(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 786 635**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 9/445 (2008.01)
G06F 21/64 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.09.2018 E 18193027 (2)**

(97) Fecha y número de publicación de la concesión europea: **29.01.2020 EP 3454246**

(54) Título: **Método para transmitir y verificar la validez de los datos de configuración en un sistema electrónico, sistema electrónico asociado y producto de programa informático**

(30) Prioridad:

08.09.2017 FR 1758290

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.10.2020

(73) Titular/es:

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

(72) Inventor/es:

DEGENEVE, XAVIER;
BREGARDIS, CEDRIC;
QUADRINI, MATTHIEU y
FERNANDEZ-VALBON, RAFAEL

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Método para transmitir y verificar la validez de los datos de configuración en un sistema electrónico, sistema electrónico asociado y producto de programa informático

La presente invención se refiere a un método para transmitir y verificar la validez de los datos de configuración en un sistema electrónico, un sistema electrónico y un producto de programa informático asociado con el mismo.

Los métodos para reconfigurar una pluralidad de placas electrónicas en un vehículo se conocen de los documentos US 2008/216067, US 2014/032916 y DE 10 2009 058754.

En la técnica anterior, se conoce igualmente el uso de sistemas electrónicos para el almacenamiento centralizado de datos de configuración. Los datos de configuración están destinados a diferentes módulos o también a tarjetas electrónicas que constituyen estos sistemas.

Entre estos sistemas, se puede mencionar en particular ciertos elementos del equipo acomodados a bordo de un vehículo ferroviario, tal como, por ejemplo, una consola para la comunicación con el conductor del vehículo ferroviario, equipo de tracción, equipo de red, equipo que acciona las salidas o lee las entradas. También se puede hacer mención, en particular, a ciertos elementos de equipo en el suelo a lo largo de las vías de un sistema ferroviario, en particular para la señalización, tal como, por ejemplo, de equipos que interactúan con objetos en la vía (luces de señalización, interruptores, pasos a nivel, circuitos de vía, balizas).

Los datos de configuración son necesarios para el funcionamiento de los módulos o placas electrónicas correspondientes, y se almacenan en un módulo de almacenamiento centralizado provisto para este propósito.

Cuando un sistema electrónico con almacenamiento centralizado de datos de configuración muestra un alto nivel de criticidad, los datos de configuración se almacenan en forma de una estructura de datos segura.

Esta estructura se asocia con una firma que permite verificar la validez de los datos de configuración correspondientes. La verificación de la validez de los datos comprende, en particular, la verificación de la autenticidad, la integridad y la coherencia de estos datos.

En general, la validez de los datos de configuración se verifica cada vez que arranca el sistema electrónico correspondiente.

En particular, en el momento de tal arranque, una de las placas electrónicas del sistema electrónico extrae todos los datos de configuración del módulo de almacenamiento y verifica la validez de estos datos.

Cuando se verifica la validez, dicha placa electrónica transmite los datos de configuración correspondientes a estas placas a las otras placas electrónicas.

Al recibir los datos de configuración correspondientes, cada placa electrónica almacena estos datos en su memoria interna y verifica su integridad, así como también su coherencia.

El sistema electrónico es operativo cuando cada placa ha recibido, verificado y almacenado los datos de configuración correspondientes.

Entonces se entenderá que tal método de arranque de un sistema electrónico con almacenamiento centralizado de datos de configuración es particularmente lento y no es adecuado cuando es necesario realizar reinicios frecuentes del sistema y/o cuando el sistema incluye una gran cantidad de módulos o placas electrónicas. Por lo tanto, por ejemplo, la duración de un arranque de un sistema electrónico de acuerdo con este método puede tomar hasta 30 minutos cuando el sistema está compuesto, por ejemplo, de 50 placas electrónicas.

La presente invención se refiere a un método para remediar este inconveniente de la técnica anterior al proponer un sistema electrónico y un método para transmitir y verificar la validez de los datos de configuración implementados por este sistema, lo que hace posible reducir considerablemente el tiempo de reinicio de tal sistema.

Para este propósito, la invención se refiere a un método para transmitir y verificar la validez de los datos de configuración de acuerdo con la reivindicación 1.

De acuerdo con otros aspectos ventajosos de la invención, el método comprende una o más de las características de las reivindicaciones 2 a 10.

La invención también se refiere a un producto de programa informático que comprende instrucciones de software que, cuando se implementan mediante un equipo informático, implementan el método como se definió anteriormente.

La invención también se refiere a un sistema electrónico con almacenamiento centralizado de datos de configuración de acuerdo con la reivindicación 12.

Estas características y ventajas de la invención serán evidentes a partir de una lectura de la siguiente descripción, dada únicamente a manera de ejemplo no limitante, y con referencia a los dibujos adjuntos, en los que:

La Figura 1 muestra una vista esquemática de un sistema electrónico de acuerdo con la invención, el sistema que comprende, en particular, un módulo de almacenamiento centralizado;

La Figura 2 muestra una vista esquemática de una estructura de datos almacenada en el módulo de almacenamiento de la Figura 1; y

La Figura 3 muestra un diagrama de flujo de un método para transmitir y verificar la validez de los datos de configuración en el sistema electrónico de la Figura 1.

El sistema electrónico 10 de la Figura 1 incluye una pluralidad de placas electrónicas 12A a 12N que implementan la operación del sistema 10, y un módulo de almacenamiento centralizado 14.

El sistema electrónico 10 puede usarse en particular en el sector ferroviario y tiene, por ejemplo, un elemento de equipo instalado a bordo de un vehículo ferroviario, tal como una consola para la comunicación con el conductor del vehículo.

Cada placa electrónica 12A a 12N proporciona un servicio al sistema electrónico 10 mediante el uso de los datos de configuración específicos de esta placa. En otras palabras, los datos de configuración definen el departamento proporcionado por la placa electrónica correspondiente 12A a 12N en respuesta a los diferentes eventos que ocurren en el sistema 10.

Cada placa electrónica 12A a 12N tiene, por ejemplo, la forma de un dispositivo lógico programable que comprende, en particular, una memoria interna M. Tal dispositivo lógico programable es, por ejemplo, del tipo FPGA (matriz de puertas programable en campo).

La memoria interna M puede tener la propiedad de mantener la información almacenada, incluso cuando no se suministra con energía eléctrica.

La memoria interna se diseña para almacenar una variable de firma y variables de configuración.

La variable de firma corresponde a una firma elemental de las variables de configuración.

Las variables de configuración corresponden a configuraciones de datos recuperadas por la placa electrónica 12A a 12N, como se explicará a continuación.

De acuerdo con una variante, al menos algunas de las placas electrónicas tienen una forma más compleja, por ejemplo, la forma de un ordenador en miniatura que comprende en particular un procesador y una memoria interna.

De acuerdo con una variante, al menos algunas de las placas electrónicas son reemplazables. En este caso, se dice que el sistema electrónico 10 es adaptable.

De acuerdo con una variante, al menos algunas de las placas electrónicas son reemplazables cuando se calientan sin interrumpir el funcionamiento de las otras placas del sistema (a excepción de las comunicaciones/servicios que usan la tarjeta que se reemplaza. En este caso, se dice que el sistema electrónico 10 es adaptable cuando se calienta o está en funcionamiento.

Los datos de configuración de todas las placas 12A a 12N se almacenan al menos inicialmente en el módulo de almacenamiento centralizado 14 en forma de una estructura de datos segura 20 que se ilustra con mayor detalle en la Figura 2.

Por lo tanto, con referencia a esta Figura 2, la estructura de datos 20 comprende una pluralidad de bloques de datos de configuración 22A a 22N asociados respectivamente con las placas electrónicas 12A a 12N.

Cada uno de estos bloques de datos 22A a 22N incluye los datos de configuración específicos de la placa electrónica 12A a 12N asociada con este bloque.

Esta estructura de datos 20 se asocia con una firma global 24 que hace posible verificar la validez de los datos contenidos en esta estructura.

La firma global 24 se almacena, por ejemplo, en el módulo de almacenamiento centralizado 14 con la estructura de datos 20.

La firma global 24 se determina, por ejemplo, a partir de los datos contenidos en la estructura 20 de acuerdo con los métodos conocidos per se.

Los datos de configuración pueden modificarse, por ejemplo, por un usuario para modificar el funcionamiento del sistema a bordo 10. Por lo tanto, en el ejemplo anterior de la consola para la comunicación con el conductor, la modificación de los datos de configuración hace posible, por ejemplo, activar nuevos mensajes para el conductor.

Cuando se modifican los datos de configuración, la firma global 24 igualmente se modifica.

El módulo de almacenamiento centralizado 14 se conecta a una de las placas electrónicas 12A a 12N, por ejemplo, la placa electrónica 12A, denominada a continuación como la placa principal.

La placa principal 12A hace posible implementar un método de transmisión y verificación de la validez de los datos de configuración obtenidos del módulo de almacenamiento centralizado 14 que se explicará a continuación con referencia a la Figura 3, que muestra un diagrama de flujo de las etapas del método.

En particular, el método de transmisión y verificación de la validez de los datos de configuración corresponde a una fase de arranque PR del sistema electrónico 10.

Esta fase de arranque PR luego se implementa en el arranque inicial del sistema electrónico 10 y en el reinicio posterior.

Durante la etapa inicial 110 de la fase de arranque PR, el sistema electrónico 10 recibe un comando de arranque inicial o de reinicio. Debe señalarse que el comando recibido no indica si el arranque es inicial o modificado por los datos de configuración.

El sistema electrónico 10 activa entonces el funcionamiento de todas las placas electrónicas 12A a 12N y, en particular, el funcionamiento de la placa principal 12A.

Durante la siguiente etapa 120, la placa principal 12A extrae la estructura de datos 20 del módulo de almacenamiento 14.

Luego, la placa principal 12A verifica la validez de los datos de configuración de la estructura de datos 20.

La verificación de la validez de los datos comprende en particular la verificación de la autenticidad, la integridad y la coherencia de estos datos.

Para verificar la validez, la placa principal 12A genera una firma global SG, por ejemplo, a partir de los datos de configuración recibidos, mediante el uso de los mismos métodos que los usados para determinar la firma global 24 asociada con la estructura de datos 20.

Luego, la placa principal 12A compara la firma global generada SG con la firma 24 asociada con la estructura de datos 20.

Cuando las dos firmas coinciden, la placa principal 12A pasa a la etapa 130. En el caso contrario, la placa principal 12A pasa a la etapa 135 durante el cual genera un mensaje de error destinado, por ejemplo, al usuario e interrumpe la ejecución de la fase de arranque PR.

Durante la etapa 130, la placa principal 12A genera una firma elemental SE para cada una de las placas electrónicas 12A a 12N.

Tal firma elemental SE para una placa electrónica dada 12A a 12N se genera, por ejemplo, a partir de los datos de configuración específicos de esta placa electrónica 12A a 12N mediante el uso de, por ejemplo, métodos análogos a los usados para generar la firma global SG.

Durante la siguiente etapa 140, la placa principal 12A almacena las firmas elementales generadas SE y la firma global generada SG en su memoria interna M.

Luego, durante la misma etapa 140, la placa principal 12A proporciona a cada placa electrónica 12A a 12N las firmas elementales generadas SE y los datos de configuración específicos de esta placa 12A a 12N.

Luego, cada placa electrónica 12A a 12N recupera la firma elemental que está asociada con esta por la placa principal 12A.

Durante la siguiente etapa 145, cada placa 12A a 12N calcula su firma elemental SE a partir de las variables de configuración almacenadas en su memoria interna M mediante el uso de, por ejemplo, métodos análogos a los usados para generar la firma global SG, y fija la variable de firma a que sea igual al valor calculado de la firma elemental.

Durante la siguiente etapa 150, cada placa electrónica 12A a 12N compara la firma elemental recuperada SE con la variable de firma que tiene en su memoria interna M (debe señalarse que, si no se ha almacenado información en esta memoria M de antemano, la placa se comportará como si la variable de firma fuera diferente y los datos no fueran válidos).

Luego, cada placa electrónica (12A a 12N) verifica la validez de las variables de configuración almacenadas en su memoria interna mediante el uso de la firma elemental recuperada (SE) y la variable de firma.

Para verificar la validez de las variables de configuración correspondientes, cada placa electrónica 12A a 12N compara la variable de firma recuperada con la firma elemental recuperada SE.

Si la firma elemental SE coincide con la variable de firma, la placa electrónica correspondiente 12A a 12N valida las variables de configuración y la placa 12A a 12N pasa a la etapa 180. En el caso opuesto, la placa electrónica correspondiente 12A a 12N pasa a la etapa 160.

Durante la etapa 180, la placa correspondiente 12A a 12N recupera las variables de configuración de su memoria interna M y, por ejemplo, coloca estas variables en su lugar para que sean operativas.

Durante la etapa 160, la placa 12A a 12N recupera los datos de configuración que están asociados con esta y se proporcionan por la placa principal 12A, calcula la firma de datos recibida SE y verifica que coincida con la firma SE proporcionada.

Luego, la placa correspondiente 12A a 12N fija la variable de firma para que sea igual a la firma elemental calculada o recuperada SE y fija las variables de configuración para que sean iguales a los datos de configuración recuperados.

Al final de esta etapa 160, la placa correspondiente 12A a 12N recupera las variables de configuración de su memoria interna y, por ejemplo, coloca estas variables en su lugar para que sean operativas.

Por lo tanto, después de las etapas 160 y 180, cada placa 12A a 12N tiene sus datos de configuración y la firma SE y tiene una copia de los datos de configuración y de la firma en su memoria M.

La etapa 190 es la etapa final de la fase de arranque PR, al final de la cual el sistema electrónico 20 está operativo.

Ventajosamente, después de la etapa 180, las placas 12B a 12N verifican periódicamente que los datos de configuración usados estén en efecto autorizados. Para esto, verifican que la firma elemental SE usada, es decir, la variable de firma, sea siempre la misma que la proporcionada por la placa principal 12A.

Si este no es el caso, la placa genera un mensaje de error destinado, por ejemplo, al usuario, e interrumpe la ejecución o vuelve a la etapa 160 para recuperar los nuevos datos de configuración (esta elección depende de la función proporcionada, por ejemplo, para una función de seguridad, el producto se establecerá en un estado seguro).

Ventajosamente, el método simplifica considerablemente el reemplazo de una placa electrónica 12B, ... 12N en el sistema electrónico 10 por una nueva placa electrónica.

En este caso, el método comprende además las siguientes etapas:

reemplazar una placa electrónica 12B, ... 12N en el sistema electrónico 10 por una nueva placa electrónica;

generación de una firma elemental SE para al menos la nueva placa electrónica a partir de los datos de configuración almacenados en el módulo de almacenamiento centralizado 14;

transmisión de la firma elemental SE al menos a la nueva placa electrónica; y

ejecución de la etapa 150 de verificar las variables de configuración para la nueva placa electrónica.

Se debe entender que la invención ofrece una cierta cantidad de ventajas.

De hecho, el método de transmisión y verificación de la validez de los datos de configuración de acuerdo con la invención hace posible realizar un reinicio del sistema electrónico particularmente rápido ya que solo se enviarán los datos no presentes.

En particular, durante la fase de reinicio del sistema electrónico 10, los datos de configuración, cuando no se modifican, no se transmiten nuevamente a las placas electrónicas correspondientes.

La validez de estos datos se verifica mediante el uso de las firmas elementales correspondientes que se transmiten a las placas electrónicas correspondientes de manera particularmente rápida.

La validez de estos datos se verifica periódicamente mediante el uso de las firmas elementales correspondientes, lo que permite garantizar que se aplique correctamente un cambio de configuración (o que se llevarán a cabo las acciones apropiadas).

Esto permite reducir considerablemente el tiempo de ejecución para llevar a cabo la fase de reinicio y, por lo tanto, el tiempo total de reinicio del sistema electrónico.

REIVINDICACIONES

1. Método para transmitir y verificar la validez de los datos de configuración en un sistema electrónico (10) con almacenamiento centralizado de los datos de configuración, el sistema electrónico que comprende una pluralidad de placas electrónicas (12A, ..., 12N) capaces de implementar la operación del sistema electrónico (10) mediante el uso de datos de configuración específicos para cada una de estas placas (12A, ..., 12N) y un módulo de almacenamiento centralizado (14) capaz de almacenar centralmente los datos de configuración para el conjunto de placas electrónicas (12A, ... , 12N), cada placa electrónica (12A, ..., 12N) que comprende una memoria interna diseñada para almacenar una variable de firma y las variables de configuración;
el método que comprende las siguientes etapas:

generar (130) una firma elemental (SE) para cada una de las placas electrónicas (12A, ..., 12N) a partir de los datos de configuración almacenados en el módulo de almacenamiento centralizado (14);

transmitir (140) a cada placa electrónica (12A, ..., 12N) la firma elemental (SE) específica de esta placa (12A, ..., 12N);

calcular (145) por cada placa electrónica (12A, ..., 12N) la variable de firma de acuerdo con las variables de configuración almacenadas en la memoria interna de la placa electrónica (12A, ..., 12N);

verificar (150) por cada placa electrónica (12A, ..., 12N) la validez de las variables de configuración almacenadas en la memoria interna de la placa (12A, ..., 12N) mediante el uso de la firma elemental recibida (SE) y la variable de firma; y

el método que comprende la siguiente etapa implementada para cada placa electrónica (12A, ..., 12N), para la cual, durante la etapa de verificar (150) la validez de las variables de configuración, las variables de configuración se consideran inválidas:

recuperar (160) los datos de configuración específicos de esta placa (12A, ..., 12N) y modificar las variables de configuración a partir de los datos de configuración recuperados.

2. El método de acuerdo con la reivindicación 1, en donde cada firma elemental (SE) se genera por solo una de las placas electrónicas (12A, ..., 12N) mediante el uso de los datos de configuración específicos de cada una de las placas electrónicas (12A, ..., 12N) y se almacenan en el módulo de almacenamiento centralizado (14).

3. El método de acuerdo con la reivindicación 1 o 2, en donde los datos de configuración se almacenan como una estructura de datos segura (20) asociada con una firma global (24).

4. El método de acuerdo con la reivindicación 3, en donde el método comprende la siguiente etapa antes de la etapa de generación (130):

verificar (120) la validez de los datos de configuración de la estructura de datos (20) mediante el uso de la firma global (24) asociada con esta estructura (20);

y la etapa de generación (130) se realiza si se verifica la validez de los datos de configuración.

5. El método de acuerdo con la reivindicación 4, en donde, después de la etapa de generación, el conjunto de firmas elementales (SE) y la firma global (24) se almacenan en la memoria interna de una de las placas electrónicas (12A, ..., 12N), denominada como la placa principal (12A).

6. El método de acuerdo con la reivindicación 5, en donde las etapas de verificar (120) la validez de los datos de configuración y de generación (130) de una firma elemental (SE) para cada una de las placas electrónicas (12A, ..., 12N), se implementan por la placa principal (12A).

7. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde verificar que los datos de configuración recuperados corresponden a la firma elemental (SE) se realiza en la etapa de recuperar (160) los datos de configuración, y luego las variables de configuración se modifican a partir de los datos de configuración recuperados para almacenar los datos de configuración recuperados en la memoria interna de la placa (12A, ... 12N).

8. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el método comprende, para cada placa electrónica (12A, ..., 12N), para las cuales las variables de configuración se consideran válidas durante la etapa (150) de verificar la validez de las variables de configuración:

recuperar (180) las variables de configuración por la placa electrónica (12A, ..., 12N) de la memoria interna de esta placa (12A, ... 12N).

9. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde la etapa de recuperación (160) de los datos de configuración comprende además:

recuperar, por la placa electrónica correspondiente (12A, ..., 12N), las variables de configuración de la memoria interna de esta placa (12A, ... 12N).

10. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el método comprende las siguientes etapas:

reemplazar una placa electrónica (12B, ... 12N) en el sistema electrónico (10) por una nueva placa electrónica;

generar una firma elemental (SE) para al menos la nueva placa electrónica a partir de los datos de configuración almacenados en el módulo de almacenamiento centralizado (14);

transmitir la firma elemental (SE) al menos a la nueva placa electrónica; y

ejecutar la etapa (150) de verificar las variables de configuración para la nueva placa electrónica.

11. El producto de programa informático que comprende instrucciones de software que, cuando se implementan mediante el equipo informático, implementan el método de acuerdo con cualquiera de las reivindicaciones anteriores.

12. El sistema electrónico (10) con almacenamiento centralizado de los datos de configuración, el sistema electrónico que comprende una pluralidad de placas electrónicas (12A, ..., 12N) capaces de implementar el funcionamiento del sistema electrónico (10) mediante el uso de los datos de configuración específicos para cada una de estas placas (12A, ..., 12N), y un módulo de almacenamiento centralizado (14) capaz de almacenar los datos de configuración centralmente para todas las placas electrónicas (12A, ..., 12N), cada placa electrónica (12A, .. ., 12N) que comprende una memoria interna diseñada para almacenar una variable de firma y variables de configuración; el sistema electrónico (20) que comprende medios para implementar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 10.

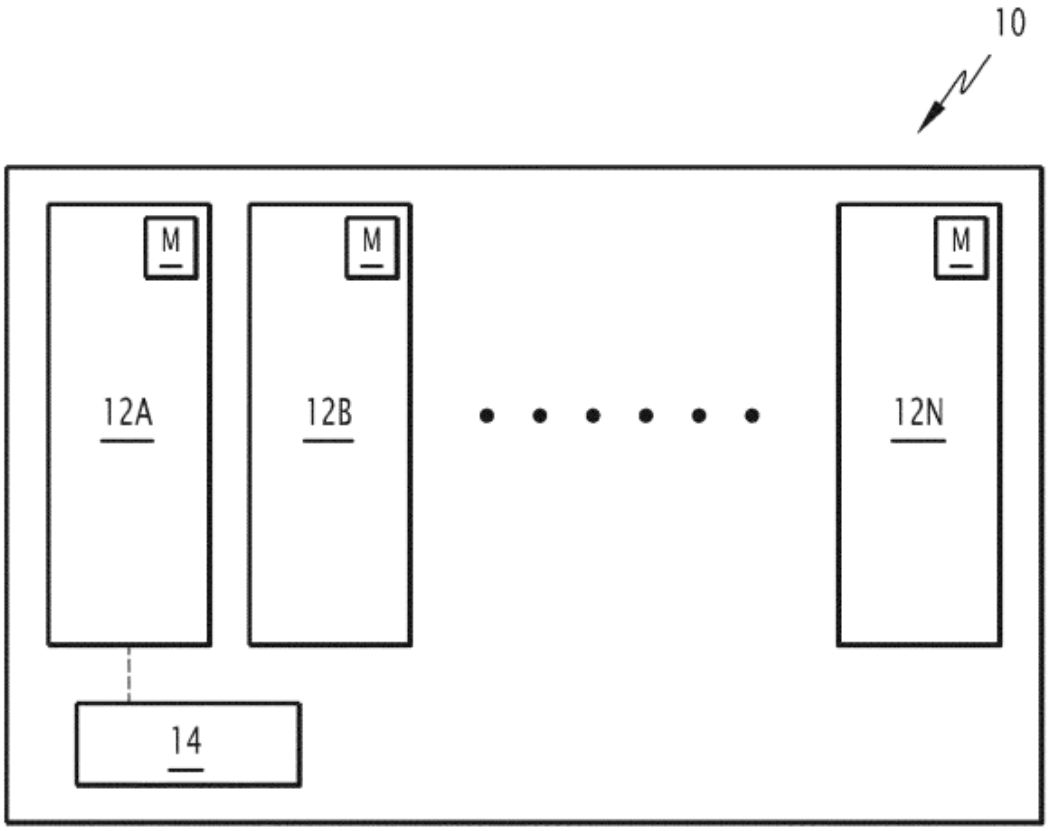

FIGURA 1

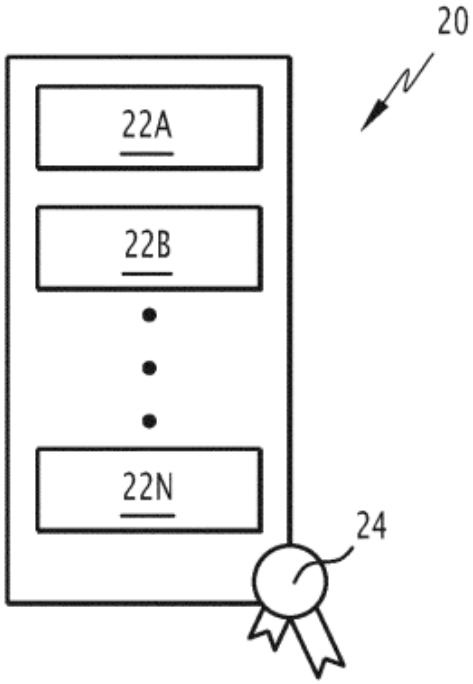

FIGURA 2

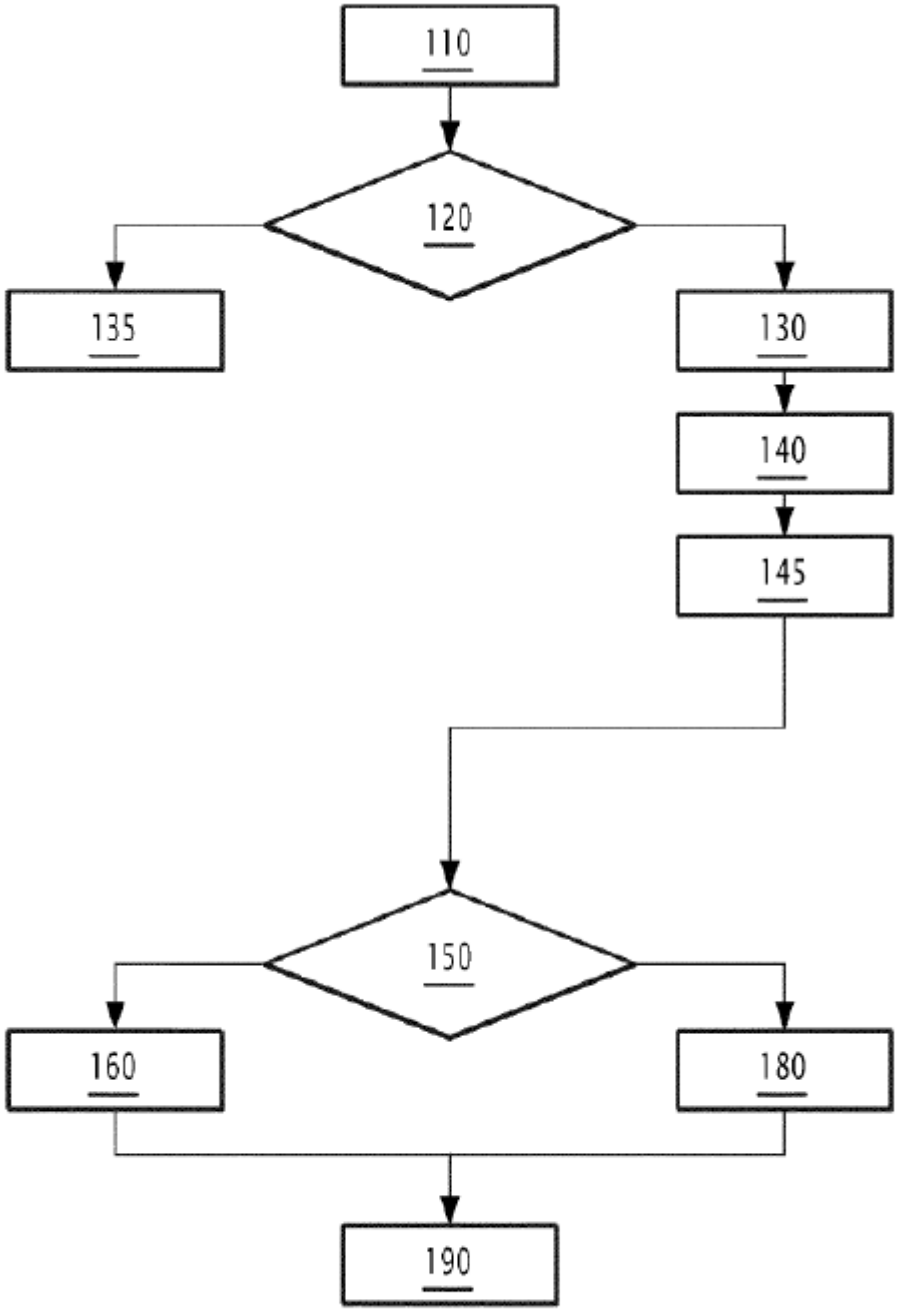

FIGURA 3