(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 349 908**

(51) Int. Cl.:
G06F 11/00 (2006.01)
G06F 11/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09151993 .4**
(96) Fecha de presentación : **03.02.2009**
(97) Número de publicación de la solicitud: **2090984**
(97) Fecha de publicación de la solicitud: **19.08.2009**

(54) Título: **Procedimiento de securización de un programa informático, dispositivo, procedimiento de actualización y servidor de actualización correspondientes.**

(30) Prioridad: **12.02.2008 FR 08 50883**

(45) Fecha de publicación de la mención BOPI:
12.01.2011

(45) Fecha de la publicación del folleto de la patente:
12.01.2011

(73) Titular/es: **Compagnie Industrielle et Financière d'Ingénierie "INGENICO"**
92 192 avenue Charles de Gaulle
92200 Neuilly sur Seine, FR

(72) Inventor/es: **Naccache, David**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

1. Campo de la invención

El campo de la invención es la securización de los programas informáticos. La invención se refiere más en particular al control permanente de los programas informáticos y a la detección de los errores o anomalías en estos programas informáticos.

La invención encuentra especial aplicación en los programas informáticos para aplicaciones críticas, por ejemplo en sistemas seguros de pago mediante tarjetas bancarias, en medios de transporte tales como aviones, como también en emplazamientos industriales tales como centrales nucleares.

2. Técnica anterior

Son ya conocidas técnicas de prueba que permiten comprobar un programa informático (o equipo lógico) y poner de manifiesto los eventuales errores o anomalías de funcionamiento (llamados «errores de programa» en español y «bugs» en inglés). A tal efecto, el documento FR2893431 describe la sucesiva utilización de dos tareas de soporte lógico independientes.

Generalmente se aplica un conjunto de muestras de datos de entrada que *a priori* son representativas del uso que se hará del programa y se comprueba que los datos salientes son conformes a los datos esperados por las especificaciones. Una vez terminado el período de prueba del programa informático, el programa informático es «puesto en producción» (instalado, difundido o comercializado) y puede por ejemplo pilotar un dispositivo en el que está integrado.

La presencia de errores de programa en programas informáticos críticos puede tener repercusiones lamentables o graves para el (los) dispositivo(s) que pilotan/verifican. Así, son críticos los programas informáticos utilizados en aplicaciones que necesitan una gran precisión y/o una fuerte seguridad, por ejemplo en los sistemas de transporte (pilotaje de los aviones, señalización ferroviaria, equipo lógico embarcado de automóviles), la producción de energía (control de las centrales nucleares), la salud (aparatos médicos), el ámbito financiero (pago electrónico) o las aplicaciones militares.

Las precauciones que se han de tomar en el desarrollo de un programa informático crítico de este tipo las define generalmente el ordenante, o están fijadas por una norma, cuyas elevadas exigencias dictan probar el programa informático en un gran número de configuraciones con el fin de tender hacia un funcionamiento sin brecha del programa informático crítico. Así, durante el período de prueba del programa informático crítico, se intenta aumentar al máximo el control del programa

informático enviándole el máximo de diferentes secuencias o estímulos posibles. El documento US6629267 describe la utilización de un servidor remoto para actualizar el programa principal que pilota un dispositivo que ha detectado una anomalía.

3. Inconvenientes de la técnica anterior

Sin embargo, es imposible someter a pruebas exhaustivas un programa informático, y en particular un programa informático crítico, en la medida en que el período de prueba a menudo es un compromiso entre el tiempo y la completitud. Además, estas pruebas pueden no cubrir por ejemplo usos atípicos o difícilmente previsibles, o evoluciones de determinados aspectos a lo largo del tiempo. Se entiende que generalmente no es posible cubrir todas las posibilidades y que, cuanto más exhaustiva es la fase de prueba, más larga será, lo que retarda en su tanto la efectiva puesta en práctica del programa.

4. Objetivos de la invención

La invención tiene como objetivo principal subsanar estos inconvenientes de la técnica anterior.

Más precisamente, es un objetivo de la invención mejorar la seguridad de los programas, y en particular de los programas críticos.

Es otro objetivo de la invención permitir reducir la duración de la fase de prueba, sin reducir considerablemente la seguridad del programa.

La invención también tiene como objetivo detectar una eventual anomalía de una manera que sea simple de poner en práctica.

Es otro objetivo de la invención permitir una reacción rápida y eficaz en caso de que se detecte una anomalía en programas de este tipo.

5. Resumen de la invención

Estos objetivos, al igual que otros que posteriormente se harán manifiestos, se logran con la ayuda de un procedimiento de securización en la utilización de un programa informático principal que pilota al menos un dispositivo que recibe y entrega datos.

De acuerdo con la invención, este procedimiento pone en práctica un programa informático secundario de control, diferente de dicho programa principal y apto para entregar los mismos datos de salida que al menos una porción, llamada porción crítica, de dicho programa principal, en presencia de datos de entrada idénticos.

Un procedimiento de securización de este tipo según la invención queda definido por la reivindicación 1.

La invención permite así someter a prueba de manera permanente y sin

bloqueo un programa, particularmente un programa principal que se utiliza para una aplicación crítica, incluso después de su fase de prueba. Para tal fin, la invención pone en práctica un programa de control (prueba) en paralelo con el programa principal, al menos para las porciones críticas de este programa principal. Esta puesta en práctica se efectúa durante la fase de «producción» del programa principal, es decir, cuando por ejemplo el programa principal pilota efectivamente un dispositivo que recibe y entrega datos, tal como por ejemplo un terminal de pago electrónico.

La ejecución en paralelo del programa principal y del programa de control permite la detección de anomalía(s) (error de programa) en el programa principal en cualquier momento en la fase de producción. Así, se puede detectar en todo momento la presencia de una anomalía, cuando los datos salientes de los dos programas son diferentes para los mismos datos entrantes. En caso de discrepancia entre estos datos de salida, se genera una información de anomalía y luego se transmite hacia un servidor remoto sin interrumpir el programa principal.

Dicho de otro modo, la invención permite la comprobación con carácter permanente de un programa principal y la detección de errores de programa, no sólo durante el período de prueba del programa principal, sino también durante el período de producción del programa principal.

La invención es además eficaz, puesto que la comprobación del programa principal está basada en datos de entrada «reales» que pueden no haber sido contemplados en el momento del período de prueba del programa principal porque corresponden, por ejemplo, a un uso atípico. La invención permite por tanto securizar de manera permanente y continua la utilización de un programa informático sin bloquear su ejecución.

La transmisión de información de anomalías hacia un servidor remoto permite señalizar de manera rápida y eficaz eventuales anomalías y, ventajosamente, aportar al programa principal, de manera diferida, los parches necesarios (que se pueden difundir hacia un parque de máquinas, si el mismo programa está puesto en práctica en todas estas máquinas, y no sólo hacia aquélla que ha señalizado la anomalía).

En una forma de realización particular de la invención, la etapa de transmisión comprende la transmisión de un informe que contiene un conjunto de información relativa a dicha anomalía, entre ella dichos datos de entrada y dichos datos de salida, destinado a permitir la identificación del origen de la anomalía y su corrección.

Ello permite determinar más rápidamente el origen de la anomalía y la corrección necesaria.

De acuerdo con una forma de realización ventajosa, el procedimiento comprende una etapa de recepción de información de corrección de dicho programa principal, transmitida por dicho servidor.

Así, la invención permite, como respuesta a la detección de una anomalía, la transmisión de información de corrección mediante un servidor remoto hacia el dispositivo pilotado por el programa principal (y, en su caso, hacia otros dispositivos que utilicen este programa). Así, el dispositivo puede securizar la utilización del programa principal, sin que haya habido una larga interrupción de su funcionamiento.

El procedimiento puede comprender asimismo, complementaria o alternativamente, una etapa de recepción de un mandato de interrupción o de modificación de dicho programa principal, transmitido por dicho servidor.

Así, el servidor puede controlar a distancia la modificación del programa principal del dispositivo o la interrupción del programa principal, si la anomalía detectada lo precisa, o la modificación del comportamiento del programa principal, por ejemplo para que pase a un modo de funcionamiento degradado o seguro, para impedir en particular que la anomalía se reproduzca (por ejemplo impidiendo la utilización de la parte del código que ha generado la anomalía) y/o para subsanar las eventuales consecuencias de la anomalía (por ejemplo bloqueando la tarjeta bancaria que ha generado la anomalía, señalizando la anomalía a un usuario (en particular en un vehículo o en un emplazamiento industrial), y/o reforzando la seguridad del dispositivo, sus equipos o su entorno (en particular para aplicaciones militares o nucleares)).

De acuerdo con otro aspecto, el procedimiento comprende una etapa de almacenamiento de un informe que contiene un conjunto de información relativa a dicha anomalía.

Así, se puede memorizar un informe en el dispositivo pilotado por el programa principal, por ejemplo antes de que las consecuencias de la anomalía lo bloqueen. En tal caso, el dispositivo puede transmitir este informe al servidor remoto en un momento diferido.

La invención se refiere asimismo a un dispositivo que comprende medios de tratamiento de datos, que ejecutan un programa principal y ponen en práctica el procedimiento anteriormente descrito.

Un dispositivo de este tipo queda definido por la reivindicación 6.

De acuerdo con diferentes formas de realización particulares de la invención, un dispositivo de este tipo puede pertenecer en particular al grupo que comprende:

- los terminales lectores de tarjetas inteligentes, en particular los terminales bancarios;
- los servidores de datos, en particular los servidores bancarios;
- los dispositivos de transacciones financieras o bursátiles;
- los dispositivos de control de aplicaciones médicas, en particular de administración de medicamentos;
- los dispositivos de control de un motor;
- los dispositivos de señalización ferroviaria;
- los dispositivos de pilotaje de los aviones;
- los dispositivos embarcados de automóviles;
- los dispositivos de control de emplazamientos industriales, en particular de producción de energía (por ejemplo centrales nucleares);
- los dispositivos de telecomunicaciones;
- los dispositivos puestos en práctica en las aplicaciones militares.

La invención se refiere asimismo a un procedimiento de actualización de un programa principal que pilota al menos un dispositivo que recibe y entrega datos, que pone en práctica el procedimiento de securización de la invención, tal como queda definido por la reivindicación 8.

Como se ha explicado más arriba, en efecto el planteamiento de la invención permite corregir o actualizar, de manera simple y eficaz, un programa principal de este tipo, tan pronto como haya sido detectada una anomalía por el programa de control, aunque este programa principal se encuentre en fase de producción.

De acuerdo con una forma de realización ventajosa, dicho parche es transmitido simultáneamente a un conjunto de dispositivos que ponen en práctica dicho programa principal.

Ello permite corregir un programa principal simultáneamente en varios dispositivos que ponen en práctica el mismo programa principal.

La invención se refiere asimismo a un servidor de actualización de un programa principal que pilota al menos un dispositivo que recibe y entrega datos, que pone en práctica el procedimiento de securización de la invención, tal como queda definido por la reivindicación 10.

6. Lista de figuras

Otras características y ventajas de la invención se harán más claramente manifiestas con la lectura de la descripción que sigue de una forma de realización preferente, dada a título de mero ejemplo ilustrativo y no limitativo, y de los dibujos que

se acompañan, en los que:

La figura 1 ilustra esquemáticamente un ejemplo de sistema en el que está puesta en práctica la invención;

la figura 2 presenta las etapas principales de un procedimiento de securización según una forma de realización de la invención, adaptado al sistema de la figura 1; y

la figura 3 presenta las etapas principales de un procedimiento de actualización según una forma de realización de la invención, adaptado al sistema de la figura 1.

7. Descripción de una forma de realización de la invención

El principio general de la invención se basa en un control permanente y no bloqueador de un programa informático, llamado programa principal. Este control se efectúa durante la «fase de producción» del programa principal, es decir, después de una fase convencional de prueba, cuando por el ejemplo el programa principal pilota un dispositivo que recibe y entrega datos.

Para tal fin, se ejecuta un programa de control en paralelo con un programa principal, al menos durante la ejecución de las porciones críticas del programa principal. Ello permite la detección de anomalía(s) en el programa principal, mediante comparación de los resultados (salidas) de los dos programas. Más precisamente, se detecta la presencia de una anomalía cuando los datos salientes de los dos programas son diferentes para los mismos datos entrantes. En caso de discrepancia entre estos datos de salida, es generada una información de anomalía y luego transmitida hacia un servidor remoto, sin interrumpir el programa principal y, por tanto, de manera transparente para los usuarios.

La figura 1 ilustra esquemáticamente un ejemplo de sistema en el que está puesta en práctica la invención. El sistema ilustrado comprende varios dispositivos D1 a Dn que pueden ser utilizados cada uno de ellos en una aplicación crítica. El dispositivo D1, por ejemplo, puede ser un terminal lector de tarjetas inteligentes (por ejemplo un terminal bancario), un servidor de datos (por ejemplo un servidor bancario), un dispositivo de control de aplicaciones médicas (en particular, de administración de medicamentos) o un dispositivo de control de un motor.

El dispositivo D1 comprende medios de tratamiento de datos, medios para recibir datos de entrada 20 y medios para entregar datos de salida 30. De manera convencional, los medios de tratamiento de datos del dispositivo D1 comprenden medios de puesta en práctica de un programa informático principal 11 que comprende

una o varias porciones críticas, es decir, porciones críticas de código y/o porciones que manejan información crítica.

De conformidad con la invención, los medios de tratamiento del dispositivo D1 también comprenden medios de puesta en práctica de un programa informático secundario de control 12. El programa secundario de control 12 es diferente del programa principal 11, pero es apto para entregar los mismos datos de salida que las porciones críticas del programa principal 11, en presencia de idénticos datos de entrada. Dicho de otro modo, el programa secundario de control 12 comprende elementos en principio idénticos a las porciones críticas del programa principal 11.

El programa principal 11 ha sido generado, por ejemplo, por un primer compilador, a partir de un código fuente y de especificaciones dadas. Por su parte, el programa de control 12 puede haber sido desarrollado directamente por un programador, o generado por un segundo compilador, distinto del primero.

La puesta en práctica del programa de control 12 permite someter a prueba y securizar las porciones críticas del programa principal 11 de manera acorde con el procedimiento de securización de la invención, cuyas principales etapas quedan detalladas en la figura 2.

Se supone en el presente caso que el programa principal 11 es ejecutado por los medios de tratamiento del dispositivo D1 y que, en primer lugar, se ejecuta una porción no crítica, en la etapa 100. Cuando se activa una porción crítica del programa principal, el procedimiento de la invención pone en práctica una etapa 102 de ejecución de la porción crítica del programa principal mediante los medios de tratamiento de datos del dispositivo D1, que entrega primeros datos de salida 31 en función de datos de entrada 20. El procedimiento de securización de la invención pone en práctica, simultánea o secuencialmente, una etapa 104 de ejecución de la misma porción crítica mediante el programa de control 12, que entrega segundos datos de salida 32 en función de los mismos datos de entrada 20. Para tal fin, el programa principal 11 puede transmitir al programa de control 12 una información 33 que indica la parte crítica del programa principal 11 que es ejecutada en la etapa 102.

El programa de control efectúa los mismos tratamientos, es decir, se supone que (en ausencia de error de programa) proporciona los mismos datos de salida que el programa principal, en presencia de los mismos datos de entrada. En cambio, estructuralmente es diferente para permitir la detección de esos errores de programa. Por ejemplo, ha sido generado por otro compilador, o escrito por un humano.

A continuación se pone en práctica, en unos medios de comparación 13 de los

medios de tratamiento comprendidos en el dispositivo D1, una etapa 106 de comparación de los primeros y de los segundos datos de salida 31, 32. Se determina entonces si estos primeros y segundos datos de salida 31, 32 son diferentes. En caso de que no existan diferencias entre los datos de salida primeros y segundos 31, 32, la ejecución del programa principal 11 puede proseguir de acuerdo con la etapa 100.

En caso de que los datos de salida primeros y segundos 31, 32 sean diferentes, se genera una información de anomalía 35 a la salida de los medios de comparación 13, de acuerdo con la etapa 108, y el programa principal 11 prosigue, en función de los primeros datos de salida 31. La existencia de una discrepancia entre los datos de salida primeros y segundos 31, 32 puede corresponder en la práctica a una anomalía o error en una porción crítica del programa principal 11 que, preferentemente, no tiene impacto en el funcionamiento del dispositivo D1 o que contribuye a una disfunción menor del dispositivo D1.

En esta forma de realización, la información de anomalía 35 generada en la etapa 108 se puede señalizar inmediatamente a un servidor S remoto, en la etapa 110, por mediación de una red de comunicaciones de las que se conocen. El servidor S puede tratar la información de anomalía 35 de manera inmediata (etapa 112) o eventualmente almacenarla para introducir en ella los parches necesarios en un momento diferido. Cuando el servidor S ha determinado una corrección de la anomalía en la etapa 114, transmite esta corrección al menos al dispositivo D1 en la etapa 116.

En una variante de realización, la etapa 108 comprende la generación de un informe que contiene un conjunto de información relativa a la anomalía, entre ella los datos de entrada 20 y los datos de salida 31, 32, destinado a permitir la identificación rápida del origen de la anomalía y la corrección necesaria. En otra variante de realización, el informe que contiene un conjunto de información relativa a dicha anomalía se puede almacenar en unos medios de memorización del dispositivo D1 y transmitirse en diferido al servidor S remoto (etapa 110).

El procedimiento de securización de la invención puede poner en práctica una etapa de recepción, mediante el dispositivo D1, de información de corrección 40 del programa principal 11, transmitida por el servidor S remoto. Así, el dispositivo D1 puede securizar la utilización del programa principal 11, sin que haya habido una larga interrupción de su funcionamiento.

El procedimiento de securización de la invención puede comprender asimismo, complementaria o alternativamente, una etapa de recepción, por parte del dispositivo D1, de un mandato de interrupción o de modificación (indicado con 41 en la figura 1)

del programa principal 11, transmitido por el servidor S.

Así, el servidor S puede controlar a distancia la modificación del programa principal 11 del dispositivo D1 o la interrupción del programa principal 11, si la anomalía detectada lo precisa, o la modificación del comportamiento del programa principal 11, por ejemplo para que pase a un modo de funcionamiento degradado o seguro, para impedir en particular que la anomalía se reproduzca (por ejemplo impidiendo la utilización de la parte del código que ha generado la anomalía) y/o para subsanar las eventuales consecuencias de la anomalía (por ejemplo bloqueando la tarjeta bancaria que ha generado la anomalía, señalizando la anomalía a un usuario (en particular en un vehículo o en un emplazamiento industrial) y/o reforzando la seguridad del dispositivo, sus equipos o su entorno (en particular para aplicaciones militares o nucleares)).

De acuerdo con el procedimiento de actualización de la invención, cuyas principales etapas se detallan en la figura 3, el servidor S puede corregir o actualizar un programa principal que pilota al menos uno de los dispositivos D1 a Dn tan pronto como haya sido detectada una anomalía por el programa de control de al menos uno de los dispositivos D1 a Dn. El servidor S remoto comprende así medios de recepción de una información de anomalía (etapa 211) emitida por uno de los dispositivos D1 a Dn. El servidor determina, por mediación de medios de tratamiento integrados, una corrección de la anomalía en la etapa 214. Para tal fin, el servidor S analiza la información de anomalía (etapa 214A) y realiza un parche de anomalía (etapa 214B), y luego difunde el parche de anomalía (indicado con 40 en la figura 1) en la etapa 216 hacia el dispositivo que ha emitido la información de anomalía o, simultáneamente, hacia los dispositivos D1 a Dn, si en todos estos dispositivos está puesto en práctica el mismo programa principal.

La técnica que la invención pone en práctica es ventajosa en el sentido de que el control del programa principal 11, que es utilizado para una aplicación crítica, se efectúa de manera permanente y no bloqueadora, incluso después de la fase de prueba del programa principal 11. El control del programa principal 11 se efectúa durante la «fase de producción» del programa principal y se basa de este modo en estímulos que pueden no haber sido contemplados durante el período de prueba. En caso de que se detecte una anomalía en el programa principal 11, la anomalía es transmitida al servidor remoto S, lo que permite una reacción rápida y eficaz para corregir esta anomalía sin bloquear (salvo, en determinadas formas de realización, si la anomalía lo justifica) la ejecución del programa principal 11.

REIVINDICACIONES

1. Procedimiento de securización en la utilización de un programa informático principal (11) que pilota al menos un dispositivo (D1,..., Dn) que recibe y entrega datos,

habiendo sido objeto dicho programa principal (11) de una fase de control durante la cual ha sido sometido a una serie de estímulos con el fin de detectar una eventual anomalía, y hallándose en fase de producción,

poniendo en práctica dicho procedimiento un programa informático secundario de control (12), diferente de dicho programa principal (11) y apto para entregar los mismos datos de salida (30) que al menos una porción, llamada porción crítica, de dicho programa principal (11), en presencia de datos de entrada (20) idénticos,

comprendiendo dicho procedimiento las siguientes etapas, al menos cuando se activa una de dichas porciones críticas de dicho programa principal (11):

- ejecución (102) de dicha porción crítica, que entrega primeros datos de salida (31) en función de datos de entrada (20);
- ejecución (104) de dicho programa de control (12), que entrega segundos datos de salida (32) en función de dichos datos de entrada (20);
- comparación (106) de dichos datos de salida primeros y segundos (31, 32) y generación (108) de una información de anomalía (35), si dichos datos de salida primeros y segundos (31, 32) son diferentes, correspondiendo dichos datos de entrada (20) a un estímulo atípico, no tratado durante dicha fase de prueba,

caracterizado porque el procedimiento comprende además las siguientes etapas:

- transmisión (110) de dicha información de anomalía (35) a un servidor (S) remoto, con vistas a un análisis y a una corrección diferida de dicho programa principal (11);
- prosecución de dicho programa principal (11), de manera transparente para un usuario, en función de dichos primeros datos de salida (31) y pese a la detección de dicha anomalía.

2. Procedimiento de securización según la reivindicación 1, caracterizado porque dicha etapa de transmisión (110) comprende la transmisión de un informe que contiene un conjunto de información relativa a dicha anomalía (35), entre ella dichos datos de entrada (20) y dichos datos de salida (31, 32), destinado a permitir la identificación del origen de la anomalía (35) y su corrección.

3. Procedimiento de securización según una cualquiera de las reivindicaciones 1 y 2, caracterizado porque comprende una etapa de recepción de información de corrección (40) de dicho programa principal (11), transmitida por dicho servidor (S).

4. Procedimiento de securización según una cualquiera de las reivindicaciones 1 a 3, caracterizado porque comprende una etapa de recepción de un mandato de interrupción o de modificación (41) de dicho programa principal (11), transmitido por dicho servidor (S).

5. Procedimiento de securización según una cualquiera de las reivindicaciones 1 a 4, caracterizado porque comprende una etapa de almacenamiento de un informe que contiene un conjunto de información relativa a dicha anomalía.

6. Dispositivo (D1,..., Dn) que comprende medios de tratamiento de datos, que entrega unos datos de salida (30) en función de datos de entrada (20), comprendiendo dichos medios de tratamiento unos medios de puesta en práctica de un programa informático principal (11), habiendo sido objeto dicho programa principal (11) de una fase de control durante la cual ha sido sometido a una serie de estímulos con el fin de detectar una eventual anomalía, y hallándose en fase de producción,

y unos medios de puesta en práctica de un programa informático secundario de control (12), diferente de dicho programa principal (11) y apto para entregar los mismos datos de salida (30) que al menos una porción, llamada porción crítica, de dicho programa principal (11), en presencia de datos de entrada (20) idénticos,

poniendo en práctica dicho dispositivo (D1,..., Dn), al menos cuando se activa, una de dichas porciones críticas de dicho programa principal (11):

- unos medios de ejecución de al menos una de dichas porciones críticas de dicho programa principal (11), que entregan primeros datos de salida (31) en función de datos de entrada (20);
- unos medios de ejecución de dicho programa de control (12), que entregan segundos datos de salida (32) en función de dichos datos de entrada (20);
- unos medios de comparación (13) de dichos datos de salida primeros y segundos (31, 32) y de generación de una información de anomalía (35), si dichos datos de salida primeros y segundos (31, 32) son diferentes, correspondiendo dichos datos de entrada (20) a un estímulo atípico, no tratado durante dicha fase de prueba,

caracterizado porque comprende:

- medios de transmisión de dicha información de anomalía (35) a un servidor (S) remoto, con vistas a un análisis y a una corrección diferida de dicho programa principal (11);

y porque dichos medios de ejecución de dicho programa principal (11) prosiguen su tratamiento, de manera transparente para un usuario, en función de dichos primeros datos de salida (31) y pese a la detección de dicha anomalía.

7. Dispositivo según la reivindicación 6, caracterizado porque pertenece al grupo que comprende:

- los terminales lectores de tarjetas inteligentes, en particular los terminales bancarios;
- los servidores de datos, en particular los servidores bancarios;
- los dispositivos de transacciones financieras o bursátiles;
- los dispositivos de control de aplicaciones médicas, en particular de administración de medicamentos;
- los dispositivos de control de un motor;
- los dispositivos de señalización ferroviaria;
- los dispositivos de pilotaje de los aviones;
- los dispositivos embarcados de automóviles;
- los dispositivos de control de emplazamientos industriales, en particular de producción de energía (por ejemplo centrales nucleares);
- los dispositivos de telecomunicaciones;
- los dispositivos puestos en práctica en las aplicaciones militares.

8. Procedimiento de actualización, por un servidor remoto (S), de un programa principal (11) que pilota al menos un dispositivo (D1,..., Dn) que recibe y entrega datos, poniendo en práctica dicho dispositivo (D1,..., Dn) el procedimiento de securización de una cualquiera de las reivindicaciones 1 a 5,

caracterizado porque comprende las siguientes etapas, ejecutadas por el servidor remoto:

- recepción de la información de anomalía (211), emitida por uno de dichos dispositivos (D1,..., Dn), cuando los primeros datos (31), entregados por el programa principal (11) en presencia de datos de entrada (20) particulares, difieren de los segundos datos de salida (32) entregados por el programa de control (12);

- análisis de dicha anomalía (214A) y realización de un parche (214B); y
- transmisión de dicho parche (216) hacia dicho dispositivo emisor de dicha información de anomalía.

9. Procedimiento de actualización según la reivindicación 8, caracterizado porque dicho parche (40) es transmitido simultáneamente de dicho servidor remoto (S) a un conjunto de dispositivos (D1,..., Dn) que ponen en práctica dicho programa principal (11).

10. Servidor (S) de actualización de un programa principal (11) que pilota al menos un dispositivo (D1,..., Dn) que recibe y entrega datos, poniendo en práctica dicho dispositivo el procedimiento de securización de una cualquiera de las reivindicaciones 1 a 5,

caracterizado porque dicho servidor (S) comprende:

- medios de recepción de la información de anomalía (35), emitida por uno de dichos dispositivos (D1,..., Dn), cuando los primeros datos (31), entregados por el programa principal (11) en presencia de datos de entrada (20) particulares, difieren de los segundos datos de salida (32) entregados por el programa de control (12);
- medios de análisis de dicha anomalía (35) y de realización de un parche (40); y
- medios de transmisión de dicho parche (40) a dicho dispositivo (D1,..., Dn) emisor de dicha información de anomalía.

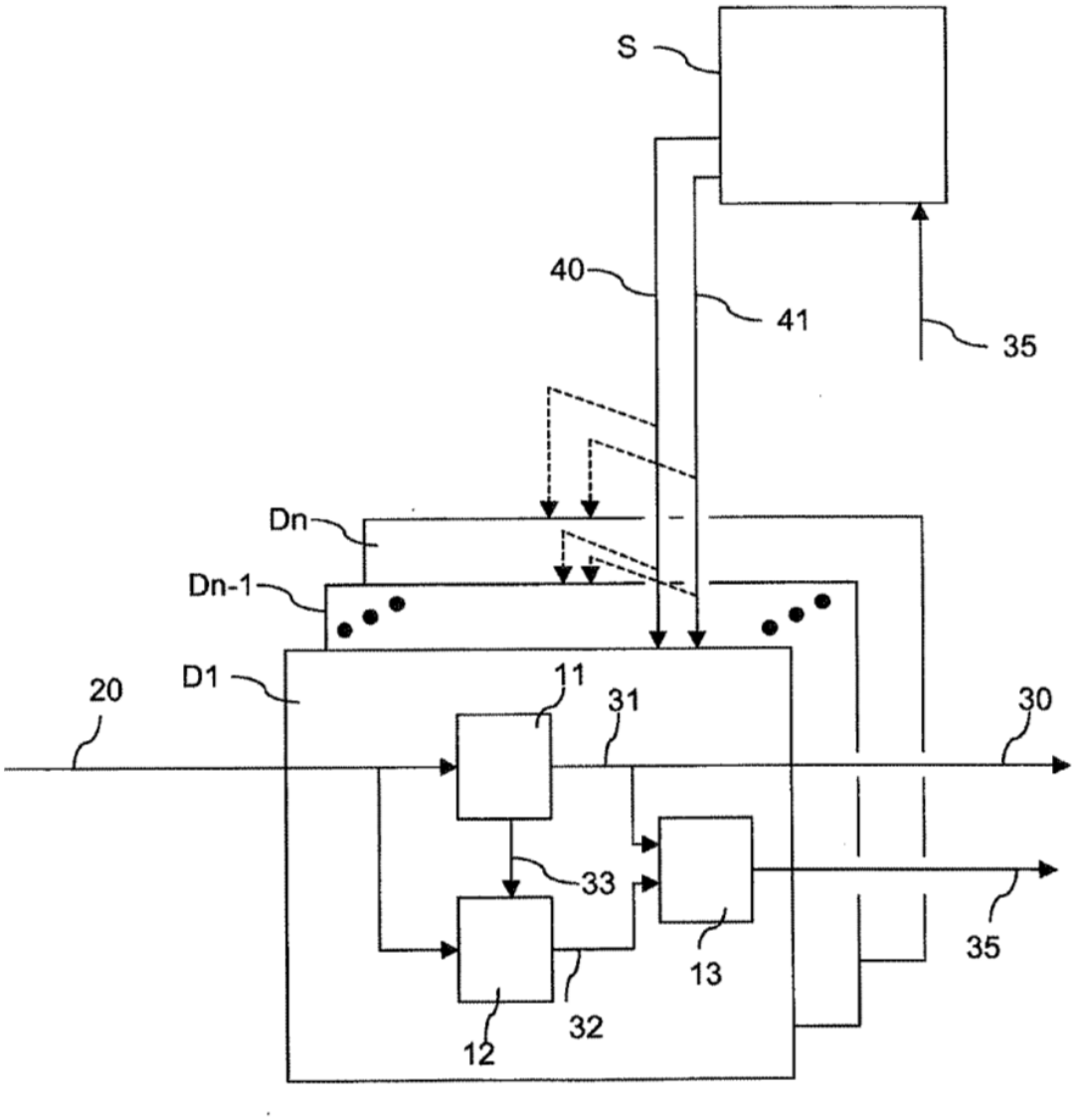

Figura 1

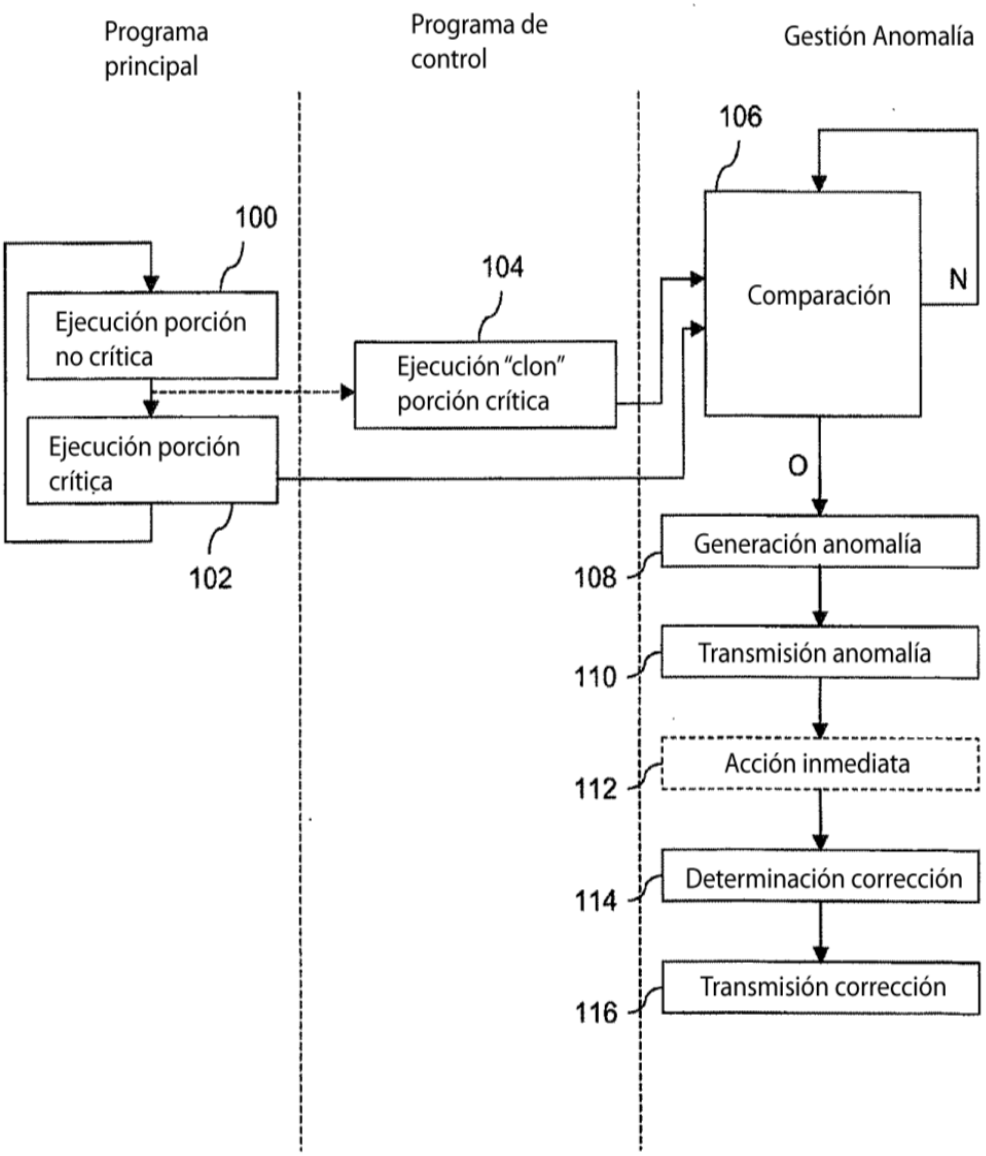
Programa principal
Programa de control
Gestión Anomalía
100
Ejecución porción no crítica
Ejecución porción crítica
102
104
Ejecución "clon" porción crítica
106
Comparación
N
O
108
Generación anomalía
110
Transmisión anomalía
112
Acción inmediata
114
Determinación corrección
116
Transmisión corrección

Figura 2

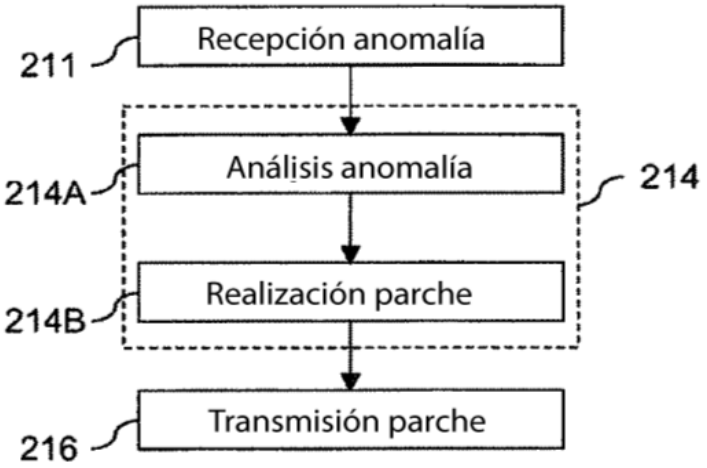
211
Recepción anomalía
214A
Análisis anomalía
214
214B
Realización parche
216
Transmisión parche

Figura 3