(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 577 104**

(51) Int. CI.:

***G06F 11/16*** (2006.01)
***G06F 11/18*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.07.2013 E 13176326 (0)**

(97) Fecha y número de publicación de la concesión europea: **25.05.2016 EP 2824572**

(54) Título: **Dispositivo de prevención de fallos y método para operar el dispositivo de prevención de fallos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**13.07.2016**

(73) Titular/es:

**THALES DEUTSCHLAND GMBH (100.0%)**
**Thalesplatz 1**
**71254 Ditzingen, DE**

(72) Inventor/es:

**ILIE, GABRIEL CRISTIAN;**
**MARINGER, DANIEL;**
**NIEDERMAYER, KLAUS y**
**GRUND, DANIEL**

(74) Agente/Representante:

**ISERN JARA, Nuria**

## DESCRIPCIÓN

Dispositivo de prevención de fallos y método para operar el dispositivo de prevención de fallos

La invención se refiere a un sistema de prevención de fallos para un Sistema de Salida de Datos y un método para operar un sistema de prevención de fallos.

Antecedentes de la invención

La presente invención se refiere a sistemas de seguridad crítica (ferrocarril, aviación, nucleares, etc.) donde se obtienen niveles de seguridad elevados requeridos mediante la implementación de múltiples bloques funcionales independientes (canales). Se acepta en general que un fallo que produjera potencialmente una salida insegura (y en consecuencia la pérdida de la vida y/o daño de la propiedad caro) no puede producirse simultáneamente en todos los bloques. Por lo tanto, mediante la multiplicación funcional, se reduce enormemente la probabilidad de fallo inseguro en el nivel de sistema.

En la industria del ferrocarril, por ejemplo, por práctica general y por recomendaciones normalizadas específicas de seguridad (EN50129), se usa tal estructura de múltiples bloques bajo la expresión "seguridad de fallos compuesta". Tal estructura se representa en la Figura 1B. Otras estructuras también usadas en la industria se representan en la Figura 1A y en la Figura 1C.

Para la implementación de prevención de fallos compuestos como se muestra en la Figura 1B diferentes canales comparten la misma entrada mientras las salidas de los canales se someten sondeo. Las posibles salidas son "Alto" y "Bajo". Se proporciona un bloque complementario denominado "dispositivo de sondeo"; por lo que se elige la salida del sistema dependiendo del siguiente criterio: si la unanimidad (o la mayoría) de las salidas están en estado "Alto" (circuito cerrado), la salida del dispositivo de sondeo es "Alta", de otra manera la salida del dispositivo de sondeo es "Baja" (circuito abierto). Es decir un canal no puede accionar la salida en estado "Alto" únicamente por sí mismo, sino siempre en conjunto con al menos otro canal, reduciendo de esta manera el riesgo de una salida errónea, el componente crítico de la implementación de seguridad de fallos compuesta descrito anteriormente es el dispositivo de sondeo. Para asegurar la fiabilidad del dispositivo de sondeo, el dispositivo de sondeo tiene que probarse con frecuencia (que lleva tiempo) o el sistema tiene que equiparse con un dispositivo de sondeo redundante (es decir se requiere hardware adicional).

Los dispositivos de prevención de fallos compuestos como se ha descrito anteriormente se usan preferentemente para una salida digital directa (ACTIVADO/DESACTIVADO), pero requieren hardware y software adicional para subsistemas que emiten mensajes de datos completos (telegramas).

Un telegrama es un flujo de bits de datos, es decir una secuencia de bits. Preferentemente comprende un bloque de dirección, un bloque de información y un bloque de CRC. Los subsistemas que emiten telegramas se denominan como "Sistemas de Salida de Datos".

En general un telegrama se transmite hacia otro subsistema a través de un medio de transmisión de datos (tal como cables de cobre, radio, fibra óptica, etc.). El telegrama se construye de tal manera que el medio de transmisión no supone una amenaza a la función de seguridad del sistema por ruido, distorsión o interferencia. Alguna de la mayoría de las contramedidas implementadas en esta dirección son: modulación apropiada y protección de canal de acuerdo con el medio de transmisión, alfabeto restringido usado para componer el telegrama, estructura interna restringida del telegrama, encriptación de datos, códigos de comprobación de paridad (CRC) parcial (interna) y código de comprobación de paridad (CRC) general, anexados al final de la transmisión.

La mayoría de las implementaciones estructurales conocidas para Sistemas de Salida de Datos se basan en el principio de Prevención de Fallos Reactivo presentado en la Figura 1C o se basan en una estructura de salida digital compuesta presentada en la Figura 1A y 1C. Ambas soluciones requieren dispositivos de sondeo seguros o comparadores seguros.

El documento EP 0 556 805 A2 desvela un sistema de procesamiento de información para realizar una función de prevención de fallos mediante software. Al menos se proporcionan tres procesadores de información. En cada procesador de información, los mismos datos añadidos con un código de redundancia cíclica se someten a un proceso de enmascaramiento predeterminado y se codifican posteriormente basándose en un desplazamiento lógico cíclico. Se realiza un producto lógico o combinación O exclusiva de datos codificados desde los procesadores de información y se someten a un desplazamiento lógico cíclico inverso para decodificación en un dato original. Visualizando los datos decodificados en un dispositivo de visualización o similares, los datos originales se hacen identificables puesto que se visualiza un carácter que tiene un significado si los datos decodificados son normales y se visualiza un carácter no evidente en significado si los datos decodificados son anormales.

Objeto de la invención

Es un objeto de la invención proporcionar un sistema de prevención de fallos y un método para operar un sistema de prevención de fallos con una estructura sencilla.

Sumario de la invención

Este objeto se resuelve mediante un sistema de prevención de fallos de acuerdo con la reivindicación 1 y un método de acuerdo con la reivindicación 11.

De acuerdo con la invención el dispositivo de prevención de fallos comprende: al menos una unidad de memoria con un conjunto pregrabado de primeros telegramas generados fuera de línea y un conjunto pregrabado de segundos telegramas complementarios generados fuera de línea, en el que una operación XOR en uno de los primeros telegramas y su segundo telegrama complementario da como resultado un telegrama original construido fuera de línea; al menos un procesador de entrada para seleccionar uno de los primeros telegramas almacenados y uno de los segundos telegramas almacenados; un dispositivo XOR con un primer canal de entrada para transmitir el primer telegrama seleccionado, un segundo canal de entrada para transmitir el segundo telegrama seleccionado, y con un canal de salida para transmitir un tercer telegrama, siendo el tercer telegrama el resultado de una operación XOR del primer y el segundo telegramas; y un subsistema de recepción para recibir el tercer telegrama.

En contraste a sistemas de prevención de fallos compuestos conocidos a partir del estado de la técnica el sistema inventivo muestra una arquitectura simplificada. En particular han de proporcionarse menos componentes electrónicos, reduciendo de esta manera el riesgo de fallos.

El conjunto de primeros telegramas comprende n primeros telegramas, con $n \geq 1$. El conjunto de segundos telegramas comprende m segundos telegramas, con $m \geq 1$; preferentemente $m = n$. Cada segundo telegrama complementa al menos uno de los primeros telegramas. El primer y su segundo telegrama complementario están construidos a partir de un telegrama original y se almacenan en la unidad o unidades de memoria. El telegrama original que debería transmitirse de una manera segura de acuerdo con la invención comprende una secuencia de bits. Mediante la operación XOR inversa para cada telegrama original se genera un primer telegrama y un segundo telegrama, que dan como resultado un tercer telegrama que coincide con el telegrama original cuando se realiza una operación XOR con el primer y el segundo telegramas. Es decir realizando la operación XOR en un primer telegrama y su segundo telegrama complementario, se genera un tercer telegrama (el tercer telegrama es el resultado de la operación XOR) que se ajusta al telegrama original (válido). En caso de fallo (por ejemplo, se realiza una operación XOR en un primer telegrama y en un segundo telegrama no complementario) se genera un tercer telegrama que no se ajusta al telegrama original (inválido). El tercer telegrama se transmite desde el sistema de prevención de fallos a unos sistemas de recepción de seguridad crítica, por ejemplo, una lámpara de señal, tren, avión, etc.

Cada canal comprende un controlador de transmisión de 1 bit de ancho y memoria intermedia de largo del telegrama para transmitir los telegramas a o desde el dispositivo el dispositivo XOR. Para conseguir una operación XOR correcta (=operación lógica que emite verdadero cada vez que ambas entradas se diferencian), el primer, el segundo y el tercer telegramas deben tener el mismo número de bits.

El primer canal de entrada y el segundo canal de entrada están preferentemente sincronizados, en particular mediante sincronización de trama, es decir se alimenta una señal de sincronización desde el primer canal de entrada al segundo canal de entrada.

Aunque se prefieren dos canales de entrada es posible también proporcionar más de dos canales.

En una realización preferida se proporcionan dos procesadores de entrada. Un procesador de entrada (primer procesador de entrada) está dispuesto en el primer canal de entrada. El otro procesador de entrada (segundo procesador de entrada) está dispuesto el segundo canal de entrada.

Preferentemente uno de los procesadores de entrada selecciona uno de los primeros telegramas y el otro procesador de entrada selecciona uno de los segundos telegramas. En este caso el primer y el segundo telegramas se seleccionan independientemente entre sí. Por lo tanto el riesgo de producir un telegrama fallido en la salida del sistema se reduce enormemente.

Como alternativa el procesador de entrada es un procesador de entrada común, que selecciona un primer telegrama así como un segundo telegrama. Únicamente se requiere un procesador de entrada; se requiere aún una normalización alta del procesador de entrada. De otra manera esta realización difícilmente puede usarse para sistemas de alto nivel de seguridad.

Por razones de seguridad se prefiere proporcionar una primera unidad de memoria para almacenar el conjunto de primeros telegramas, y una segunda unidad de memoria para almacenar el conjunto de segundos telegramas.

En una realización especial se proporcionan dos unidades de entrada, proporcionando cada unidad de entrada una primera entrada (primera información de entrada) al primer canal de entrada y segunda entrada (segunda información de entrada) al segundo canal de entrada. Cada unidad de entrada está conectada al primer así como al segundo canal de entrada. Por lo tanto el primer canal de entrada se proporciona con dos primeras entradas y el segundo canal de entrada se proporciona con dos segundas entradas. Una comparación de las dobles primeras entradas seleccionadas y las dobles segundas entradas seleccionadas reduce respectivamente el riesgo de falsa evaluación de entrada.

Para comprobar, si el tercer telegrama es válido o no, se lleva a cabo un proceso de control. El proceso de control, que determina si el tercer telegrama es válido o no, se realiza en general en un subsistema de recepción, por ejemplo en un tren. Adicionalmente o como alternativa el sistema de prevención de fallos inventivo puede comprender un dispositivo de control para controlar si el tercer telegrama es válido o no. Por lo tanto, puede visualizarse el fallo directamente en el dispositivo de prevención de fallos. El dispositivo de control está dispuesto aguas abajo del dispositivo XOR. El tercer telegrama es válido si muestra una estructura correcta, es decir la estructura de un telegrama original desde el que se ha generado el primer y un segundo telegrama complementario (véase a continuación "método"). Se consigue la estructura correcta del telegrama original, si se realiza correctamente la operación XOR en el primer y el segundo telegrama complementario. Un tercer telegrama válido contiene un mensaje de datos complejo que se refiere a instrucciones relevantes para la seguridad para que se lleve a cabo una tarea relevante de seguridad en o mediante el sistema de recepción, por ejemplo "cambiar lámpara de señal a verde" "detener el tren" etc., que está también contenida en el telegrama original desde el que se obtienen el primer y el segundo telegramas realizando una operación XOR inversa.

En una realización preferida se proporciona un modulador para convertir el tercer telegrama en un flujo de bits modulado. El modulador (también denominado codificador de línea) convierte el tercer telegrama, por ejemplo desde un código binario a una señal analógica para enviarla al subsistema de recepción.

En una realización ventajosa el modulador comprende una memoria con capacidad menor que el número de bits de uno de los telegramas. Por lo tanto, puede evitarse una repetición inintencionada de un telegrama válido mediante el modulador/codificador de línea.

En una realización preferida se proporciona al menos un dispositivo de supervisión de CRC para controlar la suma de comprobación del tercer telegrama. De esta manera, pueden detectarse fallos dentro de un canal en un punto de tiempo temprano, es decir sin ayuda de un subsistema de recepción. Preferentemente para cada canal de entrada se proporciona un dispositivo de supervisión de CRC.

La invención también se refiere a un método para operar un sistema de prevención de fallos como se ha descrito anteriormente, comprendiendo el método las siguientes etapas:

- construcción fuera de línea de un conjunto de telegramas originales;
- generación fuera de línea de un conjunto de primeros telegramas y un conjunto de segundos telegramas complementarios, de manera que una operación XOR en uno de los primeros telegramas y su segundo telegrama complementario da como resultado uno de los telegramas originales;
- almacenar los conjuntos de primeros telegramas y segundos telegramas complementarios en al menos una unidad de memoria del sistema de prevención de fallos;
- selección de uno de los primeros telegramas y uno de los segundos telegramas mediante un procesador de entrada en dependencia de información de entrada;
- entrada del primer telegrama seleccionado en un primer canal de entrada de un dispositivo XOR;
- entrada del segundo telegrama seleccionado en un segundo canal de entrada del dispositivo XOR;
- realización de una operación XOR en el primer telegrama y el segundo telegrama dando como resultado un tercer telegrama;
- salida del tercer telegrama en el canal de salida del dispositivo XOR;
- comprobar, si el tercer telegrama es válido.

Para cada telegrama original se genera un par de telegramas complementarios, consistiendo cada par de telegramas en un primer telegrama y un segundo telegrama complementario. Cada primer telegrama y su segundo telegrama complementario se generan de manera que una operación XOR en el primer telegrama y su segundo telegrama complementario da como resultado el telegrama original correspondiente.

Preferentemente se generan varios (n) telegramas originales. El número de primeros telegramas corresponde con el número de telegramas originales (con $n \geq 1$, preferentemente $n \geq 2$). El número de segundos telegramas (m) puede diferenciarse del número de primeros telegramas, pero es preferentemente el mismo (m=n).

La selección del primer y segundo telegramas se lleva a cabo en dependencia de la información de entrada recibida mediante el procesador de entrada. La información de entrada puede comprender, por ejemplo, información con respecto a la ocupación del raíl, condiciones del tiempo, etc. La información de entrada determina qué telegrama original se ha de transmitir. Los procesadores de entrada seleccionan los correspondientes primeros y segundos telegramas para procesamiento adicional. La selección del primer telegrama y del segundo telegrama puede realizarse mediante dos procesadores de entrada independientes o procesadores de entrada dependientes (por ejemplo con una fuente de alimentación común), dependiendo del nivel de seguridad requerido.

La operación XOR se realiza preferentemente a nivel de bits, es decir se usan dos telegramas (patrones de bits) de igual longitud. La operación XOR se realiza en cada par de bits correspondientes.

La comprobación (proceso de control) de si el tercer telegrama es válido o no se hará mediante el subsistema de recepción y/o mediante un dispositivo interno, tal como un dispositivo de supervisión de CRC. En caso de que el tercer telegrama corresponda con el telegrama original el tercer telegrama es válido y se ejecuta una tarea de acuerdo con el mensaje de datos (por ejemplo se cambia la lámpara de señal a "verde"). En caso de que el tercer telegrama no corresponda con el telegrama original el tercer telegrama es inválido y se lleva a cabo una acción de estado seguro (por ejemplo mantener una lámpara de señal en "rojo" o cambiar una lámpara de señal a "rojo" respectivamente).

En una variante preferida para cada segundo telegrama se proporciona exactamente un primer telegrama complementario y viceversa, es decir para cada primer telegrama se genera un segundo telegrama separado. Por lo tanto cada primer telegrama complementa exactamente un segundo telegrama y viceversa. En este caso preferido el número de primeros telegramas almacenados en la primera unidad de memoria cumple con el número de segundos telegramas almacenados en la segunda unidad de memoria. Puede conseguirse de esta manera un nivel alto de seguridad, puesto que - en caso de que se haya seleccionado incorrectamente un primer telegrama - se proporciona únicamente un fallo del sistema si se selecciona el único segundo telegrama complementario al primer telegrama incorrectamente seleccionado. Esto, sin embargo es bastante improbable, en particular si se proporciona una pluralidad de primeros y segundos telegramas. En una variante alternativa varios primeros telegramas complementan el mismo segundo telegrama. Esta variante puede usarse para niveles de seguridad inferior o requiere un procesador de entrada altamente fiable.

Puesto que el telegrama original se construye fuera de línea la probabilidad de error puede reducirse.

En una variante preferida se lleva a cabo una supervisión de CRC del tercer telegrama mediante dispositivos de supervisión de CRC únicos o duplicados. En caso de dispositivos de supervisión de CRC duplicados se proporciona un dispositivo de supervisión de CRC para cada canal. Pueden extraerse ventajas adicionales a partir de la descripción y los dibujos desvelados. Las características mencionadas anteriormente y a continuación pueden usarse de acuerdo con la invención individual o colectivamente en cualquier realización. Las realizaciones mencionadas no se han de entender como una enumeración exhaustiva sino en su lugar tienen carácter ejemplar para la descripción de la invención.

Breve descripción de los dibujos

La invención se muestra en los dibujos y se explicará en detalle usando realizaciones ejemplares.

La Figura 1A muestra una estructura de prevención de fallos intrínseca de acuerdo con el estado de la técnica.

La Figura 1B muestra una estructura de prevención de fallos compuesta de acuerdo con el estado de la técnica.

La Figura 1C muestra una estructura de prevención de fallos reactiva de acuerdo con el estado de la técnica.

La Figura 2 muestra una estructura de prevención de fallos compuesta 2oo3 de acuerdo con el estado de la técnica.

La Figura 3 muestra una estructura de prevención de fallos compuesta 2 de 2 de acuerdo con el estado de la técnica.

La Figura 4 muestra una vista esquemática de una realización preferida del sistema de prevención de fallos inventivo usando unidades de entrada duplicadas y procesadores de entrada independientes.

La Figura 4 muestra una vista esquemática de otra realización preferida del sistema de prevención de fallos inventivo usando única unidad de entrada y un procesador de entrada común.

La Figura 5 muestra una vista esquemática de otra realización preferida del sistema de prevención de fallos inventivo con control de CRC.

Descripción detallada de la invención y de los dibujos

Las Figuras 2 y 3 muestran diferentes estructuras de canal de una estructura de prevención de fallos compuesta de acuerdo con el estado de la técnica. La estructura de prevención de fallos compuesta comprende diferentes canales C1, C2, C3, una unidad de entrada común IU y varias salidas O1, O2, O3 (una para cada canal). Las salidas O1, O2, O3 de los canales C1, C2, C3, se someten a votación mediante un dispositivo de sondeo V, V'. Se usa el principio de "impedancia de entrada alta" para compartir de manera no intrusiva las entradas, es decir los canales de entrada se desacoplan entre sí proporcionando las resistencias de entrada R.

Una estructura de tres canales de una estructura de prevención de fallos compuesta se muestra en la Figura 2. La salida del dispositivo de sondeo V implementa una función de "mayoría", también denominada 2 de 3 (2oo3). El estado de salida digital de "Bajo" es el estado seguro.

Como otro ejemplo, se muestra una implementación de dos canales en la Figura 3. El dispositivo de sondeo de salida V' implementa una función de "unanimidad", también denominada 2 de 2 (2oo2). Al igual que antes, el estado de salida digital de "Bajo" es el estado seguro.

Suponiendo por motivos del principio de que el dispositivo de sondeo está en su propio estado de prevención de fallos, puede observarse en ambos ejemplos que incluso en fallo, un canal no puede accionar la salida en estado "Alto" únicamente por sí mismo, sino siempre en conjunto con al menos otro canal.

Los dispositivos de prevención de fallos compuestos mostrados en las figuras 2 y 3 no son adecuados para subsistemas que emiten mensajes de datos complejos (telegramas).

La Figura 4a muestra un sistema de prevención de fallos inventivo que comprende un primer canal de entrada A con un primer procesador de entrada 1a y un segundo canal de entrada B con un segundo procesador de entrada 1b, siendo los canales de entrada A, B funcionalmente idénticos. Los procesadores de entrada 1a, 1b están conectados cada uno a las unidades de entrada 2, 2', proporcionando cada unidad de entrada 2, 2' una primera entrada 3a, 3a' (primera información de entrada) al primer canal de entrada A y una segunda entrada 3b, 3b' (segunda información de entrada) al segundo canal de entrada B. Las entradas de sistema 3a, 3a', 3b, 3b' están distribuidas de manera no intrusiva a ambos canales A, B, mediante el principio de alta impedancia o mediante sensores duplicados o combinación de ambos.

Los procesadores de entrada 1a, 1b analizan y evalúan el estado de las entradas 3a, 3a', 3b, 3b'. Las funciones tales como el filtrado de señal, supresión de rebotes, detección de umbral y/o histéresis se implementan a menudo también en este bloque funcional, dependiendo de la aplicación particular. Dado el hecho de que el número de entradas está limitado, resulta que el número de estados de la entrada está también limitado. Si por ejemplo todas las entradas son de naturaleza binaria y un sistema tuviera N entradas, no son posibles más de dos elevado la potencia de N ($2^N$) estados de entrada. Además, considerando que un estado de entrada particular está asignado con un primer y un segundo telegrama (que realmente describe el estado de las entradas al sistema de recepción), es práctico generar todos los telegramas fuera de la máquina, uno para cada estado de entrada, y pregrabarlos en las unidades de memoria 4a, 4b.

Los procesadores de entrada 1a, 1b seleccionan cada uno una de las entradas 3a, 3a', 3b, 3b' para su canal correspondiente A, B, en el cual el procesador de entrada 1a del primer canal de entrada A selecciona una de las primeras entradas, mientras que el segundo procesador de entrada 1b selecciona una de las segundas entradas. De acuerdo con las entradas seleccionadas el primer procesador de entrada 1a selecciona un primer telegrama desde la primera unidad de memoria 4a y el segundo procesador de entrada 1 b selecciona un segundo telegrama desde la segunda unidad de memoria 4b, es decir los procesadores de entrada seleccionan los telegramas pregrabados complementarios que describen el estado de entrada. En una implementación preferida, una buena descripción del mecanismo es que la unidad de memoria comprende o tiene acceso a una tabla de correspondencia que tiene las entradas establecidas como direcciones en la tabla de correspondencia. Una combinación de ajuste de entrada seleccionará un único telegrama desde la tabla de correspondencia. Esto se aplica para ambos canales. Pueden proporcionarse tablas de correspondencia separadas para los diferentes canales.

Por lo tanto una vez que se evalúan las entradas (filtradas y validadas como estables) se seleccionará un telegrama desde la unidad de memoria 4a, 4b y se transferirá a un controlador de transmisión 8a, 8b. En el arranque o tras recibir un nuevo telegrama desde los procesadores de entrada 1a, 1b, un controlador de transmisión 8a se sincroniza a sí mismo con el otro controlador de transmisión 8b para alienar la trama de transmisión (coincidir la trama de tiempo).

La salida del sistema consiste en un telegrama (tercer telegrama) que refleja el estado de entrada procesado por ambos canales A, B, de acuerdo con la función de transferencia de sistema y con acuerdo de ambos canales A, B

(principio de 2 de 2). Para conseguir esto, el primer telegrama seleccionado y el segundo telegrama seleccionado se transmiten mediante los controladores de transmisión 8a, 8b a un dispositivo XOR 5. El dispositivo XOR realiza una operación XOR con el primer telegrama seleccionado y el segundo telegrama seleccionado dando como resultado el tercer telegrama que se emite a través de un canal de salida. Un modulador 6 modula el tercer telegrama en un flujo de bits modulado para enviarlo a un subsistema de recepción 7, por ejemplo un tren o una señal de tráfico. Una unidad de control (no mostrada) del sistema de prevención de fallos y/o de la unidad de recepción comprueba si el tercer telegrama es válido o no.

En la realización preferida de esta invención y por simplicidad de exposición de principios, se usará la siguiente suposición: dado un número limitado de los estados distintivos de entrada, y dada una función de transferencia determinística del sistema, dará como resultado un número práctico de telegramas de salida. Por lo tanto todos los telegramas dependientes de la entrada posibles se componen fuera de línea y se almacenan a continuación en el sistema unidad de memorias 4a, 4b. Como alternativa, la generación de los telegramas podría hacerse en tiempo real mediante dos procesadores independientes de acuerdo con reglas predefinidas.

Además, pueden construirse también telegramas complementarios, relacionados o no relacionados con el estado de entrada pero relacionados con estados esperados y no esperados del sistema. Después de la composición fuera de línea, se prefiere modificar los telegramas originales bit a bit y a continuación almacenar los telegramas modificados (primeros y segundos telegramas) en cada unidad de memoria del canal 4a, 4b.

El algoritmo de modificación se ha de idear de tal manera que la re-composición del telegrama mediante la operación XOR a nivel de bit dará como resultado el telegrama correcto (telegrama original). Preferentemente, el algoritmo de modificación se idea de tal manera que trata el mecanismo de protección de datos implementado mediante las contramedidas presentadas anteriormente.

Por ejemplo los siguientes algoritmos son adecuados para la realización preferida de la invención.

Un enfoque sistemático:
- El primer telegrama se genera de acuerdo con especificaciones definidas.
- El segundo telegrama se "deduce" desde el canal A de tal manera que la operación XOR dará como resultado el telegrama original correcto.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Telegrama original | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| primer telegrama | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| segundo telegrama | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| | | | | | | | A XOR B a nivel de bit | | | | | | |
| tercer telegrama después de operación XOR | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |

Un enfoque estocástico:

- El primer telegrama del canal A se genera aleatoriamente.

- El segundo telegrama del canal B se "deduce" desde el canal A de tal manera que la operación XOR dará como resultado el telegrama correcto.

Otro enfoque:

- Un mecanismo de modificación se aplica en la cabida útil del telegrama.
- Un mecanismo de modificación diferente se aplica al campo de CRC del telegrama.

Lo siguiente se aplica para todos los algoritmos usados con la presente invención:

- Cualquier telegrama modificado debe fallar la comprobación de paridad general.

- Cualquier telegrama modificado puede mostrar un número suficiente (es decir suficiente para detectar un fallo con una probabilidad dada) de violaciones de reglas de composición internas, tales como violación de alfabeto, fallo de comprobación de paridad parcial, etc.

- Un telegrama de canal cualquiera al que se ha realizado la operación XOR con el canal adyacente a cualquier otro telegrama debe dar como resultado un telegrama inválido con la excepción del telegrama de par pretendido.

Durante la sincronización, todos los bits cero, uno o la señal de silencio se han de transmitir en una interfaz de línea, según se requiera o acepte mediante el protocolo de aplicación. Una vez que se consigue sincronización, ambos canales A, B deben permanecer en sincronización de trama observándose el uno al otro y usando temporización de bits común desde el modulador/codificador de transmisión 6. Hay dos memorias intermedias de 1 bit de ancho de

largo de longitud de telegrama en el controlador de transmisión 8a, 8b de cada canal A, B.

Una posible y preferida implementación de la generación de telegrama se describe a continuación: hay dos memorias intermedias de datos de longitud de un telegrama en el controlador de transmisión 8a, 8b. La memoria intermedia que mantiene el telegrama a transmitir se denomina "actual", la segunda memoria intermedia se denomina "siguiente". Cualquier nuevo telegrama seleccionado mediante el procesador de entrada 1a, 1b tras un nuevo cambio de estado de entrada se almacena siempre en la "siguiente" memoria intermedia. La memoria intermedia "actual" se mantiene y se usa para transmitir el telegrama actual, seleccionado de acuerdo con el estado de entrada anterior. Basándose en la temporización de bits recibida desde el modulador/codificador de línea 6, los telegramas complementarios almacenados en cada memoria intermedia "actual" de canal se registran en las entradas de puertas XOR. La transmisión de telegrama actual se transmite según se requiera mediante el protocolo de aplicación hasta que se cambie la entrada 3a, 3a', 3b, 3b' o el estado interno y llegue un nuevo telegrama en la "siguiente" memoria. En la llegada de telegrama nuevo, se señaliza al controlador de transmisión 8a, 8b acerca del cambio de estado de entrada/interno, el controlador de transmisión 8a, 8b finaliza el telegrama actual, declara la memoria intermedia "actual" como la "siguiente" (libre para un nuevo telegrama) y la primera "siguiente" ahora se hace la "actual". El proceso anteriormente descrito se repite cada vez que el ajuste de entrada cambia de un estado a otro.

Además, el proceso para enviar un nuevo telegrama puede accionarse mediante un cambio en el estado interno del sistema, tal como la aparición de una excepción o un error.

Para fines de prueba, el proceso puede accionarse intencionadamente mediante un mecanismo complementario interno incluso cuando no se ha detectado cambio en las entradas o en el estado de sistema interno.

A continuación se describen algunos modos de fallo del sistema de prevención de fallos de acuerdo con la presente invención, usando de esta manera las siguientes definiciones:

Un "telegrama erróneo interpretable como correcto" es un telegrama con una estructura interna correcta, con una CRC válida pero por azar no está en correspondencia con el estado de la entrada. Además, el telegrama lleva un mensaje "permisivo" cuando la entrada está en estado "restrictivo". Este tipo de telegrama se denominará como "inseguro".

Un telegrama "inválido" es un telegrama que debido a fallo, ruido o distorsión intencionada tiene una estructura incorrecta y/o la CRC no se verifica. Se espera con un alto grado de certeza que debido a la CRC incorrecta y/o debido a la modificación estructural interna, tal telegrama se rechazará mediante el subsistema de recepción.

- Fallo: la función XOR permite que pase únicamente un telegrama de canal.
  Mitigación: el tercer telegrama enviado es "un telegrama de canal", que es inválido por definición.
- Fallo: una entrada de función XOR se queda atrapada en "uno"/"cero".
  Mitigación: se envía un tercer telegrama inválido (telegrama de un canal invertido/no-invertido).
- Fallo: uno de los canales de entrada A, B no evalúa el estado de entrada correctamente (selección de entrada errónea).
  Mitigación: La operación XOR compondrá dos telegramas no complementarios; el resultado será un tercer telegrama inválido.
- Fallo: el modulador/codificador de línea 6 repite un telegrama válido, independientemente del estado de la entrada.
  Mitigaciones: el modulador/codificador de línea 6 es un circuito de memoria limitada que no puede mantener un telegrama completo.
- Fallo: ambos canales A, B repiten de manera síncrona el último telegrama válido, independientemente del estado de entrada actual. Esto significa que los fallos en los dos canales A, B con idénticos efectos tendrán que asumirse. La probabilidad para tales fallos es muy baja y para un bajo SIL (Nivel de Integridad de Seguridad), la tasa de fallo es aceptable. Por lo tanto no se requiere cambio en la estructura de sistema para bajo SIL. Sin embargo hay un par de enfoques para mitigar tal fallo:

  Mitigación: ciclos independientes en ambos canales y un reseteo a cero si un ciclo o pulso de reloj se pierde, usando una máquina complementaria tal como un dispositivo de vigilancia.

  Mitigación: la arquitectura presentada mediante esta invención es completamente adecuada para diversidad HW/SW/FW (hardware/software/cableado fijo) que reducirá enormemente la posibilidad de doble fallo similar.

  Mitigación: cuando se permita, pueden insertarse indicaciones de tiempo y números de secuencia en el protocolo de datos.

- Fallo: ambos canales interpretan erróneamente el estado de entrada de la misma manera.
  Mitigación: la arquitectura presentada mediante esta invención es completamente adecuada para diversidad

de HW/SW/FW.

- Fallo: fallo en la cadena analógica.
  Mitigación: el telegrama se distorsiona aleatoriamente o no se transmite en absoluto.

La Figura 4b muestra una realización alternativa usando únicamente un procesador de entrada 1 y una unidad de entrada 2. En este caso el procesador de entrada común 1 selecciona tanto, el primer telegrama para el primer canal A como el segundo telegrama para el segundo canal B. El procesamiento adicional es análogo al de la realización de la Figura 4a. Un procesador de entrada común puede combinarse también con una entrada duplicada (dos unidades de entrada). También, puede usarse una única unidad de entrada con varios procesadores de entrada.

Otra realización preferida de la presente invención se muestra en la Figura 5. La estructura del sistema de prevención de fallos inventivo mostrada en la Figura 5 comprende adicionalmente una función de verificación. La adición de la función de verificación mejora la estructura con la capacidad de detección temprana de fallo dentro de un canal sin ayuda desde el sistema de recepción 7. Por lo tanto el sistema puede experimentar un cierre completo evitando por sí mismo un fallo posterior de la salud del canal dentro del tiempo de reacción de reparación. A pesar de la estructura añadida de verificación, aún se mantiene la clasificación de la estructura presentada mediante esta invención como Prevención de Fallos Compuesta, ya que la verificación no trae de vuelta explícitamente todo el telegrama de salida como en los Sistemas de Prevención de Fallos Reactivos.

Como se presenta en la Figura 5, la estructura añadida comprueba el flujo de datos de salida del dispositivo XOR 5 frente al polinomio de CRC del telegrama, es decir se realiza una CRC (comprobación de redundancia cíclica). Puede requerirse un mecanismo de sincronización representado en la Figura 5 como el "Control de CRC" llevado a cabo mediante un dispositivo de supervisión de CRC 9a, 9b para asegurar funcionalidad apropiada de la máquina de verificación de CRC. Un tercer telegrama correcto producirá una señal de buena comprobación ("CRC OK") en la salida del dispositivo de supervisión de CRC 9a, 9b mostrado en la Figura 5. La señal y su posición relativa en la temporización de sistema se usan a continuación como verificación de la validez del telegrama.

La temporización de señal de verificación y uso detallado son dependientes de la aplicación, sin embargo el principio mostrado en la Figura 5 se mantiene válido para cualquier aplicación de Sistema de Salida de Datos.

Lista de números de referencia

| | |
|---|---|
| 1a, 1b | procesador de entrada |
| 2, 2' | unidades de entrada |
| 3a, 3a' | primera entrada |
| 3b, 3b' | segunda entrada |
| 4a, 4b | unidades de memoria |
| 5 | dispositivo XOR |
| 6 | modulador |
| 7 | subsistema de recepción |
| 8a, 8b | controlador de transmisión |
| 9a, 9b | dispositivo de supervisión de CRC |
| A, B, C1, C2, C3 | canales |
| IU | unidad de entrada |
| O | canal de salida |
| O1, O2, O3 | salidas |
| R | resistencias de entrada |
| V, V' | dispositivo de sondeo |

**REIVINDICACIONES**

1. Sistema de prevención de fallos para un sistema de salida de datos, comprendiendo el dispositivo

- al menos una unidad de memoria (4a, 4b) con un conjunto pregrabado de primeros telegramas generados fuera de línea y un conjunto pregrabado de segundos telegramas complementarios generados fuera de línea, en el que una operación XOR en uno de los primeros telegramas y su segundo telegrama complementario da como resultado un telegrama original construido fuera de línea,
- al menos un procesador de entrada (1, 1a, 1b) para seleccionar en dependencia de información de entrada que describe un estado de entrada del sistema uno de los primeros telegramas almacenados y uno de los segundos telegramas almacenados; y
- un dispositivo XOR (5) con un primer canal de entrada (A) para transmitir el primer telegrama seleccionado, un segundo canal de entrada (B) para transmitir el segundo telegrama seleccionado, y con un canal de salida (O) para transmitir un tercer telegrama, siendo el tercer telegrama el resultado de una operación XOR del primer y segundo telegramas
- un subsistema de recepción para recibir el tercer telegrama.

2. Sistema de prevención de fallos de acuerdo con la reivindicación 1, caracterizado por que se proporcionan dos procesadores de entrada (1a, 1b).

3. Sistema de prevención de fallos de acuerdo con la reivindicación 2, caracterizado por que uno de los procesadores de entrada (1a) selecciona uno de los primeros telegramas y el otro procesador de entrada (1b) selecciona uno de los segundos telegramas.

4. Sistema de prevención de fallos de acuerdo con la reivindicación 1, caracterizado por que el procesador de entrada (1) es un procesador de entrada común, que selecciona un primer telegrama así como un segundo telegrama.

5. Sistema de prevención de fallos de acuerdo con una de las reivindicaciones anteriores, caracterizado por que una primera unidad de memoria (4a) para almacenar el conjunto de primeros telegramas, y una segunda unidad de memoria (4b) para almacenar el conjunto de segundos telegramas.

6. Sistema de prevención de fallos de acuerdo con una de las reivindicaciones anteriores, caracterizado por que se proporcionan dos unidades de entrada (2, 2'), proporcionando cada unidad de entrada (2, 2') una primera entrada al primer canal de entrada (A) y la segunda entrada al segundo canal de entrada (B).

7. Sistema de prevención de fallos de acuerdo con una de las reivindicaciones anteriores, caracterizado por que se proporciona un dispositivo de control para controlar si el tercer telegrama es válido o no.

8. Sistema de prevención de fallos de acuerdo con una de las reivindicaciones anteriores, caracterizado por que se proporciona un modulador (6) para convertir el tercer telegrama en un flujo de bits modulado.

9. Sistema de prevención de fallos de acuerdo con la reivindicación 8, caracterizado por que el modulador (6) comprende una memoria con capacidad menor que el número de bits de uno de los telegramas.

10. Sistema de prevención de fallos de acuerdo con una de las reivindicaciones anteriores, caracterizado por que se proporciona al menos un dispositivo de supervisión de CRC (9a, 9b) para controlar la suma de comprobación del tercer telegrama.

11. Método para operar un sistema de prevención de fallos de acuerdo con una de las reivindicaciones anteriores, comprendiendo el método las siguientes etapas:

- construcción fuera de línea de un conjunto de telegramas originales;
- generación fuera de línea de un conjunto de primeros telegramas y un conjunto de segundos telegramas complementarios, de manera que una operación XOR en uno de los primeros telegramas y su segundo telegrama complementario da como resultado uno de los telegramas originales;
- almacenar los conjuntos de primeros telegramas y segundos telegramas complementarios en al menos una unidad de memoria (4a, 4b) del sistema de prevención de fallos;
- selección mediante un procesador de entrada (1a, 1b) de uno de los primeros telegramas y uno de los segundos telegramas en dependencia de información de entrada que describe un estado de entrada del sistema;
- entrada del primer telegrama seleccionado en un primer canal de entrada (A) de un dispositivo XOR (5);
- entrada del segundo telegrama seleccionado en un segundo canal de entrada (B) del dispositivo XOR (5);
- realización de una operación XOR en el primer telegrama y en el segundo telegrama dando como resultado un tercer telegrama;
- salida del tercer telegrama en el canal de salida (0) del dispositivo XOR (5);
- comprobar, si el tercer telegrama es válido.

12. Método de acuerdo con la reivindicación 11, caracterizado por que para cada segundo telegrama se proporciona exactamente un primer telegrama correspondiente y viceversa.

13. Método de acuerdo con una de las reivindicaciones 11 a 12 caracterizado por que se lleva a cabo una supervisión de CRC del tercer telegrama mediante dispositivos de supervisión de CRC únicos o duplicados (9a, 9b).

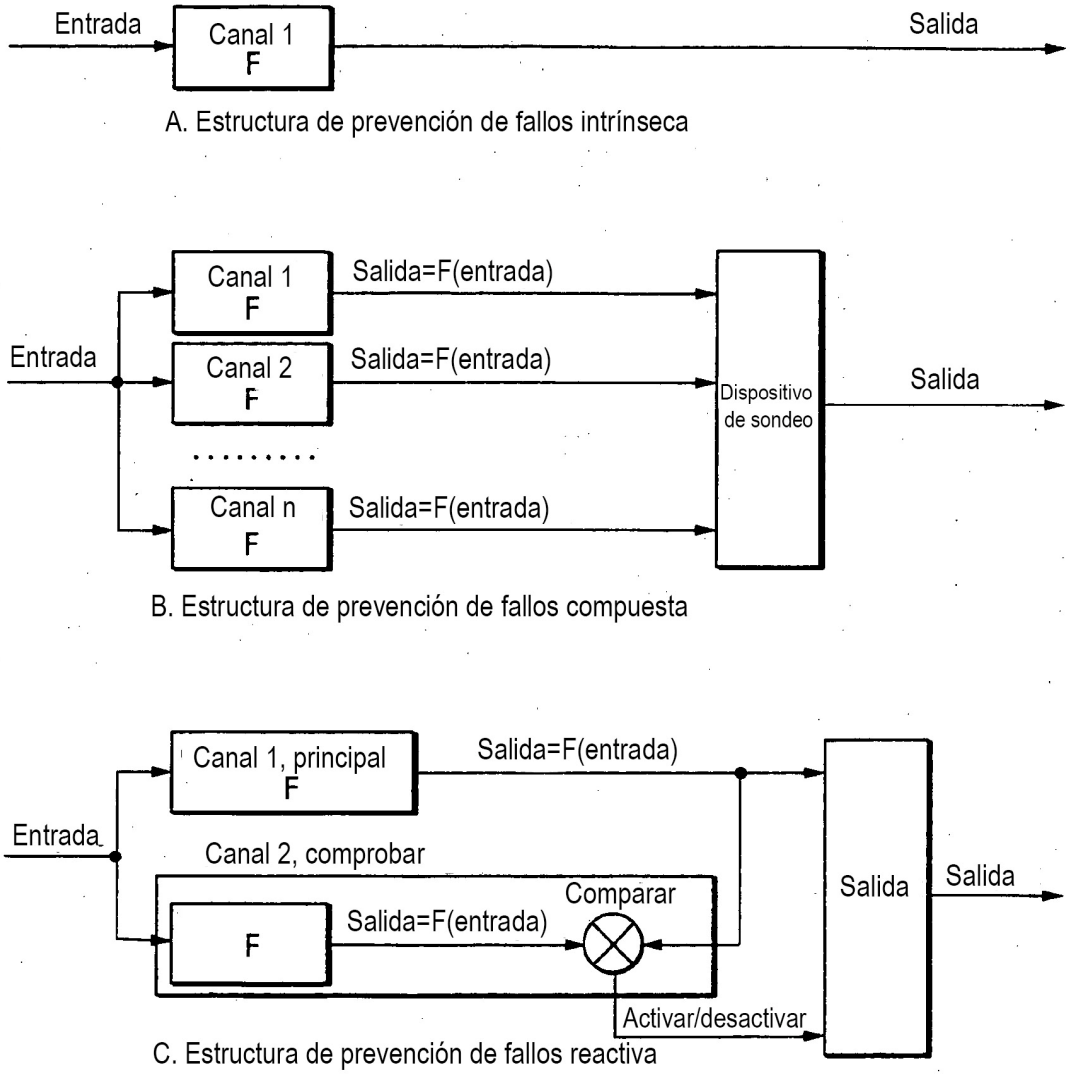
Entrada
Canal 1
F
Salida
A. Estructura de prevención de fallos intrínseca
Canal 1
F
Salida=F(entrada)
Entrada
Canal 2
F
Salida=F(entrada)
Dispositivo
de sondeo
Salida
Canal n
F
Salida=F(entrada)
B. Estructura de prevención de fallos compuesta
Canal 1, principal
F
Salida=F(entrada)
Entrada
Canal 2, comprobar
Comparar
Salida
Salida
F
Salida=F(entrada)
Activar/desactivar
C. Estructura de prevención de fallos reactiva

Fig. 1

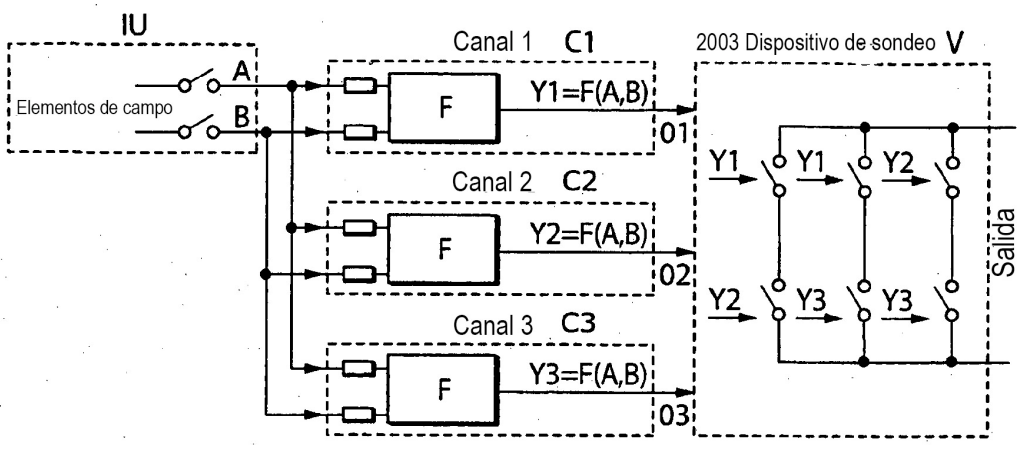
IU
Elementos de campo
A
B
Canal 1 C1
F
Y1=F(A,B)
01
Canal 2 C2
F
Y2=F(A,B)
02
Canal 3 C3
F
Y3=F(A,B)
03
2003 Dispositivo de sondeo V
Y1
Y1
Y2
Y2
Y3
Y3
Salida

Fig. 2

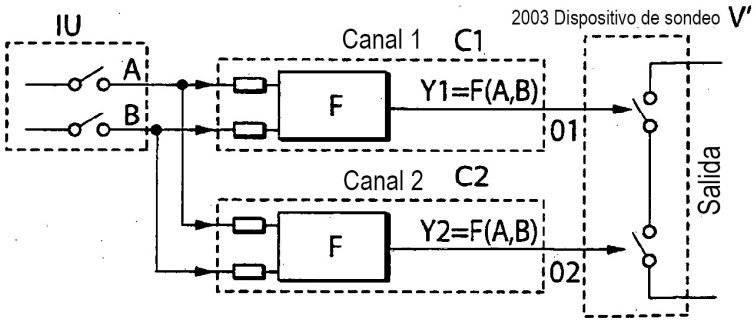
IU
A
B
Canal 1 C1
F
Y1=F(A,B)
01
Canal 2 C2
F
Y2=F(A,B)
02
2003 Dispositivo de sondeo V'
Salida

Fig. 3

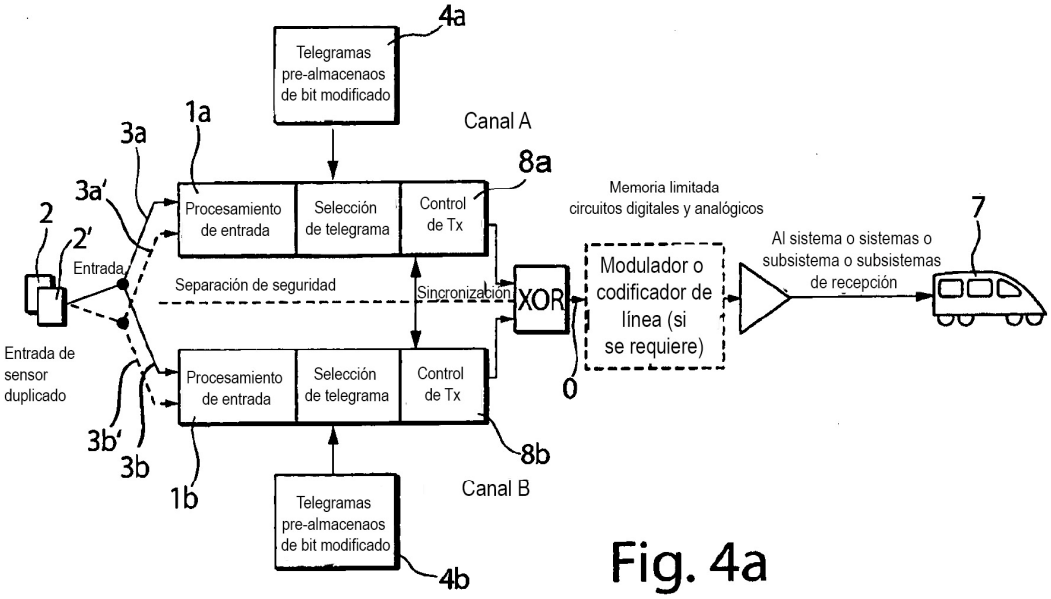
4a
Telegramas pre-almacenaos de bit modificado
Canal A
1a
3a
3a'
8a
Procesamiento de entrada
Selección de telegrama
Control de Tx
Memoria limitada circuitos digitales y analógicos
7
2
2'
Entrada
Separación de seguridad
Sincronización
XOR
Modulador o codificador de línea (si se requiere)
Al sistema o sistemas o subsistema o subsistemas de recepción
Entrada de sensor duplicado
0
3b'
3b
1b
8b
Canal B
Telegramas pre-almacenaos de bit modificado
4b

Fig. 4a

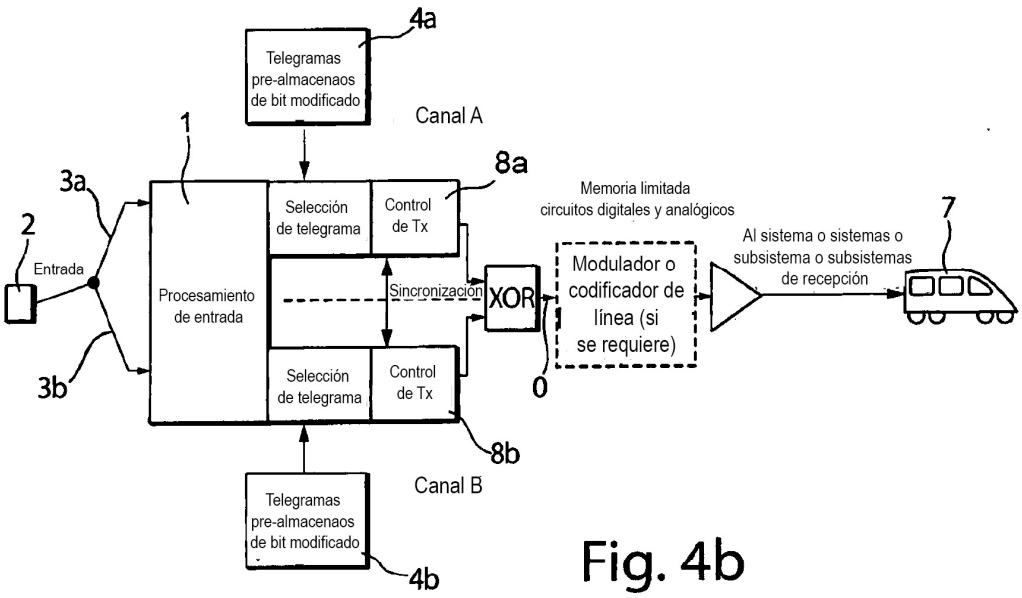
4a
Telegramas pre-almacenaos de bit modificado
Canal A
1
3a
8a
Selección de telegrama
Control de Tx
Memoria limitada circuitos digitales y analógicos
7
2
Entrada
Procesamiento de entrada
Sincronización
XOR
Modulador o codificador de línea (si se requiere)
Al sistema o sistemas o subsistema o subsistemas de recepción
0
3b
8b
Canal B
Telegramas pre-almacenaos de bit modificado
4b

Fig. 4b

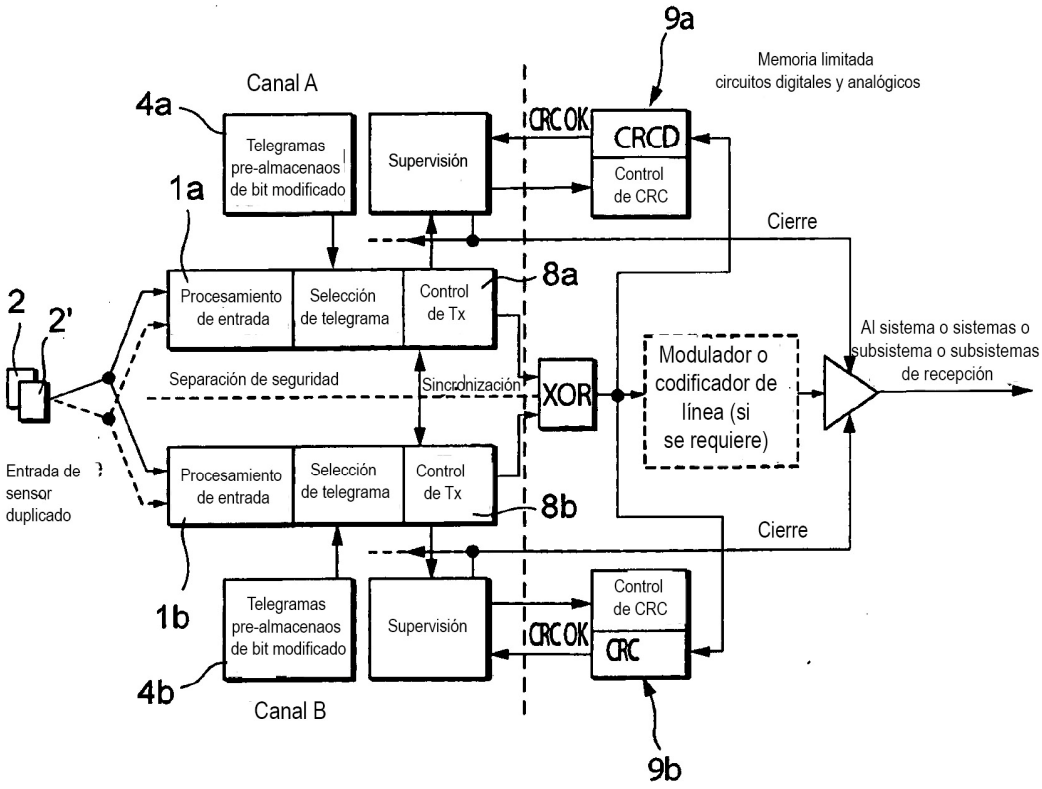
9a
Memoria limitada
circuitos digitales y analógicos
Canal A
4a
Telegramas
pre-almacenaos
de bit modificado
Supervisión
CRC OK
CRCD
Control
de CRC
1a
Cierre
8a
Procesamiento
de entrada
Selección
de telegrama
Control
de Tx
2
2'
Separación de seguridad
Sincronización
XOR
Modulador o
codificador de
línea (si
se requiere)
Al sistema o sistemas o
subsistema o subsistemas
de recepción
Entrada de
sensor
duplicado
Procesamiento
de entrada
Selección
de telegrama
Control
de Tx
8b
Cierre
1b
Telegramas
pre-almacenaos
de bit modificado
Supervisión
Control
de CRC
CRC OK
CRC
4b
Canal B
9b

Fig. 5