, se comprueba la corrección de un paquete de datos recibido por un participante en la comunicación calculando el carácter de comprobación del paquete de datos recibido y comparándolo con el carácter de comprobación contenido en el paquete de datos recibido, tomándose como valor inicial para el cálculo el carácter de comprobación del último paquete de de datos enviado. Con este diseño de la capa de seguridad puede prescindirse del uso de números de secuencia en los paquetes de datos de seguridad, necesarios en el protocolo Profi-Safe para identificar una secuencia de paquetes de datos correcta. La secuencia correcta de paquetes de datos puede obtenerla, en concreto, el participante en la comunicación según la invención directamente a partir del carácter de comprobación transmitido en el que se determina el valor inicial del carácter de comprobación que se presenta nuevamente al participante receptor de la comunicación.

Según otra forma de realización preferida, la comunicación de datos en la capa de seguridad según la invención se configura de modo que un participante en la comunicación actúa como iniciador de la transmisión de datos y, para iniciar una transmisión de datos entre los dos participantes en la comunicación, transmite un paquete de datos de identificación al otro participante en la comunicación, utilizándose preferiblemente como valor inicial del carácter de comprobación para el paquete de datos de identificación un valor fijo o un identificador del otro participante en la comunicación. Con esta forma de proceder, tras una interrupción de la comunicación, puede garantizarse de forma fiable un intercambio de datos pertinentes para la seguridad en el sistema de automatización. En este sentido, se prefiere además utilizar como identificador en el paquete de datos de identificación enviado un dato para la identificación del otro participante en la comunicación, con lo que es posible una inicialización sencilla y fiable de la conexión de comunicación.

Según otra forma de realización preferida, para iniciar una transmisión de datos entre los participantes en la comunicación en otro paquete de datos se transmite otro dato, preferiblemente por el participante en la comunicación que actúa como iniciador de la transmisión de datos, a continuación del paquete de datos de identificación. Este otro dato es un identificador de sesión aleatorio o un identificador de sesión que varía según un algoritmo predeterminado. El identificador de sesión se ocupa de que también tras una interrupción de la conexión de comunicación y una reinicialización no se presenten paquetes de datos que se repitan.

Según otra forma de realización preferida, para iniciar una transmisión de datos entre los participantes en la comunicación, preferiblemente el participante en la comunicación que actúa como iniciador de la transmisión de datos transmite al otro participante en la comunicación datos de parámetros con un paquete de datos de parámetros que sigue al paquete de datos de identificación y al paquete de datos de sesión. Con ello se garantiza que, en el marco de la capa de seguridad, también se transmiten de forma segura los parámetros operativos pertinentes para la funcionalidad del aparato. Asimismo, en este sentido se prefiere dotar al paquete de datos con un dato de clasificación que identifica los datos transmitidos en el paquete de datos.

Según otra forma de realización preferida, durante el cálculo del carácter de comprobación por el sistema de automatización se tiene en cuenta el número de secuencia que identifica la secuencia de telegrama correspondiente de la transmisión de datos entre los dos participantes en la comunicación. Preferiblemente, el número de secuencia se genera en este caso por los dos participantes de la comunicación de forma independiente entre sí según un esquema predeterminado. Mediante la inclusión del número de secuencia en el cálculo se garantiza de forma fiable que el carácter de comprobación siempre cambia durante la transmisión de una secuencia de telegrama a otra. Con esto se descarta que, cuando telegramas de datos sucesivos contengan los mismos datos, pueda producirse un carácter de comprobación idéntico, lo que podría conducir a una alarma de fallo. En este sentido, el número de secuencia no debe transmitirse conjuntamente en los paquetes de datos entre los participantes en la comunicación dado que los participantes en la comunicación pueden generar el número de secuencia de forma independiente entre sí según un esquema predeterminado. El número de secuencia puede generarse en este sentido en los distintos participantes en la comunicación, por ejemplo, mediante cálculo exponencial o también mediante la extracción a partir de un bloque de números predeterminado que conocen los dos participantes en la comunicación. La transmisión del número de secuencia entre los participantes en la comunicación conduciría a un paquete de datos innecesariamente largo. En especial, cuando se utilizan números de secuencia largos para evitar que se excedan los números de secuencia durante una comunicación de datos.

Según otra forma de realización preferida, los paquetes de datos transmitidos entre los participantes en la comunicación contienen un identificador de conexión. Con ello se garantiza que, cuando un participante en la comunicación realiza una transmisión de paquetes de datos pertinentes para la seguridad con otros participantes en la comunicación diferentes, no se produce una confusión de los paquetes de datos debido a un carácter de comprobación casualmente igual de dos paquetes de datos recibidos por diferentes participantes en la comunicación.

La invención se explicará de forma detallada mediante los dibujos adjuntos. Muestran:

la fig. 1 la estructura básica de un sistema de automatización basado en Ethernet;

la fig. 2 un flujo de datos y esquema de procesamiento fundamentales para una capa de seguridad según la invención con una primera forma de paquete de datos;

las figs. 3A a 3C, un flujo de datos y esquema de procesamiento ampliado para una capa de seguridad según la invención con una segunda forma de paquete de datos, mostrando la figura 3A una transmisión de datos de inicia-

lización, la figura 3B una transmisión de datos de parámetros, y la figura 3C una transmisión de datos de procesos; y

la fig. 4 otro flujo de datos y esquema de procesamiento fundamentales para una capa de seguridad según la invención con una tercera forma de paquete de datos.

Con las redes de comunicación pueden intercambiarse de forma sencilla y utilizarse conjuntamente datos y/o recursos entre estaciones de trabajo, denominadas también en lo sucesivo “estaciones de trabajo”. En este sentido, el concepto de Ethernet es el estándar de comunicación más divulgado en redes de comunicación limitadas localmente. En Ethernet, múltiples participantes en la comunicación están conectados entre sí a través de un medio de transmisión común, realizándose el encapsulado de los datos que van a transmitirse en denominados “paquetes de datos” también denominados en lo sucesivo “telegramas”, con un formato predeterminado. En este sentido, Ethernet está compuesta por tres áreas, el hardware, es decir, el medio de transmisión y las interfaces de red de los participantes en la comunicación, el conjunto de protocolos que controlan el acceso a través del medio de transmisión, y la forma de los paquetes de Ethernet. En este caso, para conectar a los participantes en la comunicación puede utilizarse cualquier topología de red.

La figura 1 muestra una topología de red preferida para una red Ethernet. Aquí, los participantes 1 en la comunicación están conectados en forma de estrella mediante conexiones 2 punto a punto con un puesto 3 de conmutación central, el denominado “switch”. El switch 3 se ocupa de que los telegramas de datos entrantes sólo se conmuten a la salida a la que está conectado el participante en la comunicación que debe recibir el telegrama. Los telegramas de datos se almacenan temporalmente en el switch para poder emitirlos a la salida correcta.

Cada uno de los participantes 1 en la comunicación presenta, tal como muestra la figura 1, una unidad 11 de conexión de red. La unidad 11 de conexión de red realiza la codificación de los datos que deben enviarse y la decodificación de los datos recibidos. Además, en la unidad 11 de conexión también se gestionan todas las medidas de control necesarias para el funcionamiento de la red, es decir, la unidad 11 de conexión realiza la gestión y la formación de los paquetes de datos.

En el uso de una red Ethernet, tal como se muestra en la figura 1, en el marco de un sistema de automatización en el que los participantes en la comunicación son ordenadores de control y sistemas de máquinas de sensores y actores, un requisito importante, además de la capacidad de tratamiento en tiempo real, es decir, la necesidad de que los ordenadores de control emitan las señales de proceso a los actores basándose en las señales de proceso registradas por los sensores en intervalos de tiempo de proceso determinados, es garantizar que, en caso de fallo del sistema de automatización o de un componente importante, no existe ningún peligro para las personas o el medio ambiente. Por tanto, los ordenadores de control en el sistema de automatización deben realizar, además de las funciones de control normales, también funciones de seguridad que garantizan que, en caso de fallo de un componente importante del sistema de automatización, se encargan de que el sistema de automatización pase automáticamente a un estado seguro según el denominado “principio Fail-Safe”, es decir, que se realice una desconexión de emergencia de las máquinas conectadas.

El número de las funciones de seguridad en un programa de control que se ejecuta en un sistema de automatización normalmente es menor que el número de las funciones de control no críticas. No obstante, durante la realización de las funciones de seguridad debe asegurarse de forma fiable un desarrollo sin fallos de la transmisión de datos. En especial, debe garantizarse que, durante la transmisión de datos pertinentes para la seguridad entre los participantes en la comunicación en el sistema de automatización, se minimiza la probabilidad de que, debido a un fallo de la transmisión, se falseen los datos de tal modo que ya no pueda detectarse esta falsificación.

Para garantizar que la funcionalidad de funciones de control pertinentes para la seguridad no se ve afectada por funciones de control no pertinentes para la seguridad en el ordenador de automatización, el protocolo de red utilizado en el tramo de transmisión de datos está dotado de una capa de seguridad adicional que controla en el sistema de automatización el intercambio de datos de seguridad entre los participantes en la comunicación. Para garantizar una transmisión segura de paquetes de datos en un tramo de transmisión de datos entre dos participantes en la comunicación en el marco de la capa de seguridad en el sistema de automatización, según la invención, se dota a cada paquete de datos con un carácter de comprobación que se calcula a partir de los otros datos del paquete de datos, utilizando la unidad 11 de conexión del participante 1 de la comunicación el carácter de comprobación del último paquete de datos recibido por el otro participante en la comunicación como valor inicial para el cálculo del carácter de comprobación para un siguiente paquete de datos que debe enviarse al otro participante en la comunicación.

Mediante la forma de proceder según la invención en la que el carácter de comprobación en un paquete de datos se calcula con un valor inicial dinámico utilizándose siempre como valor inicial el carácter de comprobación del telegrama entrante anterior, puede garantizarse que en un ciclo de transmisión de datos no se presentan paquetes de datos idénticos que podrían conducir a una falsificación de los datos. Los paquetes de datos idénticos, especialmente en caso del uso de una topología de red Ethernet con un switch, tal como se muestra en la figura 1, representan un peligro de que, en este caso, los telegramas de datos intercambiados entre los participantes en la comunicación puedan almacenarse temporalmente y sólo puedan transmitirse al destinatario en un momento posterior.

En el procedimiento según la invención para la transmisión de datos, el participante en la comunicación que recibe un paquete de datos puede además comprobar fácilmente si el paquete de datos es correcto calculando el carácter de comprobación del paquete de datos recibido y comparándolo con el carácter de comprobación contenido en el paquete de datos recibido, tomándose como valor inicial para el cálculo el carácter de comprobación del último paquete de datos enviado. Esto lo realiza preferiblemente la unidad 11 de conexión del participante 1 en la comunicación. En caso de que exista una coincidencia del carácter de comprobación calculado con el carácter de comprobación contenido en el paquete de datos recibido, el paquete de datos puede valorarse como correcto.

La figura 2 muestra un flujo de datos y un esquema de trabajo del procedimiento según la invención para la transmisión de datos entre dos participantes en la comunicación. Uno de los participantes en la comunicación de la transmisión de datos, en caso de sistemas de automatización, un ordenador de control, actúa en este caso como iniciador de la transmisión de datos. Una máquina que contiene un sistema de sensores y actores en el sistema de automatización representa al respondedor en la transmisión de datos según la invención. La figura 2 muestra dos secuencias de telegramas durante el intercambio de datos entre el iniciador y el respondedor, transmitiéndose en cada secuencia de telegrama en cada caso un paquete de datos desde el iniciador al respondedor y desde el respondedor nuevamente al iniciador. Los paquetes de datos están compuestos en este caso por un área de datos de usuario que contiene los datos seguros, es decir, las señales de procesos necesarias en el marco del control de seguridad, y un área de datos de control, que aquí comprende, de forma opcional, un número de secuencia y, de forma obligatoria, un carácter de comprobación.

El número de secuencia indica de qué secuencia de telegrama se trata en la transmisión de datos en el marco de la versión del programa de seguridad. En este caso, el iniciador predetermina, en su paquete de datos enviado al respondedor, el número de secuencia, basándose en el cual el respondedor vuelve a transmitir conjuntamente de nuevo el número de secuencia en el paquete de datos devuelto. En la siguiente secuencia de telegrama se aumenta entonces una unidad el número de secuencia del iniciador en el paquete de datos enviado.

Sin embargo, en el marco de la transmisión de datos según la invención, puede prescindirse básicamente de la transmisión de un número de secuencia. Para constatar que ha tenido lugar una transmisión de datos falseada, tanto en el iniciador como también en el respondedor es suficiente con valorar el carácter de comprobación del paquete de datos recibido. El carácter de comprobación es preferiblemente un carácter de seguridad de bloque CRC (cyclic, Redundancy Check, comprobación de redundancia cíclica) con el que pueden detectarse fallos en el paquete de datos con una seguridad muy alta. El valor CRC se calcula entonces a partir de los datos de usuario y, dado el caso, también a partir del número de secuencia en el paquete de datos, utilizándose, según la invención, como valor inicial del cálculo CRC el valor CRC del último paquete de datos recibido.

En el paquete de datos de la secuencia i de telegramas mostrado en la figura 2 y enviado por el iniciador al respondedor, el valor CRC del paquete de datos que va a enviarse se calcula con el valor CRC del último valor CRC CRC_A $i-1$ recibido por el respondedor. El valor CRC que se obtiene entonces en el paquete de datos enviado es CRC_A i . Este valor CRC lo utiliza entonces el respondedor nuevamente como valor inicial en el cálculo CRC del paquete de datos devuelto por el respondedor al iniciador, obteniéndose como valor CRC entonces CRC_B i . El iniciador utiliza entonces este valor CRC en la siguiente secuencia $i+1$ de telegramas como valor inicial para el cálculo CRC para el siguiente paquete de datos que ha de enviársele al respondedor. El valor CRC CRC_A $i+1$ se emplea entonces nuevamente para el cálculo CRC del paquete de datos devuelto por el respondedor, obteniéndose como valor CRC CRC_B $i+1$. Con ello, el participante receptor de la comunicación siempre puede constatar de forma sencilla la correcta recepción de un paquete de datos porque el valor CRC del paquete de datos recibido se compara con un valor CRC calculado sobre la base del valor inicial almacenado.

Para garantizar adicionalmente, según la invención, que un programa de seguridad se inicia en la red entre los participantes en la comunicación correctos, durante un nuevo inicio del programa de seguridad o al reanudarlo tras una interrupción de la comunicación, se realiza una fase de inicialización tal como se muestra en la figura 3A. El paquete de datos mostrado en la figura 3A contiene en este caso un campo de datos de comandos que indica el significado de los datos de usuario en el paquete de datos, por ejemplo, si los datos de usuario son datos de identificación o datos de proceso. Sin embargo, de forma alternativa, el significado de los datos de usuario en los paquetes de datos de una secuencia de paquetes de datos para la implementación de un programa de seguridad también puede hacerse dependiente de la secuencia de los paquetes de datos. Así, por ejemplo, puede establecerse que los primeros dos datos enviados por el iniciador al respondedor siempre contengan datos de inicialización y los otros paquetes de datos posteriores contengan datos seguros. Al mismo tiempo, también puede establecerse que el respondedor transmita siempre únicamente datos de proceso al iniciador. La longitud de los paquetes de datos puede estar configurada de forma básicamente fija o variable. Además del campo de datos de comandos, el paquete de datos también puede contener otros campos de datos, por ejemplo, un campo de control / estado, tal como se muestra en la figura 3A.

Como se muestra adicionalmente en la figura 3A, durante el nuevo inicio del programa de control, para establecer una comunicación de datos segura el iniciador realiza una inicialización enviando al respondedor en la primera secuencia de telegrama un paquete de datos con el campo de datos de comandos "identificación" y datos seguros que permiten una identificación. El paquete de datos de identificación se protege en este caso con un valor CRC como carácter de comprobación, cuyo valor inicial es un valor predeterminado de forma fija, por ejemplo, el identificador del aparato del respondedor. Los datos de identificación pueden ser en este caso datos de dirección ajustados desde fuera

ES 2 335 788 T3

que identifican a los dos participantes de la comunicación o también sólo al respondedor. En este sentido, también pueden ser identificadores de aparatos y / o números de serie del iniciador o del respondedor.

El respondedor, que conoce el valor inicial del cálculo CRC del primer paquete de datos recibido, comprueba el valor CRC CRC_A 1 del primer paquete de datos recibido del iniciador para constatar si ha tenido lugar una transmisión de datos correcta. A continuación, el respondedor toma entonces el valor CRC CRC_A 1 del primer paquete de datos del iniciador como valor inicial para el cálculo CRC CRC_B 1 del paquete de datos que debe enviarse de vuelta al iniciador. Este paquete de datos devuelto utiliza como comando preferiblemente el mismo identificador que está contenido en la parte de datos de comandos del paquete de datos de identificación transmitido por el iniciador para indicar que se trata del paquete de datos devuelto de la primera secuencia de telegrama. El iniciador comprueba entonces el paquete de datos devuelto por el respondedor al iniciador de la primera secuencia de telegrama en relación con la correcta transmisión de los datos mediante el cálculo del total CRC que cabe esperar sobre la base del valor CRC_A 1 inicial conocido y comparándolo con el total CRC CRC_B 1 del paquete de datos recibido.

En una segunda secuencia de telegrama, el iniciador envía entonces otro paquete de datos de inicialización al respondedor que contiene un número de sesión como sesión de comando y como datos seguros. El valor CRC CRC_A 2 de este segundo paquete de datos se calcula en este caso con el valor CRC CRC_B 1 del paquete de datos devuelto por el respondedor. El número de sesión transmitido puede generarse en este caso de forma aleatoria o según un algoritmo predeterminado, y debe garantizar que, tras una interrupción de la conexión de comunicación, no puede transmitirse ningún paquete de datos a partir de la transmisión de datos precedente o que estos se detectan.

El respondedor, que conoce el valor inicial CRC_B 1 para el cálculo CRC del paquete de datos enviado por el iniciador, comprueba el paquete de datos de sesión recibido mediante el cálculo del valor CRC que cabe esperar sobre la base del valor inicial conocido, y toma entonces el valor CRC CRC_A 2 nuevamente como valor inicial para un segundo paquete de datos que debe enviarse al iniciador, con el cual pueden transmitirse opcionalmente datos seguros. En el caso de este segundo paquete de datos devuelto, se utiliza como comando preferiblemente el comando sesión del paquete de datos recibido del iniciador.

Tras el establecimiento de la conexión de comunicación segura, el iniciador puede transmitir opcionalmente al respondedor otros datos de parámetros seguros que son necesarios para el funcionamiento del respondedor. En la figura 3B, se muestran dos de estas secuencias de telegramas, la secuencia 3 de telegramas que sigue a la transmisión del paquete de datos de sesión y la última secuencia de telegrama realizada con datos de parámetros.

Para la transmisión de los paquetes de datos con los datos de parámetros, el iniciador toma el último valor CRC CRC_B 2 recibido como valor inicial para el cálculo CRC del primer paquete de datos de parámetros, que dota adicionalmente con el comando datos de parámetro y parámetro 1 de datos seguros. El respondedor comprueba el valor CRC CRC_A 3 del paquete de datos recibido y toma este valor CRC como valor inicial para un cálculo CRC del paquete de datos de respuesta al iniciador. Así, pueden transmitirse tantos datos de parámetro seguros al respondedor como se desee. En el ejemplo mostrado en la figura 3B, se transmiten secuencias de telegramas con datos de parámetros seguros desde el iniciador al respondedor. El respondedor transmite en los paquetes de datos de respuesta siempre de forma opcional datos seguros, utilizándose datos de parámetros como comando en los paquetes de datos de respuesta.

Tras la finalización de la transmisión de parámetros, el iniciador realiza, tal como se muestra en la figura 3C, una transmisión de datos de proceso. Para ello, el iniciador dota a los paquetes de datos con el comando datos de proceso y con los datos de proceso datos seguros y los protege con un total CRC CRC_A n+3 que se calcula con el valor CRC CRC_B n+2 como valor inicial transmitido en la última respuesta de datos de parámetro por el respondedor al iniciador. El respondedor envía nuevamente los datos de proceso en su paquete de datos de respuesta protegido con el total CRC CRC_B n+3, que se calcula con el total CRC CRC_A n+3 transmitido por el iniciador como valor inicial.

La figura 4 muestra otro flujo de datos y esquema de trabajo para un procedimiento según la invención para la transmisión de datos entre dos participantes en la comunicación. El flujo de datos y el esquema de trabajo corresponden en este caso fundamentalmente al flujo de datos y al esquema de trabajo mostrados en la figura 2. Sin embargo, en el paquete de datos, a diferencia del paquete de datos mostrado en la figura 2, siempre se transmite adicionalmente un identificador de la conexión, tal como se transmite ya en la figura 3A durante la fase de inicialización en la parte de datos de comando en el marco del paquete de datos de identificación. El identificador de la conexión puede ser, al igual que los datos de identificación según la figura 3, una dirección ajustada desde fuera que identifica a los dos participantes en la comunicación o también sólo al respondedor. En este caso, también puede tratarse nuevamente de identificadores de aparatos y / o números de serie del iniciador o el respondedor. Mediante la transmisión del identificador de la conexión se garantiza de forma fiable que, cuando el iniciador realiza al mismo tiempo con varios respondedores una transmisión de datos pertinentes para la seguridad, no se produce ninguna confusión de los paquetes de datos debido a un carácter de comprobación casualmente igual de los paquetes de datos contenidos por diferentes respondedores.

Asimismo, en el flujo de datos mostrado en la figura 4, siempre se incluye conjuntamente el número de secuencia del cálculo del carácter de comprobación del participante correspondiente en la comunicación. Sin embargo, este número de secuencia no se transmite conjuntamente sino que lo genera el participante en la comunicación de forma independiente según el mismo esquema. El número de secuencia puede, por ejemplo, calcularse exponencialmente de forma automática tras la inicialización o extraerse de un bloque de números determinado de forma fija. Dado que el

ES 2 335 788 T3

número de secuencia no se transmite conjuntamente, la longitud del paquete de datos tampoco se alarga innecesariamente. Al mismo tiempo, el número de secuencia generado por los participantes en la comunicación puede elegirse con la longitud que se desee para evitar de forma fiable que este se exceda. Mediante la inclusión del número de secuencia en el cálculo del carácter de comprobación se garantiza que, cuando los paquetes de datos no varían de una secuencia de telegrama a la siguiente, se produzca a pesar de ello un cambio del carácter de comprobación y se garantiza con ello que no se active una falsa alarma indeseada.

Con la forma de proceder según la invención, en la que, al transmitir paquetes de datos, se dotan los paquetes de datos con caracteres de comprobación que se calculan con el carácter de comprobación del último paquete de datos recibido por el otro participante en la comunicación como valor inicial, existe la posibilidad de conseguir de forma sencilla y fiable una transmisión segura de los datos tal como se requiere en el marco de una capa de seguridad en un sistema de automatización. En especial, existe la posibilidad de utilizar como protocolo de red el protocolo Ethernet y utilizar una estructura de red con switchs que almacenan temporalmente los paquetes de datos dado que, según la invención, se evita que dentro del desarrollo de un programa de seguridad se repitan los paquetes de datos.

Según la invención, la transmisión de los datos se realiza además de modo que primero se realiza una inicialización con una transmisión de números de identificación y una transmisión de números de sesión, con lo que se evita que, durante un nuevo inicio, pueda producirse una repetición de los paquetes de datos. Además, en el marco de la transmisión de datos según la invención existe la posibilidad de transmitir también parámetros operativos que se necesitan para la funcionalidad de los aparatos del respondedor en el sistema de automatización.

REIVINDICACIONES

- 5 1. Procedimiento para la transmisión de paquetes de datos en un tramo de transmisión de datos entre dos participantes en la comunicación, conteniendo los paquetes de datos en cada caso un carácter de comprobación que se calcula a partir de los otros datos del paquete de datos, **caracterizado** porque un participante en la comunicación utiliza el carácter de comprobación del último paquete de datos recibido por el otro participante en la comunicación como valor inicial en el cálculo del carácter de comprobación para un siguiente paquete de datos que ha de enviarse al otro participante en la comunicación.
- 10 2. Procedimiento según la reivindicación 1, **caracterizado** porque un paquete de datos recibido por un participante en la comunicación se identifica como correcto calculando el carácter de comprobación del paquete de datos recibido y comparándolo con el carácter de comprobación contenido en el paquete de datos recibido, tomándose para el cálculo el carácter de comprobación del último paquete de datos enviado como valor inicial.
- 15 3. Procedimiento según la reivindicación 1 ó 2, **caracterizado** porque el paquete de datos contiene un dato de clasificación que identifica los datos transmitidos con el paquete de datos.
- 20 4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado** porque uno de los participantes en la comunicación actúa como el iniciador de la transmisión de datos y, al comienzo de una transmisión de datos entre los dos participantes en la comunicación, transmite al otro participante en la comunicación un paquete de datos de identificación que contiene un identificador.
- 25 5. Procedimiento según la reivindicación 4, **caracterizado** porque el participante en la comunicación que actúa como iniciador de la transmisión de datos utiliza un valor fijo o un identificador del otro participante en la comunicación como valor inicial del carácter de comprobación para el paquete de datos de identificación.
- 30 6. Procedimiento según la reivindicación 4 ó 5, **caracterizado** porque el paquete de datos de identificación enviado por el participante en la comunicación que actúa como iniciador de la transmisión de datos contiene como identificador un dato para la identificación del otro participante en la comunicación.
- 35 7. Procedimiento según una de las reivindicaciones 4 a 6, **caracterizado** porque, al inicio de una transmisión de datos entre los dos participantes en la comunicación, se transmite como un dato adicional un identificador de sesión aleatorio o un identificador de sesión que varía en función de un algoritmo predeterminado.
- 40 8. Procedimiento según la reivindicación 7, **caracterizado** porque el participante en la comunicación que actúa como iniciador de la transmisión de datos transmite al otro participante en la comunicación el identificador de sesión con un paquete de datos de sesión que sigue al paquete de datos de identificación.
- 45 9. Procedimiento según una de las reivindicaciones 4 a 8, **caracterizado** porque, al inicio de una transmisión de datos entre los dos participantes en la comunicación, se transmiten datos de parámetros.
10. Procedimiento según la reivindicación 9, **caracterizado** porque el participante en la comunicación que actúa como iniciador de la transmisión de datos transmite al otro participante en la comunicación los datos de parámetros con al menos un paquete de datos de parámetros que sigue al paquete de datos de identificación y al paquete de datos de sesión.
- 50 11. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado** porque como tramo de transmisión de datos se utiliza un bus de campo basado en Ethernet.
- 55 12. Procedimiento según una de las reivindicaciones 1 a 11, **caracterizado** porque durante el cálculo del carácter de comprobación se considera un número de secuencia que identifica la secuencia de telegrama correspondiente de la transmisión de datos entre los dos participantes en la comunicación.
13. Procedimiento según la reivindicación 12, **caracterizado** porque los dos participantes en la comunicación generan el número de secuencia que identifica una secuencia de telegrama de forma independiente entre sí según un esquema predeterminado.
- 60 14. Procedimiento según una de las reivindicaciones 1 a 13, **caracterizado** porque los paquetes de datos transmitidos entre los dos participantes en la comunicación incluyen en cada caso un identificador de conexión.
- 65 15. Sistema de automatización con dos participantes (1) en la comunicación conectados a través de un tramo (2) de transmisión de datos que presentan en cada caso una unidad (11) de conexión para transmitir paquetes de datos en el tramo de transmisión de datos entre los dos participantes en la comunicación, presentando la unidad (11) de conexión medios para formar paquetes de datos con un carácter de comprobación calculado a partir de los otros datos en el paquete de datos, **caracterizado** porque el valor inicial para el cálculo del carácter de comprobación para un paquete de datos que ha de enviarse al otro participante en la comunicación es el carácter de comprobación del último paquete de datos recibido por el otro participante en la comunicación.

16. Sistema de automatización según la reivindicación 15, **caracterizado** porque la unidad (11) de conexión de los participantes (1) en la comunicación presenta medios para identificar como correcto un paquete de datos recibido por uno de los participantes en la comunicación calculando el carácter de comprobación del paquete de datos recibido y comparándolo con el carácter de comprobación contenido en el paquete de datos recibido, tomándose como valor inicial para el cálculo el carácter de comprobación del último paquete de datos enviado.

17. Sistema de automatización según la reivindicación 15 ó 16, **caracterizado** porque la unidad (11) de conexión de los participantes (1) en la comunicación presenta medios para dotar al paquete de datos con un dato de clasificación que identifica los datos transmitidos con el paquete de datos.

18. Sistema de automatización según una de las reivindicaciones 15 a 17, **caracterizado** porque uno de los participantes en la comunicación actúa como iniciador de la transmisión de datos y su unidad (11) de conexión presenta medios para generar un paquete de datos de identificación que contiene un identificador como primer paquete de datos que debe transmitirse en una transmisión de datos entre los dos participantes en la comunicación.

19. Sistema de automatización según la reivindicación 18, **caracterizado** porque la unidad (11) de conexión del participante en la comunicación que actúa como iniciador de la transmisión de datos utiliza un valor fijo o un identificador del otro participante en la comunicación como valor inicial del carácter de comprobación para el paquete de datos de identificación.

20. Sistema de automatización según la reivindicación 18 ó 19, **caracterizado** porque el paquete de datos de identificación enviado por el participante en la comunicación que actúa como iniciador de la transmisión de datos contiene como identificador un dato para la identificación del otro participante en la comunicación.

21. Sistema de automatización según una de las reivindicaciones 18 a 20, **caracterizado** porque la unidad (11) de conexión del participante en la comunicación que actúa como iniciador de la transmisión de datos presenta medios para generar, tras el paquete de datos de identificación, un paquete de datos de sesión que contiene un identificador de sesión aleatorio o un identificador de sesión que varía en función de un algoritmo predeterminado.

22. Sistema de automatización según la reivindicación 21, **caracterizado** porque la unidad (11) de conexión del participante en la comunicación que actúa como iniciador de la transmisión de datos presenta medios para generar, tras el paquete de datos de identificación y el paquete de datos de sesión, al menos un paquete de datos de parámetros que contiene datos de parámetros para el otro participante en la comunicación.

23. Sistema de automatización según una de las reivindicaciones 15 a 22, **caracterizado** porque el tramo de transmisión de datos es un bus de campo basado en Ethernet.

24. Sistema de automatización según una de las reivindicaciones 15 a 23, **caracterizado** porque la unidad (11) de conexión de los participantes (1) en la comunicación presenta medios que, durante el cálculo del carácter de comprobación, tienen en cuenta un número de secuencia que identifica la secuencia de telegrama correspondiente de la transmisión de datos entre los dos participantes en la comunicación.

25. Sistema de automatización según la reivindicación 24, **caracterizado** porque la unidad (11) de conexión de los participantes (1) en la comunicación presenta medios para generar un número de secuencia que identifica una secuencia de telegrama según un esquema predeterminado.

26. Sistema de automatización según una de las reivindicaciones 15 a 25, **caracterizado** porque la unidad (11) de conexión de los participantes (1) en la comunicación presenta medios para dotar al paquete de datos con un identificador de conexión.

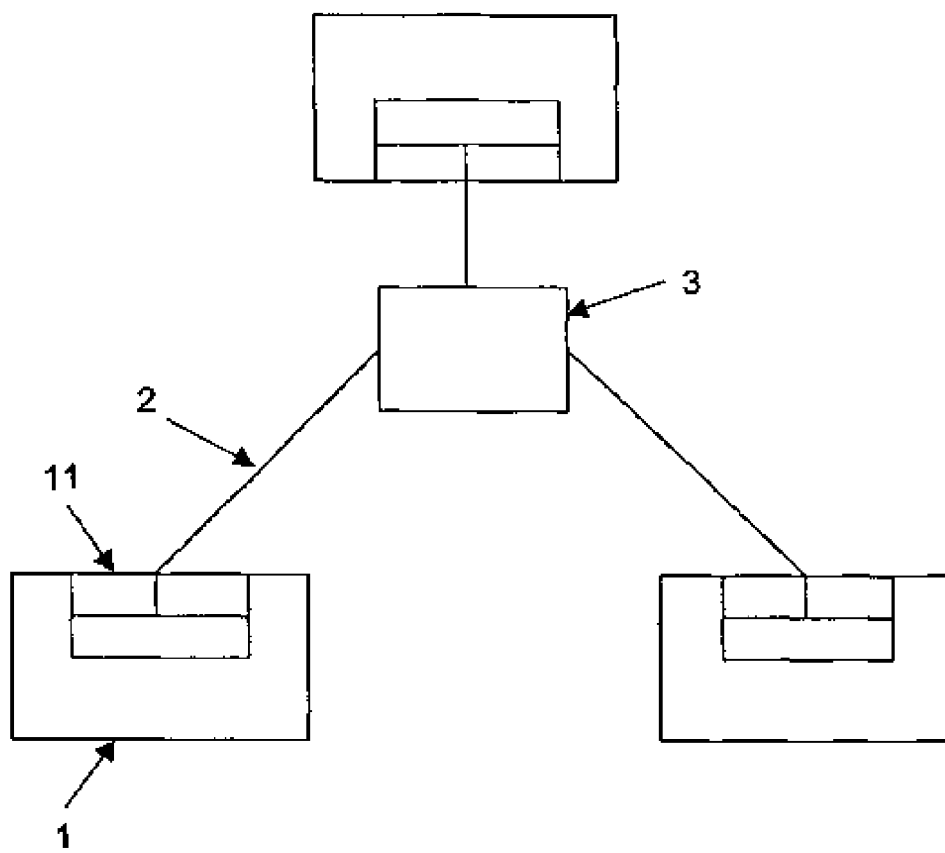


Fig. 1

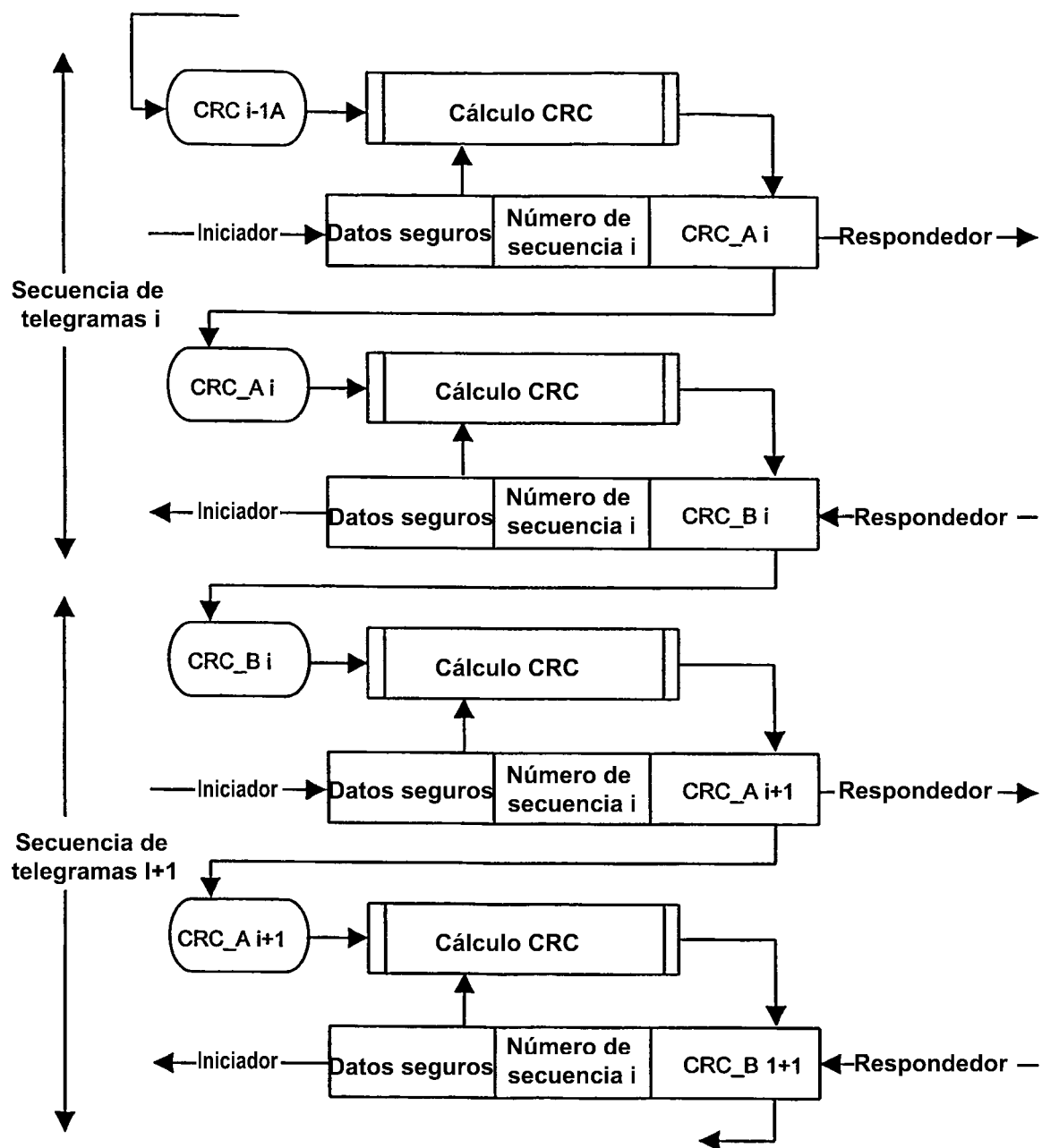


Fig. 2

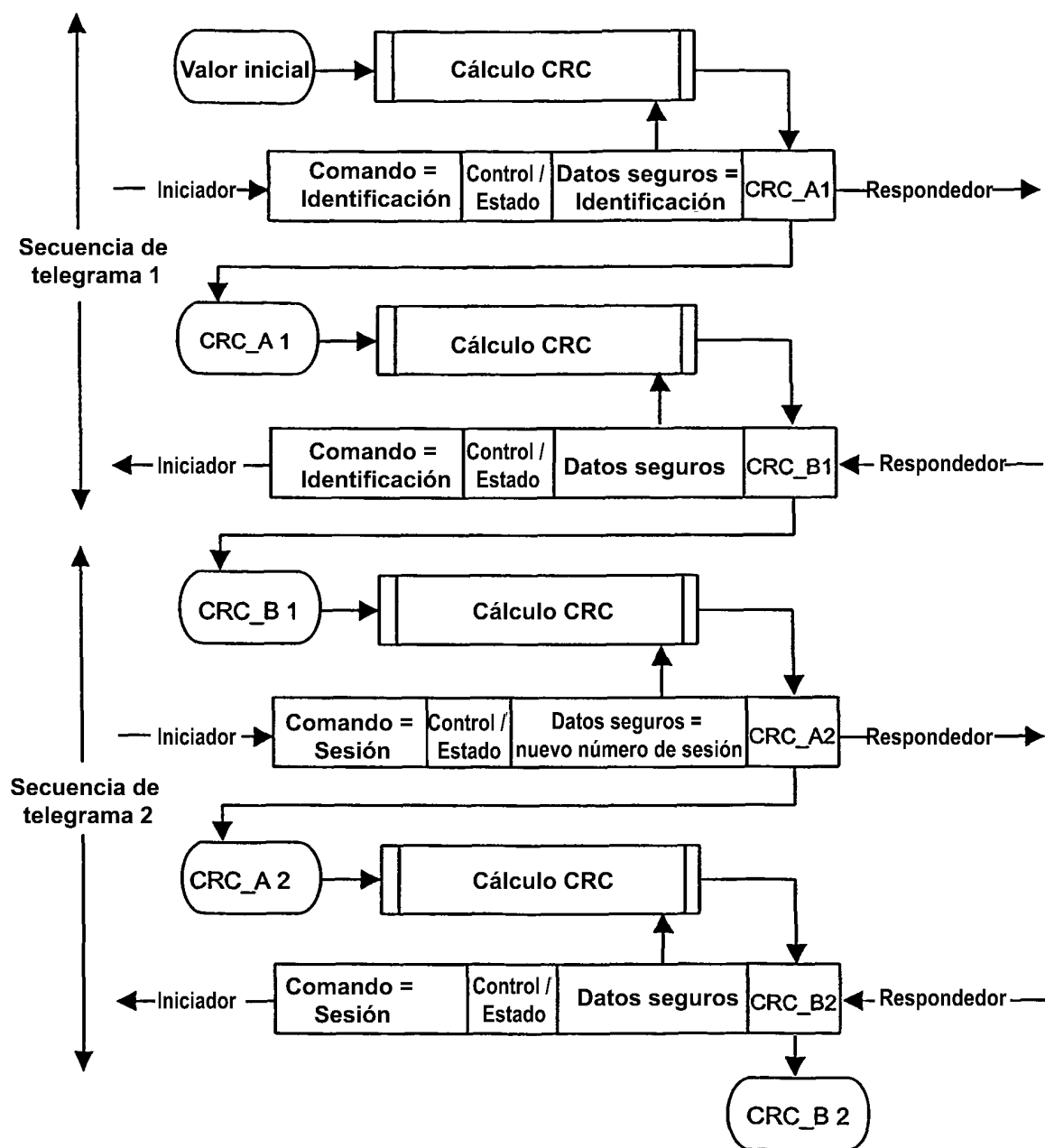


Fig. 3A

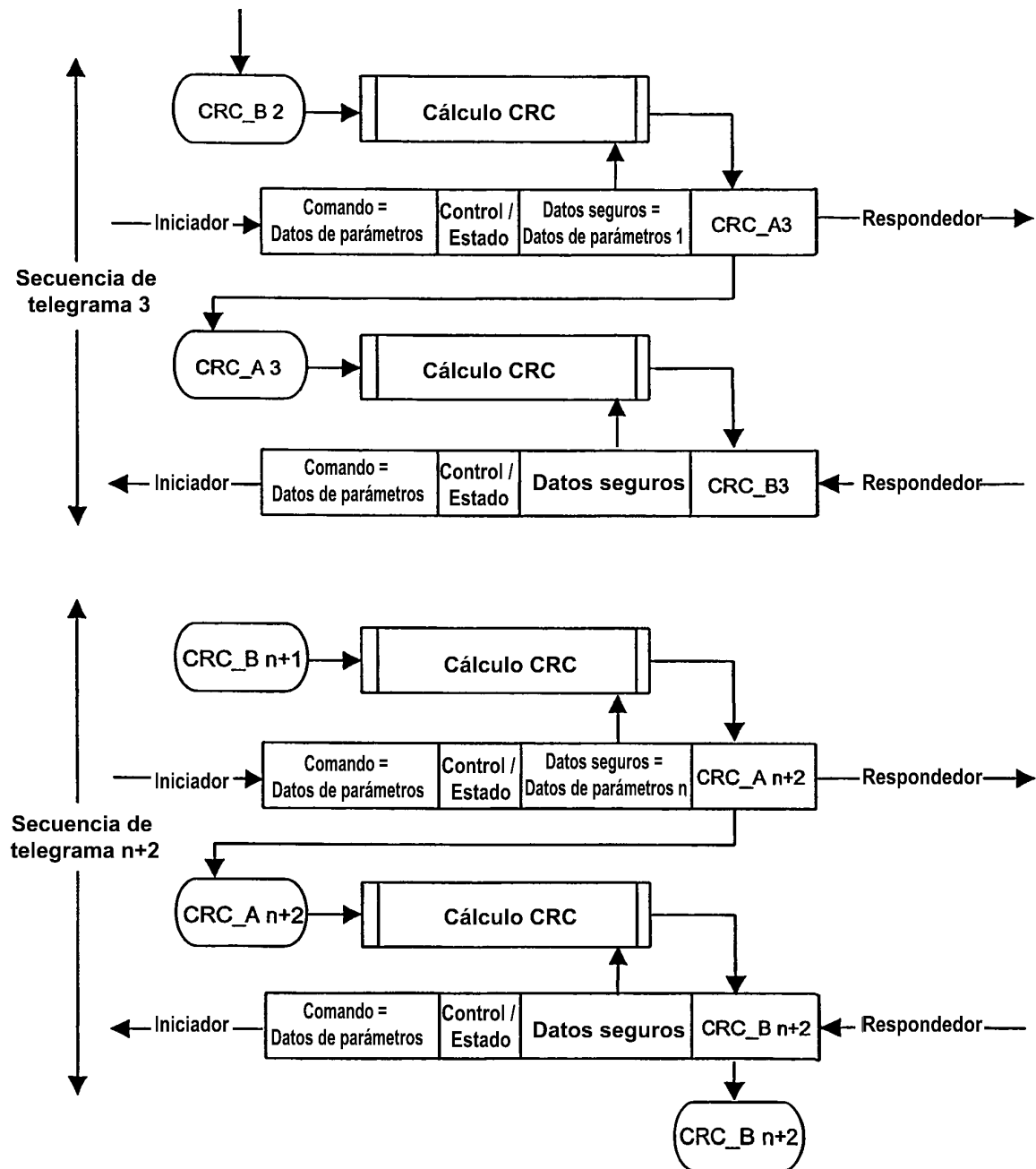


Fig. 3B

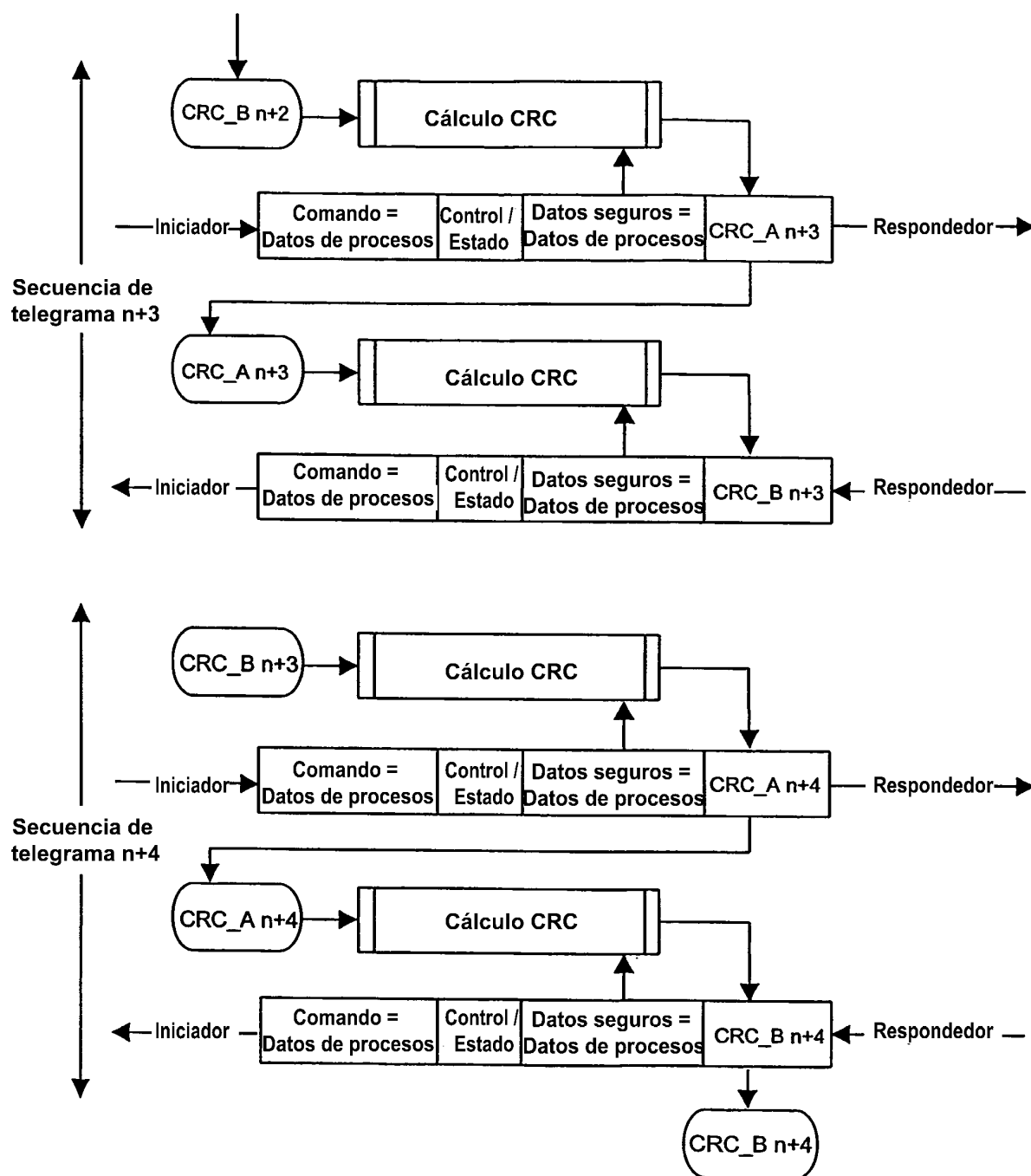


Fig. 3C

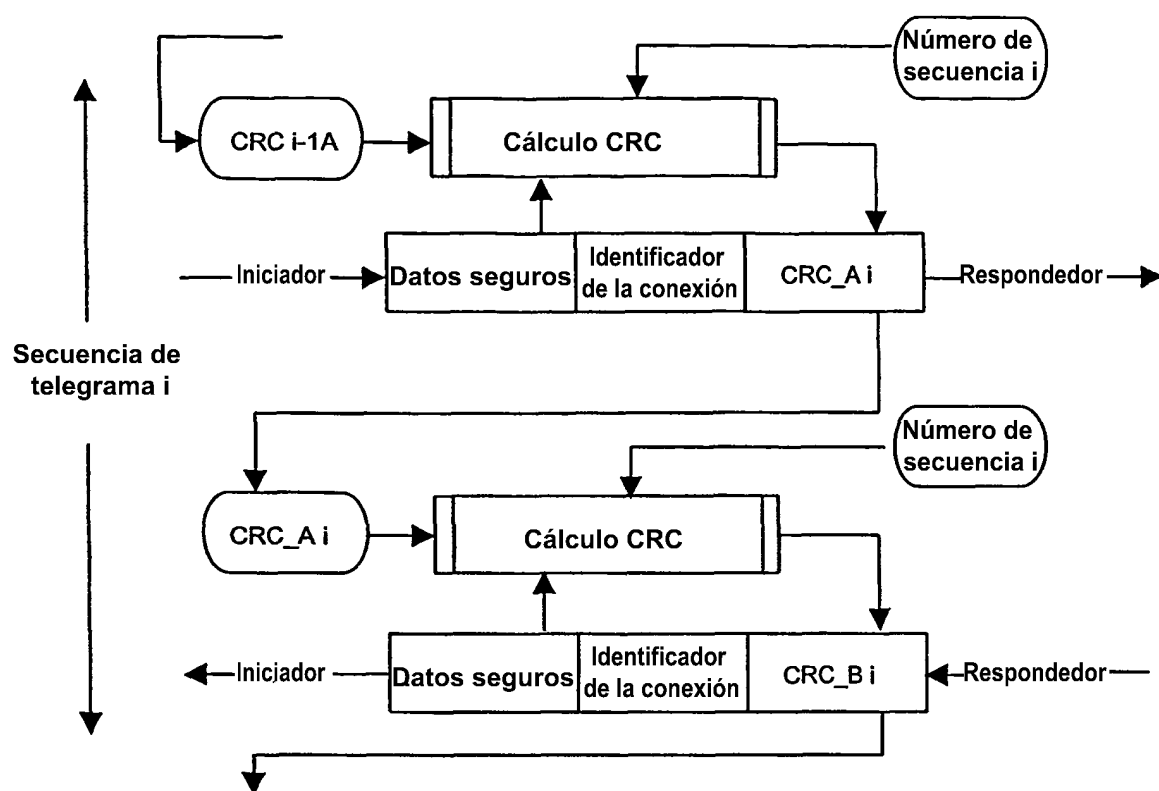


Fig. 4