(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 606 693**

(51) Int. CI.:

G06F 1/10 (2006.01)
G01R 31/3185 (2006.01)
G01R 31/317 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.08.2014 E 14179703 (5)**

(97) Fecha y número de publicación de la concesión europea: **07.09.2016 EP 2983059**

(54) Título: **Dispositivo de protección contra fallas en circuitos de árbol de reloj**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.03.2017

(73) Titular/es:

WINBOND ELECTRONICS CORP. (100.0%)
No. 8, Keya 1st Road, Daya District
Taichung City 428, TW

(72) Inventor/es:

TASHER, NIR

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Dispositivo de protección contra fallas en circuitos de árbol de reloj

Campo técnico

La presente invención se refiere en general a un circuito electrónico digital y en particular a los métodos y sistemas de protección de fallas en circuitos de árbol de reloj.

Antecedentes de la invención

Se utilizan diferentes técnicas para acceder, analizar o extraer información de un circuito electrónico seguro, tal como un circuito criptográfico. Algunos ataques, denominados como inyección de falla, normalmente implica provocar una falla en el circuito, por ejemplo, al hacer contacto físico o dañar líneas de señales, mediante la aplicación de láser de alta potencia o pulsos electromagnéticos, o al provocar impulsos de ruido en el suministro de energía u otras interfaces externas. Se espera que la falla provoque que el circuito genere información sensible, o de lo contrario ayude a que el atacante penetre el circuito o se almacene la información.

Un ejemplo para un circuito de distribución de reloj se divulga en el documento US 2008/284483 A1. El circuito tiene una pluralidad de reguladores. El circuito tiene etapas plurales de reguladores dispuestas a lo largo de trayectorias de ramificación para dividir una señal de reloj y está configurada de tal manera que las salidas de una pluralidad de reguladores en una etapa final y/o una etapa intermedia que están en cortocircuito, se incluye en relación con por lo menos un regulador de una pluralidad de reguladores en la misma etapa sobre una ruta de ramificación, un selector para la recepción de una salida de un regulador adyacente ubicado hacia la red en términos de conectar una cadena a lo largo de la cual se conecta la pluralidad de reguladores en prueba, y una señal en un nodo de ramificación que corresponde a por lo menos un regulador mediante una primera entrada y una segunda entrada respectivamente, selecciona uno de la primera entrada y la segunda entrada en funciona de una señal de control seleccionada, y suministrando la entrada seleccionada a un regulador.

Resumen de la invención

La presente invención se define mediante el circuito integrado (CI) de la reivindicación 1 y el método de la reivindicación 6. En las reivindicaciones dependientes se definen características adicionales.

Una realización de la presente invención que se describe aquí proporciona un circuito integrado (CI) que incluye circuitos de árbol de reloj y circuitos de protección. El circuito de árbol de reloj se configura para distribuir una señal de reloj a través del CI. El circuito de protección se registra por varias instancias de la señal de reloj que se muestrean en múltiples puntos de muestreo en el circuito de árbol de reloj y se configura para detectar una falla en el circuito de árbol de reloj en respuesta a una anomalía en uno o más de las instancias de señal de reloj.

En algunas realizaciones, el circuito de protección incluye una cascada de etapas de lógica que se registran por las instancias respectivas de señal de reloj y un detector que está configurado para detectar la falla al identificar en una salida de la cascada una desviación de una salida prevista. En una realización, las etapas de lógica incluyen biestables respectivos (FF). En una realización divulgada, la cascada de etapas de lógica se configura para generar un patrón alterno de valores lógicos, y el detector se configura para identificar la desviación del patrón alternante.

En una realización, el detector se configura para descartar desviaciones en la salida de la cascada que se producen dentro de un intervalo predefinido después de inicialización. En una realización alternativa, el circuito de protección se configura para inicializar las etapas de lógica de la cascada para producir inicialmente la salida esperada. En algunas realizaciones, en respuesta a la detección de falla, el circuito de protección se puede configurar para emitir una alerta o actuar sobre la falla detectada.

Se proporciona adicionalmente, según una realización de la presente invención, un método que incluye distribuir una señal de reloj a través de un circuito integrado (CI) utilizando un circuito de árbol de reloj. Varias instancias de la señal de reloj se muestrean a múltiples puntos de muestreo respectivos en el circuito de árbol de reloj. El circuito de protección se registra por las instancias múltiples de la señal de reloj. Se detecta una falla en el circuito de árbol de reloj, utilizando el circuito de protección, en respuesta a una anomalía en una o más de instancias de la señal de reloj.

La presente invención se comprenderá más completamente a partir de la siguiente descripción detallada de las realizaciones de la misma, tomada junto con los dibujos en los que:

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que ilustra esquemáticamente un circuito integrado (CI) que comprende el circuito de protección de árbol de reloj, de acuerdo con una realización de la presente invención; y

La figura 2 es un diagrama de flujo que ilustra esquemáticamente un método para la protección de falla de árbol de reloj, de acuerdo con una realización de la presente invención.

Descripción detallada de las realizaciones

Resumen

Realizaciones que se describen en el presente documento proporcionan mejores métodos y sistemas para detección de fallas en circuitos de árbol de reloj de circuito integrado (CI). En las realizaciones divulgadas, un CI comprende circuitos de árbol de reloj (también conocido como "árbol del reloj" por abreviar) que distribuye una señal de reloj de una fuente de reloj a diferentes unidades de hardware a través del CI. El circuito de árbol de reloj normalmente comprende circuito que abarcan grandes porciones del CI, así como los componentes activos como amplificadores, reguladores, enganches y/o inversores.

En algunos casos, el árbol de reloj puede ser objeto de ataques de falla que intentan analizar la funcionalidad de CI u obtener acceso a información almacenada en el CI, por ejemplo. Un ataque de falla por lo general aplica alguna anomalía constante o temporal en el árbol de reloj, en un intento de forzar el CI en un estado anormal que evade sus mecanismos de protección. Aunque la descripción que sigue se centra en ataques de falla, las técnicas reveladas también se pueden utilizar para detectar fallas que no son ocasiones por los ataques.

En algunas realizaciones, el CI consta de circuitos de protección que detectan, alertan y posiblemente actúan sobre ataques de falla en el árbol de reloj. El circuito de protección es registrado mediante múltiples instancias de señal de reloj, que se muestrean en múltiples puntos de muestreo en el árbol de reloj, e identifica una falla en el árbol de reloj mediante la detección de una anomalía en una o más instancias de la señal de reloj.

En una realización de ejemplo, el circuito de protección comprende una cascada de etapas biestables (FF) cuyas entradas de reloj se registran por las instancias respectivas de la señal de reloj. La primera etapa FF que tiene su salida negada se devuelve a su entrada. Bajo condiciones normales, la salida de la cascada es un patrón alterno "1010101010...". Cualquier desviación de este patrón indica una anomalía en una o más de las entradas de reloj de las etapas de FF, es decir, en uno o más de los casos muestreados de la señal de reloj. El circuito de procesamiento se compone de un detector, que detecta fallas en el árbol de reloj mediante la identificación de las desviaciones del patrón "101010..." esperado en la salida de la cascada. En realizaciones alternativas, también se pueden utilizar otros patrones adecuados (por ejemplo, un patrón seudoaleatorio aun predecible).

La técnica divulgada es altamente eficaz y sensible en la detección de diversos tipos de ataques de falla en el circuito de árbol de reloj. Al mismo tiempo, el circuito de protección es pequeño y fácil de implementar.

Descripción del sistema

La figura 1 es un diagrama de bloques que ilustra esquemáticamente un circuito 20 integrado (CI) que comprende un circuito de protección de árbol de reloj, conforme a una realización de la presente invención. El CI 20 puede abarcar, por ejemplo, un microprocesador, un dispositivo de memoria, un CI específico de aplicación (ASIC) personalizado, una matriz de puertas programables sobre el terreno (FPGA) o cualquier otro tipo adecuado de CI.

El CI 20 consta de un árbol 24 de reloj, que distribuye una señal de reloj de una fuente 28 de reloj hardware 40 funcional a través del CI. El árbol 24 de reloj comprende rastros 32 conductores, así como componentes 36 activos tales como amplificadores, reguladores, enganches o inversores. El Hardware 40 puede abarcar cualquier número adecuado y tipos de unidades funcionales, que se distribuyen sobre el área del CI 20 como se desee. Como tal, el árbol 24 de reloj puede abarcar gran parte de la zona de CI, o incluso todo el CI.

El principio del árbol de reloj, en la fuente de reloj, se conoce como raíz. De la raíz hacia el hardware funcional, el circuito de árbol de reloj se divide en varias ramificaciones. Los bordes de las ramificaciones, que conducen el hardware funcional, se denominan hojas.

El ejemplo de la figura 1 se refiere a una señal de reloj individual y un árbol de reloj individual, por motivos de claridad. El CI de la vida real a menudo contiene múltiples árboles de reloj que distribuyen múltiples señales de reloj. También, las técnicas descritas se pueden aplicar en forma similar en dichos CI.

Protección contra fallas de árbol de reloj

En algunas realizaciones, el CI 20 consta de circuitos de protección para detectar fallas en el árbol de reloj, como errores provocado por ataques de fallas hostiles. Tal ataque puede abarcar, por ejemplo, cortar el árbol de reloj en uno o más puntos, inyectar un impulso de ruido de voltaje en algún punto o puntos en el árbol de reloj, obligando a un voltaje fijo o tierra en algún punto o puntos en el árbol de reloj, o cualquier otro tipo de manipulación o anomalía.

En el presente ejemplo, el circuito de protección de CI 20 consta de un registro 44 de cambio, que comprende varias etapas en la cascada 52 biestables (FF) y un detector 48. Varias líneas 56 de muestreo extraen varias instancias de la señal de reloj desde múltiples puntos de muestreo correspondientes a través de árbol 24 de reloj. Las instancias múltiples de la señal de reloj se dirigen al registro 44 de cambio y accionan las entradas de reloj respectivas de las etapas 52 FF. Se denota el número de etapas FF y el número de casos de la señal de reloj, N.

En otras palabras, cada etapa de 52 FF es registrada por una instancia respectiva de la señal de reloj, que se extrae de un punto de muestreo respectivo de árbol 24 de reloj. Instancias de la señal de reloj pueden ser muestreadas en la raíz, en las hojas o en cualquier ramificación intermedia del árbol de reloj. Se puede elegir el número y las localizaciones de los puntos de muestreo según se desee, por ejemplo, al azar, o para proteger unidades específicas de hardware o funciones en el CI.

La primera etapa FF en el registro de cambio (la etapa más a la izquierda en la figura) tiene su salida negada (*Q*) devuelta a su entrada (D). La salida (Q) de cada etapa FF activa la entrada (D) de la siguiente etapa, y la salida de la última etapa FF sirve como salida de la cascada.

Bajo condiciones normales de estado estable, la señal en la salida de la cascada alterna entre "1" y "0" a la velocidad de la señal de reloj. Condiciones de estado estacionario se alcanzan por lo general en ciclos de reloj de N después de reiniciar o inicialización, ya que los estados iniciales de las etapas FF son impredecibles, y ciclos de N son necesarios para que la alteración del patrón “1010101010..." se propaguen hacia la salida. En una realización alternativa, los estados iniciales de las etapas 52 FF se pueden establecer en la inicialización del sistema a valores conocidos que ya corresponden al patrón esperado. En el presente ejemplo, etapas FF de orden par se pueden restablecer a Lógica '0' y etapas FF de orden impar se pueden restablecer a lógica '1'.

Si ocurre una falla en algún punto o puntos en el árbol de reloj, por ejemplo, como resultado de un ataque, una o más se las instancias de señal de reloj exhibirán algunas anomalías. Por ejemplo, una o más instancias de la señal de reloj pueden ser apagadas (posiblemente indicando que fue cortado el árbol de reloj), una o más instancias de la señal de reloj se pueden pegar en alguna tensión fija o tierra, o se puede encontrar un impulso de ruido transitorio en una o más instancias de la señal de reloj. Alternativamente, se puede mostrar cualquier otra anomalía adecuada en una o más instancias de la señal de reloj.

Una anomalía en una instancia determinada de la señal del reloj provoca anomalías en temporizar la etapa 52 FF respectiva en el circuito de protección. Como resultado, la salida del registro 44 de cambio se desviará del patrón esperado "10101010...”.

En algunas realizaciones, el detector 48 monitorea la salida del registro 44 de cambio y comprobar las desviaciones del patrón esperado "10101010...". El detector también normalmente proporciona la señal de reinicio de CI, con el fin de descartar el intervalo inicial de N ciclos después de reiniciar o inicialización, durante la cual el cambio de registro de salida legítimamente se desvía del patrón esperado.

En respuesta a la detección de una desviación del patrón esperado, el detector 48 normalmente activa una alerta de falla. El circuito de protección CI puede tomar varias acciones en respuesta a una alerta de falla, tales como apagar porciones del CI, borrar ciertos datos del CI, emitir una alerta externa, o cualquier otra acción adecuada.

Las configuraciones de CI 20 y en particular el circuito de protección que se muestra en la figura 1 son configuraciones de ejemplo que se describen solamente por motivos de claridad conceptual. En realizaciones alternativas, se puede utilizar cualquier otra configuración de circuitos de protección y/o CI adecuados. Por ejemplo, el circuito de protección puede abarcar cualquier otro circuito adecuado que es registrado por las instancias múltiples de la señal de reloj, y cuya salida es la indicadora de la presencia o ausencia de fallas en el árbol de reloj. Dependiendo del diseño específico del circuito de protección, el patrón esperado puede tener cualquier otro formato apropiado. Por ejemplo, el patrón puede abarcar un patrón seudoaleatorio, pero predecible.

La figura 2 es un diagrama de flujo que ilustra esquemáticamente un método para la protección de falla de árbol de reloj, según una realización de la presente invención. El método comienza con la extracción de varias instancias de señal de reloj de múltiples puntos de muestreo en árbol 24 de reloj, según la etapa 60 de muestreo de reloj. Las instancias de señal de reloj extraídas activan las entradas de reloj de etapas 52 FF respectivas del registro 44 de cambio, en una etapa 64 de temporización.

El detector de 48 revisa si la salida del registro 44 de cambio se desvía desde el patrón esperado "10101010...", a una etapa 68 de revisión. Si no es así, el método regresa a la etapa 60 anterior. Si se encuentra una desviación, el detector 48 emite una alerta de falla, a una etapa 72 de detección de falla.

Se apreciará que las realizaciones descritas anteriormente se citan a modo de ejemplo, y que la presente invención no se limita a lo que se ha demostrado particularmente y descrito anteriormente.

REIVINDICACIONES

1. Un circuito (20) integrado "CI", que comprende:

Un circuito (24) de árbol de reloj configurado para distribuir una señal de reloj en el circuito (20) integrado; y

un circuito de protección registrado por varias instancias de la señal de reloj que se muestrean en múltiples puntos de muestreo en el circuito (24) árbol de reloj, en la que el circuito (20) integrado se caracteriza porque:

El circuito de protección se configura para detectar una falla en el circuito (24) árbol de reloj en respuesta a una anomalía en una o más de las instancias de la señal de reloj; y

El circuito de protección comprende una cascada de etapas (52) de lógica que se registran por las instancias respectivas de la señal de reloj y un detector (48) que está configurado para detectar la falla al identificar una desviación en la salida de la cascada desde una salida esperada.

2. El CI de acuerdo con la reivindicación 1, en el que las etapas de lógica comprenden biestables "FF" respectivos.

3. El CI de acuerdo con la reivindicación 1, en el que la cascada de etapas de lógica se configura para generar un patrón alterno de valores lógicos, y en el que el detector se configura para identificar la desviación del patrón alterno.

4. El CI de acuerdo con la reivindicación 1, en el que el detector está configurado para descartar desviaciones en la salida de la cascada que se producen dentro de un intervalo predefinido después de inicialización.

5. El CI de acuerdo con la reivindicación 1, en el que el circuito de protección se configura para inicializar etapas de lógica de la cascada para producir inicialmente la salida esperada.

6. Un método de distribución de una señal de reloj a través de un circuito integrado “CI” (20) que utiliza circuitos (24) de árbol de reloj;

instancias de múltiples muestreos de la señal de reloj en múltiples puntos de muestreo respectivos en el circuito (24) de árbol de reloj; y

temporizar circuitos de protección mediante múltiples instancias de señal de reloj; en el que el método se caracteriza porque:

se utiliza el circuito de protección, detectando una falla en el circuito (24) de árbol de reloj en respuesta a una anomalía en una o más de las instancias de la señal de reloj,

en el que el circuito de protección comprende una cascada de etapas (52) de lógica y un detector (48), en el que la temporización del circuito de protección comprende temporizar las etapas de lógica utilizando las instancias respectivas de señal de reloj, y en donde detectar la falla comprende identificar en una salida de la cascada una desviación de una salida esperada.

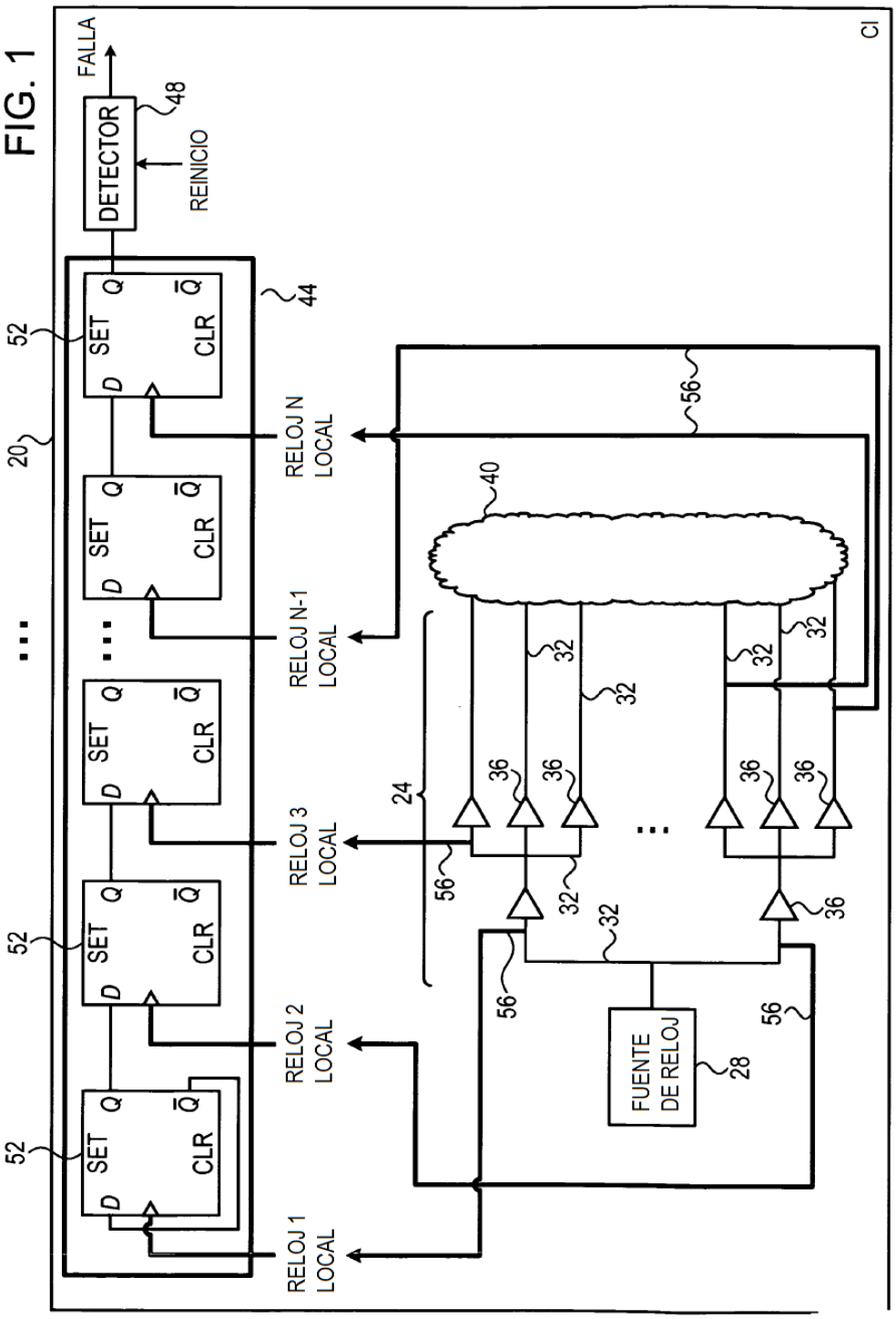
7. El método de acuerdo con la reivindicación 6, en el que las etapas de lógica comprenden biestables "FF" respectivos.

8. El método de acuerdo con la reivindicación 6, en el que temporizar los circuitos de protección comprende generar un patrón alterno de valores lógicos, y en donde detectar la falla comprende identificar la desviación del patrón alterno.

9. El método de acuerdo con la reivindicación 6, en el que identificar la desviación comprende no tener en cuenta las desviaciones en la salida de la cascada que ocurren dentro de un intervalo predefinido después de inicialización.

10. El método de acuerdo la reivindicación 6, en el que identificar la desviación comprende inicializar las etapas de lógica de la cascada con el fin de producir inicialmente la salida esperada.

FIG. 1


CI
FALLA
DETECTOR
48
REINICIO
44
20
52
SET
CLR
D
Q
RELOJ N LOCAL
RELOJ N-1 LOCAL
RELOJ 3 LOCAL
RELOJ 2 LOCAL
RELOJ 1 LOCAL
40
24
32
36
56
FUENTE DE RELOJ
28

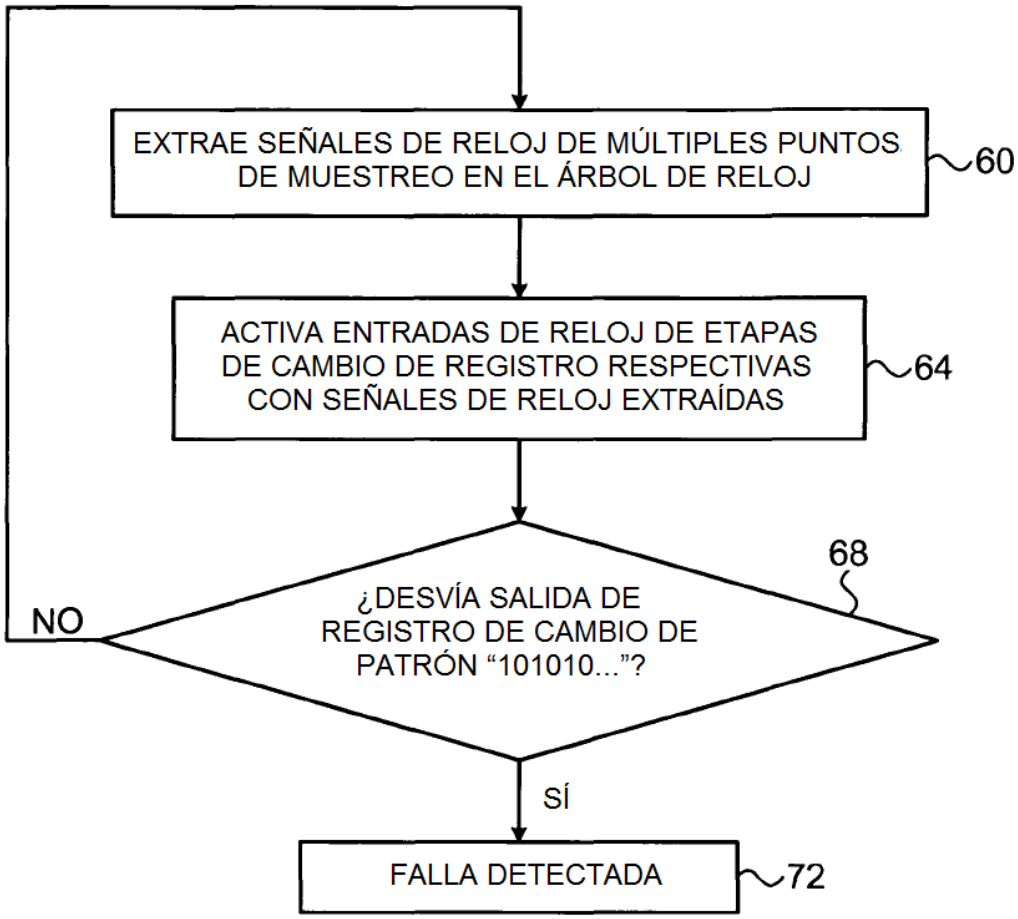

EXTRAE SEÑALES DE RELOJ DE MÚLTIPLES PUNTOS DE MUESTREO EN EL ÁRBOL DE RELOJ
60
ACTIVA ENTRADAS DE RELOJ DE ETAPAS DE CAMBIO DE REGISTRO RESPECTIVAS CON SEÑALES DE RELOJ EXTRAÍDAS
64
68
¿DESVÍA SALIDA DE REGISTRO DE CAMBIO DE PATRÓN “101010...”?
NO
SÍ
FALLA DETECTADA
72

FIG. 2