(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 585 111**

(51) Int. CI.:

B61L 21/04 (2006.01)
G06F 11/07 (2006.01)
G06F 21/64 (2013.01)
G06F 21/55 (2013.01)
B61L 19/06 (2006.01)
G05B 9/03 (2006.01)
B61L 27/00 (2006.01)
G06F 11/16 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.06.2013 E 13172857 (8)**

(97) Fecha y número de publicación de la concesión europea: **18.05.2016 EP 2677454**

(54) Título: **Calculador, conjunto de comunicación que consta de tal calculador, sistema de gestión ferroviaria que consta de tal conjunto y procedimiento de fiabilidad de datos en un calculador**

(30) Prioridad:

19.06.2012 FR 1255728

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.10.2016

(73) Titular/es:

ALSTOM TRANSPORT TECHNOLOGIES (100.0%)
48 rue Albert Dhalenne
93400 Saint-Ouen, FR

(72) Inventor/es:

GALLOIS, XAVIER y
VIBERT, GUILLAUME

(74) Agente/Representante:

PONTI SALES, Adelaida

DESCRIPCIÓN

Calculador, conjunto de comunicación que consta de tal calculador, sistema de gestión ferroviaria que consta de tal conjunto y procedimiento de fiabilidad de datos en un calculador

[0001] La presente invención se refiere a un procedimiento de fiabilidad de datos en un calculador, siendo el calculador apto para proporcionar un dato de salida a partir de un dato de entrada, y que consta al menos de dos módulos de tratamiento de datos y un órgano de cálculo vinculado a cada módulo de tratamiento, comprendiendo el procedimiento una etapa de cálculo, por cada módulo de tratamiento, de un dato intermedio a partir del dato de entrada, consistiendo dicho cálculo en la aplicación de una función de cálculo al dato de entrada, siendo la función de cálculo idéntica para todos los módulos de tratamiento.

[0002] La presente invención se refiere igualmente a un calculador, apto para proporcionar un dato de salida a partir de un dato de entrada, que consta de:

- al menos dos módulos de tratamiento de datos, constando cada módulo de tratamiento de unos primeros medios de cálculo de un dato intermedio a partir del dato de entrada, siendo dichos primeros medios de cálculo aptos para aplicar una función de cálculo al dato de entrada, siendo la función de cálculo idéntica para todos los módulos de tratamiento,

- un órgano de cálculo vinculado a cada módulo de tratamiento.

[0003] La presente invención se refiere igualmente a un conjunto de comunicación que comprende tal calculador.

[0004] La presente invención se refiere igualmente a un sistema de gestión ferroviaria que comprende tal conjunto de comunicación.

[0005] Se conoce un calculador del tipo precitado. Tal calculador es apto para tratar unos datos y/o unas informaciones que circulan en una red de comunicación y se utiliza generalmente en un sistema de comunicación segura, por ejemplo un sistema de gestión ferroviaria. A fin de garantizar las funciones críticas de seguridad requeridas por el sistema de gestión ferroviaria, la probabilidad de aparición de un dato erróneo y no detectable en salida de tal calculador se debe reducir al máximo. La norma de seguridad ferroviaria europea EN 50 128 establece, por ejemplo, que los equipos relativos a la seguridad de los trenes estén concebidos de manera que su probabilidad de fallo a petición esté comprendida entre 10^{-9} y 10^{-7}. Una técnica conocida para garantizar la seguridad se llama «seguridad compuesta» y consiste en hacer realizar los mismos tratamientos por varios módulos de tratamiento de datos de un mismo calculador, proceder después a un «voto mayoritario». A tal efecto, cada módulo calcula un dato de salida a partir de un mismo dato de entrada. Por otro lado, tal calculador consta generalmente de unos medios de arbitraje aptos para garantizar la función de «voto mayoritario» entre los datos de salida calculados.

[0006] Los medios de arbitraje de tal calculador constan no obstante como mínimo de una capa material, a veces completada por una capa de software. Ahora bien, el fallo de tal capa material puede conllevar un fallo de seguridad que puede conducir a unos incidentes críticos para el sistema de comunicación segura.

[0007] Un objeto de la invención es por tanto proponer un procedimiento de fiabilidad de datos en un calculador que permite liberarse de la utilización de medios materiales dedicados para garantizar la función de voto mayoritario del calculador.

[0008] A tal efecto, la invención tiene como objeto un procedimiento de fiabilidad de datos en un calculador del tipo precitado, caracterizado porque comprende las etapas siguientes:

- el cálculo, por cada módulo de tratamiento, de un código de seguridad intermedio a partir del dato intermedio correspondiente,

- la transmisión al órgano de cálculo, por cada módulo de tratamiento, del código de seguridad intermedio y del dato intermedio,

- el cálculo, por el órgano de cálculo, de un código de seguridad a partir de los códigos de seguridad intermedios,

- la selección, por el órgano de cálculo, de un dato intermedio entre los datos intermedios recibidos, comprendiendo el dato de salida del calculador el dato intermedio seleccionado y

- la transmisión con destino a un dispositivo de recepción, por el órgano de cálculo, del código de seguridad y del dato de salida.

[0009] Según otros aspectos ventajosos de la invención, el procedimiento comprende una o varias de las características siguientes, tomadas aisladamente o según todas las combinaciones técnicamente posibles:

- cada módulo de tratamiento consta de unos primeros medios de memorización de al menos una variable de cifrado y de una función de cifrado, siendo la función de cifrado idéntica para todos los módulos de tratamiento y durante la etapa de cálculo de un código de seguridad intermedio a partir del dato intermedio correspondiente, dicho cálculo consiste en aplicar, por cada módulo de tratamiento, la función de cifrado al menos al dato intermedio y a la variable de cifrado;

- el órgano de cálculo consta de unos segundos medios de memorización de al menos una constante de descifrado y una función de consolidación y durante la etapa de cálculo de un código de seguridad a partir de los códigos de seguridad intermedios, dicho cálculo consiste en aplicar, por el órgano de cálculo, la función de consolidación a cada código de seguridad intermedio recibido y a la constante de descrifrado;

- el procedimiento consta además, entre la etapa de cálculo de un dato intermedio y la etapa de cálculo de un código de seguridad intermedio, de una etapa de transmisión, por cada módulo de tratamiento, del valor de su dato intermedio a los otros módulos de tratamiento y una etapa de prueba, por cada módulo de tratamiento, de la existencia de un valor mayoritario entre el conjunto de los valores de los datos intermedios, siendo el valor mayoritario el valor más frecuente entre los valores de datos intermedios, si este valor existe;

- si la prueba de existencia de un valor mayoritario es negativa durante la etapa de prueba correspondiente, el procedimiento consta de una etapa de supresión por uno de los módulos de tratamiento de su variable de cifrado;

- el procedimiento consta además, antes de la etapa de cálculo de un código de seguridad intermedio, de una etapa de reinicialización, por cada módulo de tratamiento, de su variable de cifrado, siendo efectuada dicha etapa de reinicialización de manera sincronizada entre todos los módulos de tratamiento;

- el dato de salida es el dato intermedio seleccionado por el órgano de cálculo durante la etapa de selección;

- el procedimiento consta además de una etapa de recepción, por el dispositivo de recepción, del código de seguridad y del dato de salida y una etapa de verificación, por el dispositivo de recepción, de la coherencia entre el código de seguridad y el dato de salida.

[0010] La invención tiene igualmente como objeto un calculador del tipo precitado, caracterizado porque los primeros medios de cálculo son aptos además para calcular un código de seguridad intermedio a partir del dato intermedio correspondiente, siendo cada módulo de tratamiento apto para transmitir al órgano de cálculo el código de seguridad intermedio y el dato intermedio correspondiente y porque el órgano de cálculo consta de unos segundos medios de cálculo de un código de seguridad a partir de los códigos de seguridad intermedios, siendo el órgano de cálculo apto para seleccionar un dato intermedio entre los datos intermedios recibidos y para transmitir el código de seguridad y el dato de salida a un dispositivo de recepción, comprendiendo el dato de salida el dato intermedio seleccionado.

[0011] La invención tiene igualmente como objeto un conjunto de comunicación que comprende un calculador y un dispositivo de recepción de datos, siendo el calculador apto para proporcionar un código de seguridad y un dato, constando el dispositivo de recepción de unos medios de memorización de un algoritmo de control, siendo el dispositivo de recepción apto para recibir el código de seguridad y el dato de salida y para verificar, por la aplicación del algoritmo de control, la coherencia entre el código de seguridad y el dato de salida, caracterizado porque el calculador es tal como se ha definido anteriormente.

[0012] La invención tiene igualmente como objeto un sistema de gestión ferroviaria caracterizado porque comprende al menos un conjunto de comunicación tal como se ha definido anteriormente.

[0013] Estas características y ventajas de la invención se mostrarán con la lectura de la descripción que aparece a

continuación, dada únicamente a título de ejemplo no limitativo, y realizada en referencia a los dibujos anexos, en los cuales:

- la figura 1 es una representación esquemática de un sistema de gestión ferroviaria que comprende un calculador según la invención, constando el calculador de dos módulos de tratamiento de datos;

- la figura 2 es una representación esquemática de uno de los módulos de tratamiento de datos del calculador de la figura 1; y

- la figura 3 es un organigrama que representa un procedimiento de fiabilidad de datos según la invención, aplicado por el calculador de la figura 1.

[0014] En la presente descripción, se denominarán «datos de seguridad» a unos datos lógicos o unas informaciones que circulan en una red de comunicación. La red de comunicación es típicamente una red no segura y cada dato de seguridad circula en la red acompañado de un código de seguridad. Un dato de seguridad emitido en la red por un dispositivo de emisión es aceptado por un dispositivo de recepción únicamente si el dispositivo de recepción determina, por medio de un algoritmo de control predeterminado, que el dato de seguridad emitido y el código de seguridad que lo acompaña son coherentes.

[0015] La figura 1 representa un sistema de gestión ferroviaria 1 que comprende un conjunto de comunicación 2. El sistema de gestión ferroviaria 1 está implantado, por ejemplo, en una estación ferroviaria. Es apto por ejemplo para determinar y hacer circular unas órdenes de mando destinadas a trenes o con destino a sistemas de seguridad de vías, tales como unas agujas.

[0016] El conjunto 2 comprende un calculador 6 y un dispositivo 8 de recepción de datos, vinculado al calculador 6 a través de una conexión de datos 10.

[0017] El calculador 6 consta de unos medios 11 de recepción de datos, un primer módulo 12A de tratamiento de datos y un segundo módulo 12B de tratamiento de datos, estando vinculado cada módulo de tratamiento 12A, 12B a los medios de recepción 11. El calculador 6 consta además de un órgano de cálculo 14, vinculado a cada módulo de tratamiento 12A, 12B y unos medios 18 de emisión de datos destinados al dispositivo de recepción 8, estando vinculados dichos medios de emisión 18 al órgano 14.

[0018] El calculador 6 es un calculador de seguridad, fijado de forma estable en el seno del sistema de gestión ferroviaria 1. El calculador 6 es apto para efectuar unos cálculos sobre unos datos de seguridad que circulan en una red de comunicación del sistema de gestión ferroviaria 1. El calculador 6 es apto, más particularmente, para proporcionar al dispositivo de recepción 8 un dato de salida Ds, a partir de un dato de entrada De, procedente de un dispositivo de comunicación, tal como otro calculador. En el ejemplo de realización descrito, los datos de entrada De y de salida Ds son unas variables formadas por una combinación de bits, por ejemplo una combinación de dieciséis bits.

[0019] El dispositivo de recepción 8 consta de una memoria de almacenamiento de un algoritmo de control, no representada. El dispositivo de recepción 8 es por ejemplo un calculador de seguridad. Es apto para recibir un código de seguridad C_S y el dato de salida Ds y para verificar, por la aplicación del algoritmo de control, la coherencia entre el código de seguridad C_S y el dato de salida Ds.

[0020] El enlace de datos 10 es, por ejemplo, un enlace radioeléctrico conforme a la norma IEEE-802-11, generalmente llamado enlace Wi-Fi™.

[0021] Los medios de recepción 11 son aptos para recibir el dato de entrada De y para suministrar este dato de entrada De en entrada de cada módulo de tratamiento 12A, 12B.

[0022] El primer módulo de tratamiento 12A y el segundo módulo de tratamiento 12B presentan cada uno una misma estructura. En lo que sigue, solo se describirá por tanto la estructura del primer módulo de tratamiento 12A.

[0023] Como se ilustra en la figura 2, el primer módulo de tratamiento 12A consta de unos primeros medios de memorización 20A, unos primeros medios de cálculo 22A, vinculados a los medios de memorización 20A, y unos medios de comunicación 24A, vinculados a los primeros medios de cálculo 22A. El primer módulo de tratamiento 12A consta además de unos medios de eliminación 26A, vinculados a los primeros medios de memorización 20A, y unos medios de sincronización 28A, vinculados a los medios de comunicación 24A.

[0024] El primer módulo de tratamiento 12A consta igualmente de unos medios de modificación 30A, vinculados a los primeros medios de memorización 20A y a los medios de sincronización 28A.

[0025] En el ejemplo de realización, los primeros medios de memorización 20A están formados por una memoria flash, conocida en sí. Como variante, los primeros medios de memorización 20A están formados por una memoria no volátil reescribible. Incluso como variante, los primeros medios de memorización 20A están formados por una memoria volátil reescribible.

[0026] Los primeros medios de memorización 20A son aptos para almacenar una variable de cifrado V_{CA}, apta para el primer módulo 12A. En el ejemplo de realización, la variable de cifrado V_{CA} está formada por una combinación de dieciséis bits. los primeros medios de memorización 20A son aptos igualmente para almacenar una función de cálculo σ, una función de cifrado Fc y una función de reinicialización F_{rein}. En el ejemplo de realización, la función de cálculo σ es la función lógica «NO», clásicamente conocida. Por otro lado, la función de cifrado Fc es, en el ejemplo de realización, la función lógica «O exclusiva», clásicamente conocida. La función de reinicialización F_{rein} es igualmente, por ejemplo, la función lógica «O exclusiva».

[0027] En el ejemplo de realización de la figura 2, los primeros medios de cálculo 22A están formados por un procesador de datos, conocido en sí. Los primeros medios de cálculo 22A están vinculados por una parte a los medios de recepción 11 y por otra parte al órgano 14. Los primeros medios de cálculo 22A reciben el dato de entrada $\underline{De}$ y proporcionan en entrada del órgano 14 un dato de salida intermedio D_{IA} y un código de seguridad intermedio C_{SIA}. Los primeros medios de cálculo 22A son aptos para calcular el valor del dato de salida intermedio D_{IA} a partir del valor del dato de entrada $\underline{De}$. El dato D_{IA} se expresa entonces, por ejemplo, del siguiente modo:

$$D_{IA} = \sigma(\underline{De}) \qquad (1)$$

[0028] En el ejemplo de realización, el dato de salida intermedio D_{IA} es una variable formada por una combinación de dieciséis bits.

[0029] Los primeros medios de cálculo 22A son aptos además para calcular el valor del código de seguridad intermedio C_{SIA} a partir del valor del dato de salida intermedio D_{IA} y del valor de la variable de cifrado V_{CA}. El código de seguridad intermedio C_{SIA} se expresa del siguiente modo:

$$C_{SIA} = Fc(F_1(D_{IA}, M_A), V_{CA}) \qquad (2)$$

[0030] F_1, respectivamente M_A, son una función, respectivamente una constante, almacenadas en los primeros medios de memorización 20A. F_1 es por ejemplo la función lógica «Y». En el ejemplo de realización, M_A es una constante formada por una combinación de dieciséis bits. M_A está formada por ejemplo por una combinación de ocho primeros bits cuyo valor es igual a uno y de ocho últimos bits cuyo valor es igual a cero.

[0031] Los primeros medios de cálculo 22A son aptos además para probar la existencia de un valor mayoritario entre varios valores de datos de salida intermedios, siendo el valor mayoritario el valor más frecuente entre los valores de datos de salida intermedios, si este valor existe.

[0032] Los medios de comunicación 24A constan de unos medios de emisión 31 A y unos medios de recepción 32A. Los medios de emisión 31A son aptos para estar vinculados a los medios de recepción 32B del segundo módulo 12B a través de un enlace de datos 34. Los medios de recepción 32A son aptos para estar vinculados a los medios de emisión 31 B del segundo módulo 12B a través del enlace de datos 35.

[0033] Los enlaces de datos 34, 35 son, por ejemplo, unos enlaces radioeléctricos conformes a la norma IEEE-802-11, generalmente llamados enlaces Wi-Fi™.

[0034] Los medios de eliminación 26A están formados por ejemplo por un procesador de datos. Son aptos para eliminar el valor corriente de la variable de cifrado V_{CA} almacenada en el seno de la memoria 20A.

[0035] Los medios de sincronización 28A constan por ejemplo de un reloj apto para suministrar unas señales a impulsos a unos instantes $\underline{i}$ regulares. Los medios de sincronización 28A son aptos para enviar unas señales de sincronización destinadas a unos medios de comunicación 24A y unos medios de modificación 30A. Los medios de

sincronización 28A son aptos además para sincronizarse con los medios de sincronización 28B del segundo módulo de tratamiento 12B, a través de las señales de sincronización transmitidas por los medios de comunicación 24A.

[0036] Los medios de modificación 30A constan por ejemplo de un generador 38A de secuencias pseudo-aleatorias y un procesador 40A. El generador 38A de secuencias pseudo-aleatorias está vinculado a los medios de sincronización 28A y al procesador 40A. El generador 38A es apto para suministrar al procesador 40A una señal pseudo-aleatoria S_{pa}, después de la recepción de una señal de sincronización suministrada por los medios de sincronización 28A. Más precisamente, en cada instante i, el generador 38A es apto para suministrar al procesador 40A una señal pseudo-aleatoria $S_{pa}(i)$.

[0037] El procesador 40A está vinculado además a los primeros medios de memorización 20A y a los medios de sincronización 28A. El procesador 40A es apto, después de la recepción de una señal de sincronización suministrada por los medios de sincronización 28A, de modificar el valor corriente de la variable de cifrado V_{CA} almacenada en el seno de los primeros medios de memorización 20A. Más precisamente, en cada instante i el procesador 40A es apto para determinar el valor corriente V_{CA} (i) de la variable de cifrado V_{CA}, a partir especialmente del valor anterior V_{CA} (i-1) de la variable de cifrado V_{CA}. El valor corriente en el instante i de la variable de cifrado V_{CA} se expresa del siguiente modo:

$$V_{CA}(i) = F_{réin}\,[S_{pa}(i), V_{CA}(i-1)] \qquad (3)$$

[0038] Los medios de modificación 30A son aptos así para modificar el valor corriente de la variable de cifrado V_{CA} almacenada en el seno de los primeros medios de memorización 20A.

[0039] El primer módulo de tratamiento 12A es apto así para calcular y para suministrar en entrada del órgano 14 el dato de salida intermedio D_{IA} y el código de seguridad intermedio C_{SIA}.

[0040] Los primeros medios de memorización 20B del segundo módulo de tratamiento 12B son aptos para almacenar una variable de cifrado V_{CB}, apta para el módulo 12B, y una función de cálculo σ, idéntica a la función de cálculo σ del primer módulo de tratamiento 12A. En el ejemplo de realización, la variable de cifrado V_{CB} está formada por una combinación de dieciséis bits. Los primeros medios de memorización 20B son aptos igualmente para almacenar una función de cifrado Fc, idéntica a la función de cifrado Fc del primer módulo de tratamiento 12A, y una función de reinicialización F_{rein}, idéntica a la función de reinicialización F_{rein} del primer módulo de tratamiento 12A.

[0041] Los medios de modificación 30B del segundo módulo de tratamiento 12B son aptos para modificar el valor corriente de la variable de cifrado V_{CB} almacenada en el seno de los primeros medios de memorización 20B. El valor corriente en el instante i de la variable de cifrado V_{CB} se expresa del siguiente modo:

$$V_{CB}(i) = F_{réin}\,[S_{pa}(i), V_{CB}(i-1)] \qquad (4)$$

[0042] El segundo módulo de tratamiento 12B es apto así para calcular y para suministrar, en entrada del órgano de cálculo 14, un dato de salida intermedio D_{IB} y un código de seguridad intermedio C_{SIB}. El dato de salida intermedio D_{IB} y el código de seguridad intermedio C_{SIB} se expresan del siguiente modo:

$$D_{IB} = \sigma(\underline{De}) \qquad (5)$$

$$C_{SIB} = Fc\,(F_1(D_{IB}, M_B), V_{CB}) \qquad (6)$$

[0043] F_1, respectivamente M_B, son una función, respectivamente una constante, almacenadas en los primeros medios de memorización 20B. La función F_1 es idéntica a la función F_1 del primer módulo de tratamiento 12A. En el ejemplo de realización, M_B es una constante formada por una combinación de dieciséis bits. M_B está formada por ejemplo por una combinación de ocho primeros bits cuyo valor es igual a cero y de ocho últimos bits cuyo valor es igual a uno.

[0044] En el ejemplo de realización descrito, el dato de salida intermedio D_{IB} es una variable formada por una combinación de dieciséis bits.

[0045] En cada instante i, los valores de las variables de cifrado V_{CA}, respectivamente V_{CB} del módulo de tratamiento 12A, respectivamente 12B, verifican entre ellas una misma relación matemática, por ejemplo la relación matemática siguiente:

$$F_2 [V_{CA}(i), V_{CB}(i)] = K \qquad (7),$$

donde F_2 es por ejemplo la función lógica «O exclusiva» y K es una constante. En el ejemplo de realización, K es una constante formada por una combinación de dieciséis bits.

[0046] Los módulos de tratamiento 12A, 12B son aptos para intercambiarse unos datos según un protocolo de comunicación sincronizado, a través de sus medios de comunicación y sus medios de sincronización respectivos.

[0047] El órgano de cálculo 14 suministra en entrada unos medios de emisión 18 el dato de salida Ds así como el código de seguridad C_S. El órgano 14 consta de unos segundos medios de memorización 42 y unos segundos medios de cálculo 44, vinculados a los segundos medios de memorización 42.

[0048] Los segundos medios de memorización 42 están formados, por ejemplo, por una memoria flash. Los segundos medios de memorización 42 son aptos para almacenar una constante de descifrado K_D y una función de consolidación F_{conso}. En el ejemplo de realización, la función de consolidación F_{conso} es la función lógica «O exclusiva» y la constante de descifrado K_D es una constante formada por una combinación de dieciséis bits.

[0049] En el ejemplo de realización descrito, los segundos medios de cálculo 44 están formados por un procesador de datos. Los segundos medios de cálculo 44 están vinculados por una parte a cada uno de los primeros medios de cálculo 22A, 22B y por otra parte a los medios de emisión 18. Los segundos medios de cálculo 44 proporcionan en entrada unos medios de emisión 18 el dato de salida Ds y el código de seguridad C_S. Los segundos medios de cálculo 44 son aptos para calcular el valor del dato de salida Ds a partir del valor de los datos de salida intermedios D_{IA}, D_{IB}. El valor del dato de salida Ds se toma, en el ejemplo de realización, como igual al valor del dato de salida intermedio D_{IA}. Como variante, el valor del dato de salida Ds se toma como igual al valor del dato de salida intermedio D_{IB}.

[0050] Los segundos medios de cálculo 44 son aptos además para calcular el valor del código de seguridad C_S a partir del valor de cada código de seguridad intermedio C_{SIA}, C_{SIB} y del valor de la constante de descifrado K_D. El código de seguridad C_S se expresa por ejemplo del siguiente modo:

$$C_S = F_{conso}(C_{SIA}, C_{SIB}, K_D) \qquad (8)$$

[0051] Los medios de emisión 18 son aptos para transmitir el dato de salida Ds y el código de seguridad CS al dispositivo de recepción 8.

[0052] En la figura 3 se representan las etapas de un procedimiento de fiabilidad de datos aplicado por el calculador 6, en un modo de realización de la invención.

[0053] En el curso de la descripción, se considera que la probabilidad de aparición de un fallo simultáneo en los módulos de tratamiento 12A, 12B es nula.

[0054] Se supone además que en el instante presente i-L, los primeros medios de memorización 20A, respectivamente 20B almacenan un valor corriente $V_{CA}(i-1)$, respectivamente $V_{CB}(i-1)$ de la variable de cifrado V_{CA}, respectivamente V_{CB}.

[0055] Durante una etapa 60 inicial, los medios de recepción 11 reciben un mensaje que consta del dato de entrada De.

[0056] En el transcurso de una etapa 62 siguiente, los medios de recepción 11 proporcionan el dato de entrada De a cada uno de los primeros medios de cálculo 22A, 22B.

[0057] En el transcurso de una etapa 64 siguiente, los primeros medios de cálculo 22A, respectivamente 22B,

calculan el valor corriente del dato de salida intermedio D_{IA}, respectivamente D_{IB} a partir del valor corriente del dato de entrada De. La expresión del dato de salida intermedio D_{IA}, respectivamente D_{IB} se da por la fórmula (1), respectivamente la fórmula (5).

[0058] Como complemento, en el transcurso de una etapa 66 siguiente, los primeros medios de cálculo 22A, respectivamente 22B, transmiten el valor corriente del dato de salida intermedio D_{IA}, respectivamente D_{IB}, a los medios de emisión 31A, respectivamente 31 B. Los medios de emisión 31A, respectivamente 31B, transmiten entonces el valor corriente del dato de salida intermedio D_{IA}, respectivamente D_{IB} a los medios de recepción 32B, respectivamente 32A, a través del enlace de datos 34, respectivamente 35. Los medios de recepción 32B, respectivamente 32A, transmiten el valor corriente del dato de salida intermedio D_{IA}, respectivamente D_{IB} a los primeros medios de cálculo 22B, respectivamente 22A.

[0059] Como complemento, durante una etapa 68 siguiente, cada uno de los primeros medios de cálculo 22A, 22B determina si existe un valor mayoritario entre los valores corrientes de los datos de salida intermedios D_{IA}, D_{IB}.

[0060] Si después de la etapa 68, cada uno de los primeros medios de cálculo 22A, 22B determina que no existe valor mayoritario entre los valores corrientes de los datos de salida intermedios D_{IA}, D_{IB}, los medios de eliminación 26A eliminan el valor corriente de la variable de cifrado V_{CA} en los primeros medios de memorización 20A en el transcurso de una etapa 70. Como variante, los medios de eliminación 26B eliminan el valor corriente de la variable de cifrado V_{CB} en los primeros medios de memorización 20B durante la etapa 70. Como complemento, una etapa 72 siguiente es aplicada entonces por los procesadores 40A, 40B, como se describe posteriormente.

[0061] Si después de la etapa 68, cada uno de los primeros medios de cálculo 22A, 22B determina que existe un valor mayoritario entre los valores corrientes de los datos de salida intermedios D_{IA}, D_{IB}, la etapa 72 se efectúa.

[0062] La etapa 72 se origina en el instante i inmediatamente después del final de la etapa 68 o de la etapa 70. En el instante i, los valores corrientes $V_{CA}(i-1)$, $V_{CB}(i-1)$ de las variables de cifrado V_{CA}, V_{CB} se convierten en unos valores anteriores. En este mismo instante i, el procesador 40A, respectivamente 40B, determina el valor corriente $V_{CA}(i)$, respectivamente $V_{CB}(i)$ de la variable de cifrado V_{CA}, respectivamente V_{CB} a partir del valor anterior $V_{CA}(i-1)$, respectivamente $V_{CB}(i-1)$ de dicha variable de cifrado. La etapa 72 se efectúa así de manera sincronizada entre los módulos de tratamiento 12A, 12B. La expresión del valor corriente de la variable de cifrado V_{CA}, respectivamente V_{CB} en el instante i es dada por la fórmula (3), respectivamente la fórmula (4).

[0063] En el transcurso de una etapa 74 siguiente, el procesador 22A, respectivamente 22B, calcula el valor corriente del código de seguridad intermedio C_{SIA}, respectivamente C_{SIB}, a partir del valor corriente del dato de salida intermedio D_{IA}, respectivamente D_{IB}, y del valor corriente de la variable de cifrado V_{CA}, respectivamente V_{CB}. La expresión del código de seguridad intermedio C_{SIA}, respectivamente C_{SIB}, es dada por la fórmula (2), respectivamente la fórmula (6).

[0064] En el transcurso de una etapa 76 siguiente, los primeros medios de cálculo 22A, respectivamente 22B, transmiten el dato de salida intermedio D_{IA}, respectivamente D_{IB} y el código de seguridad intermedio C_{SIA}, respectivamente C_{SIB} a los segundos medios de cálculo 44.

[0065] En el transcurso de una etapa 78 siguiente, los segundos medios de cálculo 44 calculan el valor corriente del código de seguridad C_S a partir del valor corriente de cada código de seguridad intermedio C_{SIA}, C_{SIB} y del valor de la constante de descifrado K_D. La expresión del código de seguridad C_S es dada por la fórmula (8).

[0066] En el transcurso de una etapa 80 siguiente, los segundos medios de cálculo 44 seleccionan un valor entre los valores de los datos de salida intermedios D_{IA}, D_{IB}. El valor seleccionado es por ejemplo el valor corriente del dato de salida intermedio D_{IA}. El valor corriente del dato de salida Ds se toma igual al valor seleccionado, dicho de otro modo igual al valor corriente del dato de salida intermedio D_{IA}.

[0067] En el transcurso de una etapa 82 siguiente, los segundos medios de cálculo 44 transmiten el dato de salida Ds y el código de seguridad C_S a los medios de emisión 18. Los medios de emisión 18 transmiten entonces el dato de salida Ds y el código de seguridad C_S al dispositivo de recepción 8.

[0068] En el transcurso de una etapa 83 siguiente, el dispositivo de recepción 8 recibe el dato de salida Ds y el código de seguridad C_S.

[0069] En el transcurso de una etapa 84 siguiente, el dispositivo de recepción 8 verifica, por aplicación del algoritmo de control, la coherencia entre el dato de salida Ds y el código de seguridad C_S.

[0070] Según un primer aspecto de la invención, el procedimiento de fiabilidad de datos según la invención permite garantizar así la función de «voto mayoritario» del calculador. En efecto, si los valores de los datos de salida intermedios D_{IA}, D_{IB} son idénticos, el dato de salida Ds toma por valor el valor mayoritario, en este caso el único valor posible. Por otro lado, si los valores de los datos de salida intermedios D_{IA}, D_{IB} difieren, el código de seguridad C_S toma un valor particular, diferente del valor que toma cuando los valores de los datos de salida intermedios D_{IA}, D_{IB} son idénticos.

[0071] Así, si los valores de los datos de salida intermedios D_{IA}, D_{IB} difieren, el dispositivo de recepción 8 determina una incoherencia entre el dato de salida Ds emitido y el código de seguridad C_S. El dispositivo de recepción 8 rechaza entonces el dato de salida Ds. El calculador 6 que aplica el procedimiento según la invención permite proporcionar por tanto en todos los casos ya sea un dato de salida Ds correcto, o un dato de salida Ds erróneo pero detectable.

[0072] Según un segundo aspecto de la invención, independiente y complementario del primer aspecto, el procedimiento de fiabilidad de datos permite garantizar la función de «pasivación» del calculador 6. Más particularmente, las etapas 66, 68 y 70 corresponden a la aplicación de esta función de «pasivación».

[0073] La etapa 72 de reinicialización permite por otro lado ventajosamente al calculador 6 auto-probar de manera periódica la función de «pasivación», y protegerse así del riesgo de fallo de los medios de eliminación 26A, 26B. Este riesgo corresponde a una imposibilidad para los medios de eliminación de eliminar la variable de cifrado V_{CA}, respectivamente V_{CB}, En los primeros medios de memorización 20A, respectivamente 20B. Además, en caso de fallo que se produzca en uno de los módulos de tratamiento durante la etapa 72 de reinicialización, la relación matemática de la fórmula (7), verificada teóricamente en cada instante i por las variables de cifrado V_{CA}, V_{CB}. Entre ellas, no se verifica más. Gracias a esta característica, la función de «pasivación» del calculador 6 sigue estando garantizada permanentemente, incluso en caso de fallo en uno de los módulos de tratamiento durante la etapa 72.

[0074] Se concibe así que el procedimiento de fiabilidad de datos según este modo de realización de la invención permite liberarse de la utilización de medios materiales dedicados para garantizar la función de voto mayoritario del calculador.

[0075] Este modo de realización constituye el modo de realización preferencial de la invención.

[0076] El experto en la materia comprenderá que la invención se aplica de la misma manera a un procedimiento de fiabilidad de datos que no consta de las etapas 66, 68, 70 y 72.

[0077] Como variante no representada, el calculador consta de un número N1 de módulos 12 de tratamiento de datos, siendo N1 un número entero superior o igual a tres. Cada módulo de tratamiento 12 consta de unos primeros medios de memorización 20 y de unos primeros medios de cálculo 22. Los primeros medios de memorización 20 de un módulo de tratamiento 12 son aptos para almacenar una variable de cifrado V_C, apta para el módulo. Cada uno de los primeros medios de cálculo 22 recibe el dato de entrada De y proporciona en entrada del órgano 14 un dato de salida intermedio D_I y un código de seguridad intermedio C_{SI}. De manera análoga al modo de realización preferencial de la invención, los módulos de tratamiento 12 son aptos para intercambiarse unos datos según un protocolo de comunicación sincronizado, a través de sus medios de comunicación y sus medios de sincronización respectivos. Además, las funciones de cálculo σ, las funciones de cifrado Fc y las funciones de reinicialización F_{rein} de cada uno de los módulos de tratamiento son idénticas.

[0078] Según esta variante de realización, cada uno de los primeros medios de cálculo 22 es apto además para verificar la correspondencia entre el valor del dato de salida intermedio D_I correspondiente y un eventual valor mayoritario. Además, el procedimiento consta de dos etapas suplementarias 86, 88. Las etapas 86, 88 se efectúan entre la etapa 68 y la etapa 72 si después de la etapa 68, cada uno de los primeros medios de cálculo 22 determina que existe un valor mayoritario entre los valores de los datos de salida intermedios D_I.

[0079] Durante la etapa 86, cada uno de los primeros medios de cálculo 22 verifica si el valor de su dato de salida intermedio D_I es igual al valor mayoritario.

[0080] Si después de la etapa 86, cada uno de los primeros medios de cálculo 22 verifica que el valor de su dato

de salida intermedio D_I es igual al valor mayoritario, la etapa 72 se efectúa.

[0081] Si después de la etapa 86, al menos uno de los primeros medios de cálculo 22 verifica que el valor de su dato de salida intermedio D_I no es igual al valor mayoritario, los medios de eliminación del módulo de tratamiento correspondiente eliminan el valor corriente de la variable de cifrado V_C en los primeros medios de memorización 20 en el transcurso de la etapa 88.

[0082] El experto en la materia comprenderá que, durante la etapa 76, los primeros medios de cálculo 22 de cada módulo de tratamiento 12 transmiten el dato de salida intermedio D_I correspondiente y el código de seguridad intermedio C_{SI} correspondiente, a los segundos medios de cálculo 44 del órgano de cálculo 14.

[0083] Durante la etapa 78 siguiente, los segundos medios de cálculo 44 calculan el valor corriente del código de seguridad C_S a partir del valor corriente de cada código de seguridad intermedio C_{SI} transmitido durante la etapa 76.

[0084] Durante la etapa 80 siguiente, los segundos medios de cálculo 44 seleccionan un valor entre los valores de los datos de salida intermedios D_I transmitidos durante la etapa 76. El valor corriente del dato de salida Ds se toma entonces igual al valor seleccionado.

[0085] En el transcurso de la etapa 82 siguiente, los segundos medios de cálculo 44 transmiten el dato de salida Ds y el código de seguridad C_S a los medios de emisión 18. Los medios de emisión 18 transmiten entonces el dato de salida Ds y el código de seguridad C_S al dispositivo de recepción 8.

[0086] En el transcurso de la etapa 83 siguiente, el dispositivo de recepción 8 recibe el dato de salida Ds y el código de seguridad C_S.

[0087] En el transcurso de la etapa 84 siguiente, el dispositivo de recepción 8 verifica, por aplicación del algoritmo de control, la coherencia entre el dato de salida Ds y el código de seguridad C_S.

[0088] Según otra variante de realización particular, no representada, el calculador consta de tres módulos 12A, 12B, 12C de tratamiento de datos. La condición de «voto mayoritario» se cumple entonces cuando al menos dos de los tres módulos han producido unos datos de salida coherentes a partir del mismo dato de entrada.

[0089] Un calculador constituido de este modo consta entonces de tres pares (12A; 12B), (12B; 12C) y (12C; 12A) de módulos de tratamiento, perteneciendo cada módulo 12A, 12B, 12C a dos pares.

[0090] En cada módulo de tratamiento 12A, 12B, 12C, el proceso de generación del código de seguridad intermedio se dobla entonces. En particular, dos códigos de seguridad intermedios $C_{SI\text{-}AB}$, $C_{SI\text{-}AC}$, $C_{SI\text{-}BA}$, $C_{SI\text{-}BC}$, $C_{SI\text{-}CA}$, $C_{SI\text{-}CB}$ son generados por cada módulo 12A, 12B, 12C. Más precisamente, cada módulo 12A, 12B, 12C genera un código para cada par (12A; 12B), (12B; 12C) y (12C; 12A) al cual pertenece.

[0091] Los primeros medios de memorización 20 de cada módulo 12A, 12B, 12C son aptos para almacenar dos variables de cifrado Vc1 y Vc2, relativas al módulo.

[0092] Cada uno de los primeros medios de cálculo 22 recibe el dato de entrada De y proporciona en entrada del órgano 14 un dato intermedio D_I y dos códigos de seguridad intermedios C_{SI}: el módulo 12A calcula dos códigos $C_{SI\text{-}AB}$ y $C_{SI\text{-}AC}$; el módulo 12B calcula dos códigos $C_{SI\text{-}BA}$ y $C_{SI\text{-}BC}$; el módulo 12C calcula dos códigos $C_{SI\text{-}CA}$ y $C_{SI\text{-}CB}$.

[0093] El órgano 14 selecciona un par de módulos entre los tres pares posibles (12A; 12B), (12B; 12C) y (12C; 12A), sobre la base de un voto mayoritario de los datos D_I recibidos.

[0094] El órgano 14 calcula entonces el código de seguridad C_S a partir de los códigos de seguridad intermedios asociados al par seleccionado. Así, si el par (12A; 12B) ha sido seleccionado entonces el código de seguridad C_S se calcula a partir de los códigos intermedios $C_{SI\text{-}AB}$ y $C_{SI\text{-}BA}$.

[0095] Se concibe así que el procedimiento de fiabilidad de datos según la invención permite liberarse de la utilización de medios materiales dedicados para garantizar la función de voto mayoritario y de pasivación del calculador.

REIVINDICACIONES

1. Procedimiento de fiabilidad de datos en un calculador (6), siendo el calculador (6) apto para proporcionar un dato de salida (Ds) a partir de un dato de entrada (De), y que consta al menos de dos módulos (12A, 12B) de tratamiento de datos y un órgano de cálculo (14) vinculado a cada módulo de tratamiento (12A, 12B), comprendiendo el procedimiento una etapa (64) de cálculo, por cada módulo de tratamiento (12A, 12B), de un dato intermedio (D_{IA}, D_{IB}) a partir del dato de entrada (De), consistiendo dicho cálculo en la aplicación de una función de cálculo (σ) al dato de entrada (De), siendo la función de cálculo (σ) idéntica para todos los módulos de tratamiento (12A, 12B),

estando el procedimiento **caracterizado porque** comprende las etapas siguientes:

- el cálculo (74), por cada módulo de tratamiento (12A, 12B), de un código de seguridad intermedio (C_{SIA}, C_{SIB}) a partir del dato intermedio (D_{IA}, D_{IB}) correspondiente,

- la transmisión (76) al órgano de cálculo (14), por cada módulo de tratamiento (12A, 12B), del código de seguridad intermedio (C_{SIA}, C_{SIB}) y del dato intermedio (D_{IA}, D_{IB}),

- el cálculo (78), por el órgano de cálculo (14), de un código de seguridad (C_S) a partir de los códigos de seguridad intermedios (C_{SIA}, C_{SIB}),

- la selección (80), por el órgano de cálculo (14), de un dato intermedio entre los datos intermedios (D_{IA}, D_{IB}) recibidos, comprendiendo el dato de salida (Ds) del calculador (6) el dato intermedio seleccionado y

- la transmisión (82) con destino a un dispositivo de recepción (8), por el órgano de cálculo (14), del código de seguridad (C_S) y del dato de salida (Ds).

2. Procedimiento según la reivindicación 1, **caracterizado porque** cada módulo de tratamiento (12A, 12B) consta de unos primeros medios de memorización (20A, 20B) de al menos una variable de cifrado (V_{CA}, V_{CB}) y de una función de cifrado (Fc), siendo la función de cifrado (Fc) idéntica para todos los módulos de tratamiento (12A, 12B) y **porque** durante la etapa (74) de cálculo de un código de seguridad intermedio (C_{SIA}, C_{SIB}) a partir del dato intermedio (D_{IA}, D_{IB}) correspondiente, dicho cálculo consiste en aplicar, por cada módulo de tratamiento (12A, 12B), la función de cifrado (Fc) al menos al dato intermedio (D_{IA}, D_{IB}) y a la variable de cifrado (V_{CA}, V_{CB}).

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado porque** el órgano de cálculo (14) consta de unos segundos medios de memorización (42) de al menos una constante de descifrado (K_D) y una función de consolidación (F_{conso}) y **porque** durante la etapa (78) de cálculo de un código de seguridad (C_S) a partir de los códigos de seguridad intermedios (C_{SIA}, C_{SIB}), dicho cálculo consiste en aplicar, por el órgano de cálculo (14), la función de consolidación (F_{conso}) a cada código de seguridad intermedio (C_{SIA}, C_{SIB}) recibido y a la constante de descrifrado (K_D).

4. Procedimiento según la reivindicación 2 ó 3, **caracterizado porque** consta además, entre la etapa (64) de cálculo de un dato intermedio y la etapa (74) de cálculo de un código de seguridad intermedio, de una etapa (66) de transmisión, por cada módulo de tratamiento (12A, 12B), del valor de su dato intermedio (D_{IA}, D_{IB}) a los otros módulos de tratamiento (12A, 12B) y una etapa (68) de prueba, por cada módulo de tratamiento (12A, 12B), de la existencia de un valor mayoritario entre el conjunto de los valores de los datos intermedios (D_{IA}, D_{IB}), siendo el valor mayoritario el valor más frecuente entre los valores de datos intermedios (D_{IA}, D_{IB}), si este valor existe.

5. Procedimiento según la reivindicación 4, **caracterizado porque**, si la prueba de existencia de un valor mayoritario es negativa durante la etapa (68) de prueba correspondiente, el procedimiento consta de una etapa (70) de supresión por uno de los módulos de tratamiento (12A, 12B) de su variable de cifrado (V_{CA}, V_{CB}).

6. Procedimiento según una de las reivindicaciones de 2 a 5, **caracterizado porque** consta además, antes de la etapa (74) de cálculo de un código de seguridad intermedio, de una etapa (72) de reinicialización, por cada módulo de tratamiento (12A, 12B), de su variable de cifrado (V_{CA}, V_{CB}), siendo efectuada dicha etapa (72) de reinicialización de manera sincronizada entre todos los módulos de tratamiento (12A, 12B).

7. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** el dato de salida (Ds) es el dato intermedio seleccionado por el órgano de cálculo (14) durante la etapa (80) de selección.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** consta además de una etapa (83) de recepción, por el dispositivo de recepción (8), del código de seguridad (C_S) y del dato de salida (Ds) y una etapa (84) de verificación, por el dispositivo de recepción (8), de la coherencia entre el código de seguridad (C_S) y el dato de salida (Ds).

9. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado porque** el calculador consta de tres módulos de tratamiento de datos, estando los tres módulos de tratamiento distribuidos en tres pares de módulos, perteneciendo cada módulo a dos pares distintos, **porque** cada módulo de tratamiento calcula dos códigos de seguridad intermedios a partir del dato intermedio correspondiente, estando asociado cada código de seguridad intermedio a uno de los dos pares al cual pertenece el módulo, **porque** cada módulo de tratamiento transmite al órgano de cálculo (14) el dato intermedio y los dos códigos de seguridad intermedios asociados, **porque** el órgano de cálculo (14) calcula el código de seguridad (Cs) a partir de un primer código de seguridad intermedio transmitido por uno de los módulos de tratamiento y asociado a un primer par de módulos y de un segundo código de seguridad intermedio transmitido por otro módulo, estando asociado dicho segundo código de seguridad intermedio al primer par de módulos y **porque** el dato intermedio seleccionado por el órgano de cálculo (14) es uno de los datos intermedios asociados a los módulos del primer par de módulos.

10. Calculador (6) apto para proporcionar un dato de salida (Ds) a partir de un dato de entrada (De) que consta:

- al menos de dos módulos (12A, 12B) de tratamiento de datos, constando cada módulo de tratamiento (12A, 12B) de unos primeros medios (22A, 22B) de cálculo de un dato intermedio (D_{IA}, D_{IB}) a partir del dato de entrada (De), siendo dichos primeros medios de cálculo aptos para aplicar una función de cálculo (σ) al dato de entrada (De), siendo la función de cálculo (σ) idéntica para todos los módulos de tratamiento (12A, 12B),

caracterizado porque los primeros medios (22A, 22B) de cálculo son aptos además para calcular un código de seguridad intermedio (C_{SIA}, C_{SIB}) a partir del dato intermedio (D_{IA}, D_{IB}) correspondiente, siendo cada módulo de tratamiento (12A, 12B) apto para transmitir al órgano de cálculo (14) el código de seguridad intermedio (C_{SIA}, C_{SIB}) y el dato intermedio (D_{IA}, D_{IB}) correspondiente y **porque** el órgano de cálculo (14) consta de unos segundos medios (44) de cálculo de un código de seguridad (C_S) a partir de los códigos de seguridad intermedios (C_{SIA}, C_{SIB}), siendo el órgano de cálculo (14) apto para seleccionar un dato intermedio entre los datos intermedios (D_{IA}, D_{IB}) recibidos y para transmitir el código de seguridad (C_S) y el dato de salida (Ds) a un dispositivo de recepción (8), comprendiendo el dato de salida (Ds) el dato intermedio seleccionado.

11. Conjunto de comunicación (2) que consta de un calculador (6) y un dispositivo (8) de recepción de datos, siendo el calculador (6) apto para proporcionar un código de seguridad (C_S) y un dato (Ds), constando el dispositivo de recepción (8) de unos medios de memorización de un algoritmo de control, siendo el dispositivo de recepción (8) apto para recibir el código de seguridad (C_S) y el dato de salida (Ds) y para verificar, por la aplicación del algoritmo de control, la coherencia entre el código de seguridad (C_S) y el dato de salida (Ds), **caracterizado porque** el calculador (6) es conforme a la reivindicación 10.

12. Sistema de gestión ferroviaria (1) **caracterizado porque** comprende al menos un conjunto (2) según la reivindicación 11.

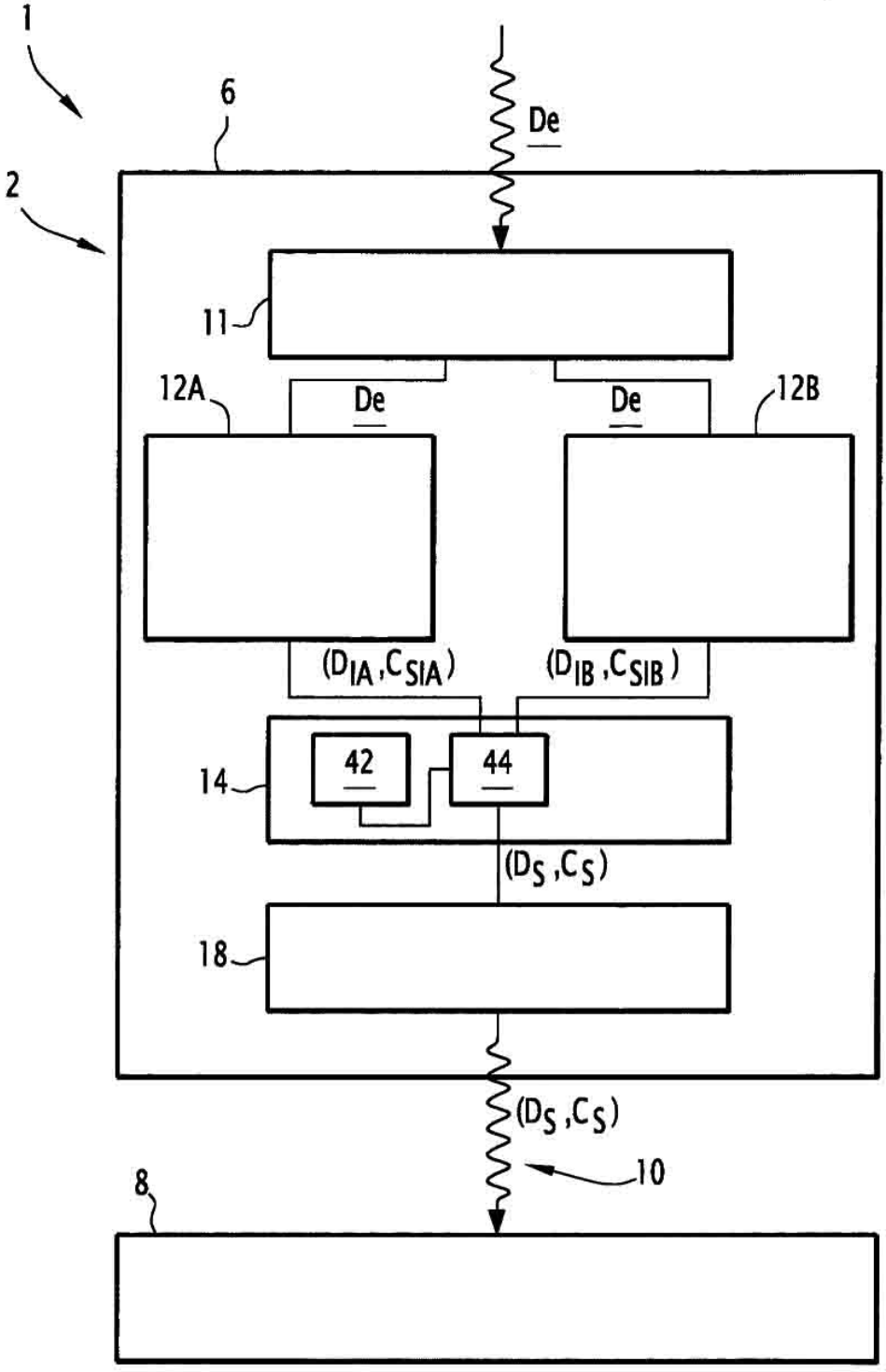
1
6
De
2
11
12A
De
De
12B
(DIA ,CSIA)
(DIB ,CSIB)
14
42
44
(DS ,CS)
18
(DS ,CS)
10
8

FIG.1

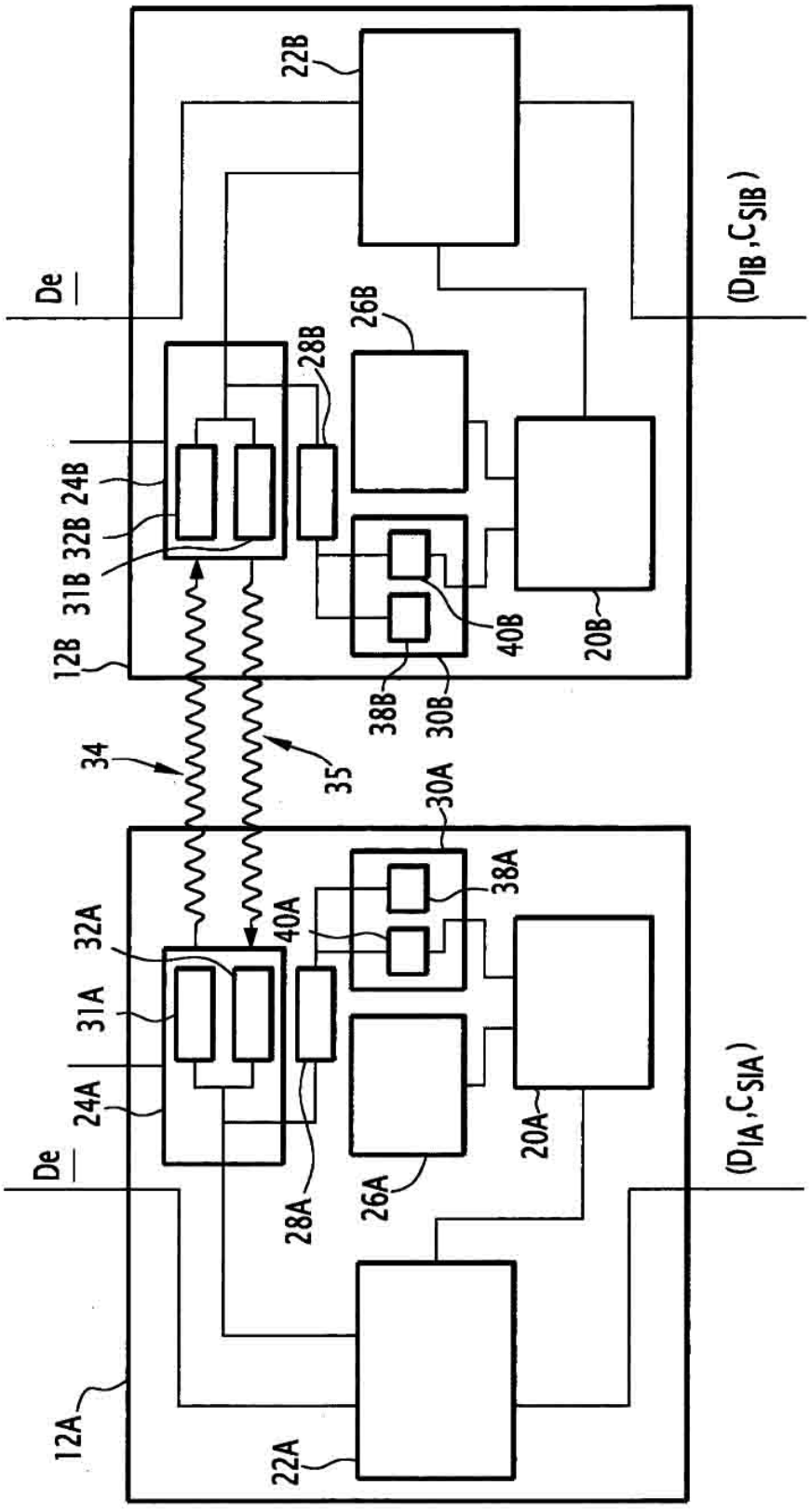
22B
De
(D_{IB}, C_{SIB})
26B
28B
24B
32B
31B
12B
40B
20B
38B
30B
34
35
30A
38A
32A
40A
31A
24A
De
(D_{IA}, C_{SIA})
20A
28A
26A
12A
22A

FIG.2

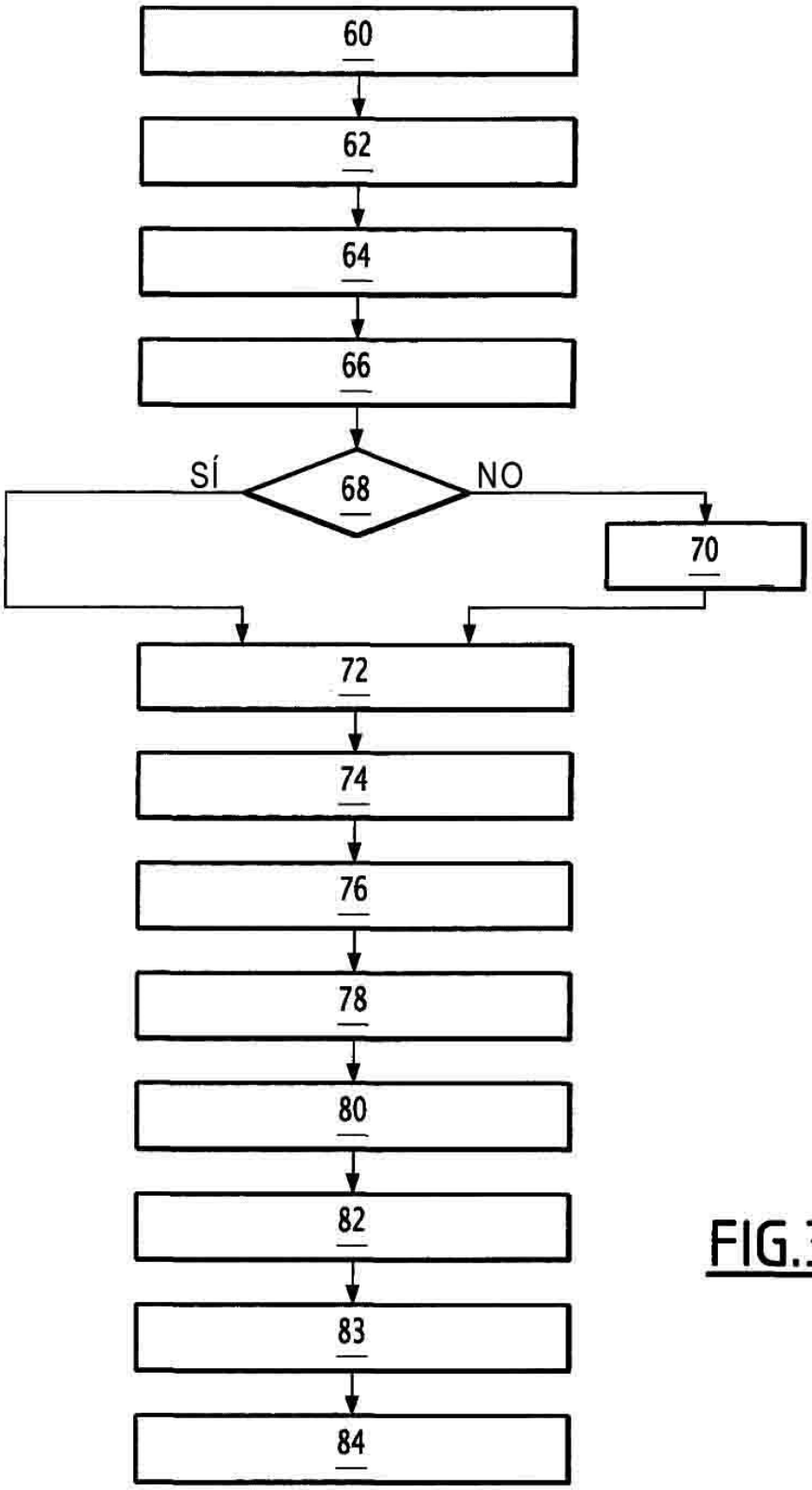

FIG.3