

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 981 578**

51 Int. Cl.:

G01R 31/28 (2006.01)
G01R 31/317 (2006.01)
G01R 31/30 (2006.01)
G01R 19/165 (2006.01)
G01R 19/25 (2006.01)
G01R 19/30 (2006.01)
G06F 21/75 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **04.08.2014** **E 14179710 (0)**

97 Fecha y número de publicación de la concesión europea: **08.05.2024** **EP 2982997**

54 Título: **Método y aparato para la detección de fallos de tensión de alimentación en un dispositivo de circuito integrado monolítico**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2024

73 Titular/es:

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

72 Inventor/es:

TASHER, NIR;
TEPER, VALERY;
CHENG, DENNIS CHIN y
HUANG, KOYING

74 Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

ES 2 981 578 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método y aparato para la detección de fallos de tensión de alimentación en un dispositivo de circuito integrado monolítico

Antecedentes de la invención

Campo de la Invención

5

La presente invención se refiere a la detección del funcionamiento fuera de especificación de dispositivos de circuitos integrados monolíticos, y más concretamente a la detección de fallos de tensión de alimentación en dispositivos de circuitos integrados monolíticos.

Descripción de la técnica relacionada

10

Algunos tipos de dispositivos de circuitos integrados monolíticos contienen uno o varios circuitos analógicos de detección que supervisan las condiciones de funcionamiento del dispositivo como, por ejemplo, las tensiones de alimentación o internas, la temperatura y la frecuencia de reloj, para detectar cuándo el dispositivo funciona fuera de unos márgenes específicos. Cuando se detecta una condición fuera de especificación de este tipo, el circuito de detección analógica hace que el dispositivo de silicio monolítico se coloque en un estado, como el apagado o el reinicio, que evite el funcionamiento incorrecto del dispositivo o daños al dispositivo o al sistema en el que se utiliza el dispositivo.

15

Establecer los márgenes de las condiciones de funcionamiento es un reto, ya que el circuito de detección puede dispararse en falso si los márgenes son demasiado estrechos, y puede volverse demasiado insensible si los márgenes son demasiado amplios.

20

Es conveniente mejorar la supervisión de las condiciones de funcionamiento de los circuitos de detección de dispositivos para reducir el riesgo de falsos disparos, por un lado, y de falta de capacidad de respuesta, por otro.

US 2011/074398 A1 divulga un módulo de monitorización y control que está configurado para monitorizar los eventos de estatismo durante la etapa de depuración, una etapa de caracterización y/o durante el funcionamiento normal del CI.

25

US 2003/ 226082 A1 se describe un circuito de detección de fallos de tensión que incluye un comparador de tensión para detectar un fallo comparando una tensión de referencia con una tensión de detección de fallos.

US 7 003 412 B1 divulga un método para determinar las condiciones de sobretensión o subtensión mediante la comparación de una tensión de alimentación con una tensión de referencia en un comparador.

30

DE 101 20 147 A1 desvela un circuito para detectar fallos de tensión cortos comparando una primera entrada con una segunda entrada en un comparador.

EP 0 568 440 A1 desvela un circuito para detectar una lectura incorrecta determinando si la tensión de alimentación introducida se encuentra o no dentro del intervalo definido

35

US 2006/214672 A1 divulga un circuito para detectar el ruido de la fuente de alimentación mediante la comparación de la tensión de un conducto de alimentación con la tensión de un conducto de alimentación de referencia.

US 2006/033486 A1 divulga un circuito para detectar un voltaje transitorio comparando un voltaje transitorio con un voltaje umbral para un sistema electrónico.

40

EP 1 804 199 A1 divulga un circuito electrónico para detectar interferencias accidentales o deliberadas comparando una tensión de alimentación del sistema con una tensión umbral en la alimentación del circuito electrónico.

Por fin, WO 2006/114727 A1 divulga un sistema de supervisión de la tensión de alimentación distribuida para detectar la diafonía, o el ruido de alimentación, etc., comparando una medición de la tensión de alimentación actual con un valor medio de la tensión de alimentación producido por un filtro y un convertidor digital-analógico.

45

Breve descripción de la invención

La presente invención se dirige a un método para detectar un fallo de acuerdo con la reivindicación 1 y a un dispositivo de circuito integrado monolítico de acuerdo con la reivindicación 7. Las realizaciones de la invención se describen en las reivindicaciones dependientes.

50

Breve descripción de las distintas vistas de los dibujos

La FIGURA 1 es un diagrama esquemático de bloques de varias señales asociadas a un detector de fallos de tensión de alimentación adaptativo ilustrativo.

La FIGURA 2 es una tabla que muestra niveles ilustrativos de tensión umbral y ajustes de anchura de impulso para el detector de fallos de la FIGURA 1.

La FIGURA 3 es un conjunto de formas de onda que muestran diversas operaciones del detector de fallos de la FIG 1.

- 5 La FIGURA 4 es un conjunto de formas de onda de temporización idealizadas para el ajuste y el restablecimiento de las alarmas de tensión de alimentación baja y alta del detector de fallos adaptable de la FIGURA 1, utilizando la detección de fallos de tensión de alimentación adaptable.

La FIGURA 5 es un diagrama esquemático de circuito de una implementación ilustrativa del detector de fallos adaptable 10 de la FIGURA 1.

- 10 La FIGURA 6 es un diagrama de flujo que muestra una secuencia de funcionamiento ilustrativa para el detector de fallos adaptable de la FIGURA 1.

La FIGURA 7 es un diagrama esquemático de bloques de un dispositivo integrado monolítico seguro ilustrativo.

- 15 La FIGURA 8 es un diagrama esquemático de bloques de un dispositivo integrado monolítico no seguro ilustrativo.

Descripción detallada de la invención

- 20 Un dispositivo de circuito integrado monolítico puede incluir una o varias matrices de memoria digital no volátil de varios tipos, como EEPROM, Flash y SRAM, y circuitos relacionados, como memorias temporales, registros, lógica de control, circuitos de direccionamiento y bombas de tensión. Dependiendo de los requisitos funcionales, el dispositivo también puede incluir otros circuitos como procesadores, controladores de entrada/salida, convertidores analógico-digital y digital-analógico, circuitos de reinicio e interrupción, matrices de puertas programables en campo ("FPGA") y/u otros circuitos. El dispositivo de circuito integrado también puede incluir un detector de fallos de la tensión de alimentación para detectar condiciones transitorias inadecuadas de la tensión de alimentación. Ventajosamente, el umbral de detección del detector de fallos de la tensión de alimentación se configura de forma adaptativa en función del modo de funcionamiento del dispositivo o de una parte concreta del mismo, que el dispositivo conoce internamente en función de determinadas entradas recibidas por el dispositivo, como comandos, interrupciones, señales de control, etc. Consideremos, por ejemplo, un detector de fallos de tensión de alimentación que tiene un umbral de baja tensión adaptable que varía en función del modo de funcionamiento de una matriz de memoria flash en el dispositivo de circuito integrado. La tensión de alimentación mínima para un dispositivo de este tipo puede especificarse en 1,62 voltios, y el monitor de tensión de alimentación puede tener un umbral de baja tensión por defecto de 1,4 voltios (un margen de 0,22 voltios) que es adecuado para muchas operaciones comunes, incluidas las operaciones de lectura de memoria. Sin embargo, el umbral de baja tensión puede reducirse temporalmente a 1,3 voltios (un margen de 0,32 voltios) para operaciones como las de programación y borrado de la memoria, que probablemente provoquen fallos de tensión por debajo de 1,4 voltios que activarían falsamente un estado de protección si el umbral de baja tensión no se modificara de forma adaptativa. Los niveles umbral de 1,3 voltios y 1,4 voltios son ilustrativos, ya que en la práctica los distintos umbrales pueden fijarse en función de diversos factores, como los efectos de la variación del proceso, la tensión y la temperatura ("PVT") y los efectos del consumo interno de corriente.

- 35 La FIGURA 1 es un diagrama esquemático de bloques de las diversas señales asociadas a un detector ilustrativo de fallos de tensión de alimentación adaptable 10. Ilustrativamente, el detector de fallos 10 supervisa tanto los fallos de baja tensión como los de alta tensión, y proporciona señales de salida LVcc_ALARM y HVcc_ALARM para indicar una condición de alarma de umbral bajo y una condición de alarma de umbral alto, respectivamente. Ilustrativamente, LVcc_ALARM y HVcc_ALARM son señales enclavadas, que se ponen en estado de alarma enclavada cuando se violan los umbrales respectivos; concretamente, cuando la tensión de alimentación cae respectivamente por debajo del umbral bajo o supera el umbral alto. Las señales LVcc_THRESHOLD y HVcc_THRESHOLD pueden utilizarse para establecer de forma adaptativa el umbral de detección del detector de fallos de tensión de alimentación en función del modo de funcionamiento del dispositivo o de una parte concreta del mismo. Las señales de entrada adicionales pueden incluir una tensión de referencia CMOS REF o V_{REF} (BGR), una señal de reinicio GD_RESET, una señal de habilitación del detector de fallos GD_EN y una señal de reinicio de encendido POR. La señal de habilitación GD_EN y la señal de reinicio POR pueden aplicarse a una entrada de habilitación EN a través de una compuerta OR 12 o equivalente. Además, puede proporcionarse una señal de salida de detector listo DET_READY. Ciertas condiciones de funcionamiento por defecto, como el nivel de umbral bajo y la anchura de pulso y el nivel de umbral alto y la anchura de pulso, pueden establecerse durante la fabricación.

- 50 La FIGURA 2 es una tabla que muestra valores ilustrativos por defecto y adaptativos para diversos parámetros ilustrativos de umbral bajo y umbral alto, para el detector de fallos 10 de la FIGURA 1. De forma ilustrativa, el nivel de tensión de umbral bajo puede fijarse en 1,4 voltios por defecto y en 1,3 voltios de forma adaptativa, y el nivel de tensión de umbral alto puede fijarse en 2,05 voltios por defecto y en 2,15 voltios de forma adaptativa. De forma ilustrativa, el umbral bajo de duración mínima de la interferencia puede fijarse en 10 nanosegundos por defecto y en 20 nanosegundos de forma adaptativa, y el umbral alto de duración mínima de la interferencia puede fijarse en 10 nanosegundos por defecto y en 20

nanosegundos de forma adaptativa.

Los ajustes de la tensión umbral baja y alta y de la anchura de impulso para diversos modos de funcionamiento pueden establecerse teniendo en cuenta los peores casos razonables para esas operaciones, incluidos, por ejemplo, los efectos de la variación del proceso, la tensión y la temperatura ("PVT") en el peor de los casos y los efectos del consumo interno de corriente. El lado de umbral bajo de la ventana de funcionamiento para un modo de funcionamiento concreto del dispositivo, por ejemplo, puede cumplir los siguientes criterios: justo por encima del nivel de reinicio de encendido ("POR"), así como justo por encima del nivel de tensión de alimentación al que la lógica funciona correctamente. Cuando la tensión de alimentación está por debajo de este nivel, es probable que el comportamiento normal del aparato se vea comprometido y que éste se comporte de forma aleatoria. La ventana operativa predet "rmi "da de la tensión de alimentación para la detección de fallos puede ser más amplia que el rango de tensión de alimentación de la spe "ifi "ación; por ejemplo, V_{CC} en la especificación puede figurar como de 1,62 V a 1,98 V (1,8 V $\pm$ 10%), mientras que la ventana operativa para la detección de fallos correspondiente a un conjunto concreto de modos de funcionamiento del dispositivo puede determinarse como de 1,4 voltios a 2,05 voltios.05 voltios, y correspondiente a otro conjunto particular de modos de funcionamiento del dispositivo puede determinarse que sea de 1,3 voltios a 2,15 voltios, para proporcionar márgenes suficientes o una banda de guarda al rango V_{CC} de la especificación del dispositivo, incluso teniendo en cuenta los efectos de variación PVT y los efectos de consumo de corriente interna, incluidas las variaciones de tensión debidas a los efectos de impedancia y las caídas y sobretensiones de corriente debidas a la actividad del dispositivo.

Disponer de una ventana de funcionamiento ajustada de forma adaptativa para la detección de fallos es ventajoso frente a una ventana de funcionamiento estática. Algunas operaciones en el peor de los casos como, por ejemplo, las operaciones de programación y borrado en la memoria flash incorporada, pueden crear una cantidad de fluctuaciones de tensión y ruido relacionados con la impedancia que es sustancialmente mayor que las fluctuaciones de tensión y el ruido creados por otras operaciones. La operación de programación y borrado de la célula flash, por ejemplo, puede crear un gran aumento de corriente al activar la(s) bomba(s) de carga en chip. La corriente de programación de drenaje, por ejemplo, puede ser de unos 100Ua por celda flash (a unos 4 voltios de tensión de drenaje) para la inyección de electrones calientes en el canal, y por tanto puede ser acumulativamente de unos 800Ua en el caso de programar ocho celdas (es decir, un byte). La corriente de alimentación de tensión (I_{CC}) para la(s) bomba(s) de carga puede alcanzar fácilmente muchos miliamperios, ya que la tensión se bombea desde el nivel V_{CC} (normalmente 1,8 V) hasta un nivel bombeado superior de unos 4 voltios, por ejemplo. Durante la operación de borrado (tunelización), aunque la corriente de la célula es inferior a los microamperios, puede haber no obstante algunos miliamperios de corriente asociados a la activación de las bombas de carga positiva y negativa. Dichas sobretensiones de corriente debidas a la activación de la(s) bomba(s) de carga durante las operaciones de programación y borrado pueden imponer efectos de subimpulso y sobreimpulso en la tensión de alimentación, que un detector de fallos que funcione con una ventana de funcionamiento estática puede interpretar erróneamente como un evento fuera de especificación, dando lugar a una falsa alarma que, a su vez, puede desencadenar una acción de protección innecesaria y perturbadora, como el cierre o el reinicio del dispositivo.

La ventana de funcionamiento ajustada de forma adaptativa para la detección de fallos también puede tener en cuenta la duración de los fallos. El establecimiento de diferentes ajustes de la duración mínima de los fallos para los distintos modos de funcionamiento de los dispositivos permite evitar diversos problemas que aquejan a algunos modos de funcionamiento sin sacrificar la precisión de la detección de fallos en otros modos de funcionamiento. Debido a las impedancias internas inherentes en el chip, hay una cierta duración mínima de fallo, normalmente unos pocos nanosegundos, antes de que un fallo pueda ser detectado con éxito por los circuitos de detección de fallo en el chip para un modo de funcionamiento concreto. Además, puede ser ventajoso diseñar para una cierta duración mínima de fallo, por ejemplo 10Ns, ya que fallos más cortos como, por ejemplo, de 3Ns a 4Ns, pueden no tener un efecto deletéreo en un modo de funcionamiento particular.

El comportamiento anterior se ilustra en la figura 3 para un dispositivo de circuito integrado monolítico ejemplar que incluye una matriz de memoria flash y está especificado para funcionar dentro de un conjunto ilustrativo de condiciones de funcionamiento. Ilustrativamente, V_{CC} se especifica en 1,8V como se muestra en el conducto 32, sin exceder un V_{CC} máximo de 1,98V como se indica en el conducto 31, y sin ser inferior a un V_{CC} mínimo de 1,62V como se indica en el conducto 34. Basándose en un análisis de los efectos de la variación PVT y de los efectos del consumo interno de corriente, incluidas las variaciones de tensión debidas a efectos de impedancia y las caídas y sobretensiones de corriente debidas a la actividad del dispositivo, puede establecerse un umbral bajo adaptable que tenga un valor de 1,4 voltios para los modos de funcionamiento generales, como se indica en la línea 35, y un valor de 1,3 voltios para los modos de funcionamiento especialmente perturbadores, como los modos de funcionamiento de programación y borrado de la memoria flash, como se indica en la línea 36. Los voltajes de umbral bajo adaptables están por encima del nivel de voltaje de reinicio de encendido de 1,0 voltios indicado por el conducto 37, e ilustrativamente el dispositivo de circuito integrado monolítico es capaz de funcionar normalmente y sin alarmas durante los modos generales de funcionamiento con transitorios que no son inferiores a 1,4 voltios, y durante los modos de funcionamiento de programación y borrado de la memoria flash con transitorios que no son inferiores a 1,3 voltios.

La forma de onda 33 representa el posible comportamiento de V_{CC} durante el funcionamiento normal real del dispositivo. Un fallo de alta tensión 30 se produce dentro del rango V_{CC} especificado y no requiere un manejo especial. Dos fallos de baja tensión 38 y 39 están por debajo del V_{CC} mínimo especificado de 1,62 voltios. El fallo 38 se produce durante uno de los modos generales de funcionamiento y no afecta al correcto funcionamiento del circuito integrado monolítico ni supera

el umbral bajo fijado de forma adaptativa en 1,4 voltios correspondiente a los modos generales de funcionamiento, de modo que no se dispara ninguna alarma. El fallo 39 se produce durante uno de los modos de funcionamiento de programación o de borrado, y no afecta al correcto funcionamiento del circuito integrado monolítico ni supera el umbral bajo fijado de forma adaptativa en 1,3 voltios correspondiente a los modos de funcionamiento de programación y de borrado, de modo que no se dispara ninguna alarma. Si el fallo 39 se produce durante uno de los modos generales de funcionamiento para los que el umbral bajo se fija de forma adaptativa en 1,4 voltios, el fallo 39 se identifica como anormal y puede activarse una alarma.

Aunque la FIGURA 3 proporciona un ejemplo de umbral adaptativo para transitorios de baja tensión, puede establecerse un umbral adaptativo para transitorios de alta tensión de manera similar. Además, aunque los umbrales se describen como adaptables a los modos de funcionamiento de programación y borrado, por un lado, y a los modos de funcionamiento generales (modos distintos de programación y borrado), por otro, los umbrales pueden ser adaptables de diversas maneras a otros modos de funcionamiento y a otras combinaciones de modos de funcionamiento, incluidos más de dos modos de funcionamiento.

La FIGURA 4 muestra un conjunto 40 de formas de onda de temporización idealizadas para el ajuste y el restablecimiento de las alarmas de tensión de alimentación baja y alta del detector adaptativo de fallos 10 de la FIGURA 1, utilizando la detección adaptativa de fallos de tensión de alimentación. La tensión de alimentación V_{CC} se suministra generalmente a un nivel especificado, pero se muestran dos eventos de fallo ilustrativos, un fallo de baja tensión 41 que comienza en el tiempo 45 y cae por debajo del umbral bajo de adaptación LV_{CC} (sólo se muestra un único ajuste de tensión para mayor claridad), y un fallo de alta tensión 42 que comienza en el tiempo 46 y supera el umbral alto HV_{CC} (sólo se muestra un único ajuste de tensión para mayor claridad). El detector de fallos adaptativo 10 puede habilitarse en el flanco de subida de la señal de habilitación GD_EN en el tiempo 43, tras lo cual el detector de fallos adaptativo 10 señala listo mediante la transición positiva de la señal de salida de detector listo DET_READY en el tiempo 44, ilustrativamente mayor que unos 200Ns después de la señal de habilitación GD_EN . Cuando el fallo de baja tensión 41, que se produce en el tiempo 45, tiene una duración superior a la anchura de impulso mínima correspondiente a LV_{CC} , es detectado por el detector de fallo 10 que señala la alarma de baja tensión LV_{CC_ALARM} . De manera similar, cuando el fallo de alta tensión 42, que se produce en el tiempo 46, tiene una duración superior a la anchura de impulso mínima correspondiente a HV_{CC} , es detectado por el detector de fallo 10 que señala la alarma de alta tensión HV_{CC_ALARM} . Las alarmas pueden restablecerse mediante la señal GD_RESET , que ilustrativamente se afirma como un impulso de restablecimiento de una anchura superior a aproximadamente 1Ns durante un período comprendido entre el tiempo 47 y el tiempo 48. Como muestran las formas de onda LV_{CC_ALARM} y HV_{CC_ALARM} , ambas alarmas se reinician poco tiempo después del flanco descendente del impulso de reinicio.

La FIGURA 5 es un diagrama de circuito esquemático de una implementación ilustrativa 50 del detector de fallos adaptativo 10 de la FIGURA 1. El detector de fallos adaptable 10 incluye un detector de umbral bajo 60, un detector de umbral alto 70 y un circuito corrector de inestabilidad de encendido 80.

El detector de umbral bajo 60 incluye un amplificador diferencial 66 que está conectado en su entrada inversora a una resistencia en serie 64 y 65 conectada entre V_{CC} y tierra para proporcionar una polarización adecuada al amplificador diferencial 66. Las resistencias 64 y 65 pueden recortarse adecuadamente durante la fabricación para establecer la polarización deseada. La entrada no inversora se conecta a una tensión de referencia para establecer el umbral bajo seleccionado. Ilustrativamente, la tensión de referencia puede ser una tensión de referencia CMOS proporcionada por un circuito en el que la resistencia 61, el MOSFET 62 y la resistencia 63 están conectados en serie entre V_{CC} y masa. Una o ambas resistencias 61 y 63 pueden hacerse variables utilizando cualquier técnica deseada. Una técnica adecuada bien conocida en el arte es la de varios transistores MOSFET (no mostrados) para conmutar varias resistencias hacia dentro o hacia fuera para establecer dos o más niveles de referencia CMOS diferentes. La señal de umbral bajo $LV_{CC_THRESHOLD}$ puede ser una señal de tensión variable aplicada a las compuertas de dichos transistores MOSFET para controlar sus estados de encendido/apagado. Durante el funcionamiento por defecto del detector de umbral bajo 60, la tensión en la entrada inversora del amplificador diferencial 66 es mayor que la tensión en la entrada no inversora, de modo que aparece una tensión baja en la salida del amplificador diferencial 66 que es enclavada por el sujetador 67. Sin embargo, cuando un fallo hace que V_{CC} caiga por debajo del umbral bajo seleccionado, la tensión en la entrada inversora del amplificador diferencial 66 se hace menor que la tensión en la entrada no inversora, provocando una transición positiva en la salida del amplificador diferencial 66 que es enclavada por el sujetador 67 para generar la alarma de umbral bajo LV_{CC_ALARM} .

El detector de umbral alto 70 incluye un amplificador diferencial 74 que está conectado en su entrada no inversora a una resistencia en serie 71 y 72, que está conectada entre V_{CC} y masa para proporcionar una polarización adecuada al amplificador diferencial 74. Las resistencias 71 y 72 pueden recortarse adecuadamente durante la fabricación para establecer la polarización deseada. La entrada inversora del amplificador diferencial 74 se conecta a una tensión de referencia para establecer el umbral alto seleccionado. Ilustrativamente, la tensión de referencia 73 puede ser un circuito de referencia de espacio de banda variable ("BGR"), que varía una tensión de referencia V_{REF} en función del umbral alto deseado. Durante el funcionamiento por defecto del detector de umbral alto 70, la tensión en la entrada no inversora del amplificador diferencial 74 es menor que la tensión en la entrada inversora, de modo que aparece una señal baja en la salida del amplificador diferencial 74, que mantiene baja la salida de la puerta AND 84, que a su vez es enclavada por el sujetador 75. Sin embargo, cuando un fallo hace que V_{CC} se eleve por encima del umbral alto seleccionado, la tensión en

la entrada no inversora del amplificador diferencial 74 se hace mayor que la tensión en la entrada inversora, provocando una transición positiva en la salida del amplificador diferencial 74 que eleva la salida de la puerta AND 84 a un nivel alto (suponiendo un nivel alto del circuito corrector de inestabilidad de encendido 80), que a su vez es enclavado por el sujetador 75 para generar la alarma de umbral alto HV_{CC}_ALARM.

5 Observe que el detector de umbral bajo 60 no responde normalmente a las perturbaciones altas, mientras que el detector de umbral alto 70 no responde normalmente a las perturbaciones bajas. Si se produce un fallo alto, la tensión en la entrada inversora del amplificador diferencial 66 simplemente sube más, manteniendo así baja la salida del amplificador diferencial 66. Si se produce un fallo de baja, la tensión de la entrada no inversora del amplificador diferencial 74 simplemente desciende, manteniendo así baja la salida del amplificador diferencial 74.

10 El circuito corrector de inestabilidad de encendido 80 corrige un problema que se da en muchos tipos de circuitos de referencia de espacio de banda, a saber, que dichos circuitos son inestables hasta que V_{CC} alcanza un determinado nivel mínimo. En particular, dichos circuitos de referencia de espacio de banda son inestables durante el encendido cuando V_{CC} tiende a ser muy baja; por ejemplo, cuando V_{CC} tiende a estar en el rango de 0,8 voltios a 1,3 voltios. Como V_{CC} es inferior al umbral bajo durante este periodo, el detector de umbral bajo 60 aplica una señal alta al inversor 82, que a su vez aplica una señal baja a la puerta AND 84, bloqueando así cualquier señal generada por el amplificador diferencial 74 en el circuito de umbral alto 70, que puede ser falsa, para que no llegue al sujetador 75.

15 Los circuitos de espacio de banda variable adecuados son bien conocidos en la técnica. En un tipo adecuado de circuito de espacio de banda, pueden utilizarse transistores MOSFET (no mostrados) para conmutar varias resistencias hacia dentro o hacia fuera para establecer dos o más niveles diferentes de V_{REF} de referencia de espacio de banda. La señal de umbral alto HV_{CC}_THRESHOLD puede ser una señal de tensión variable aplicada a las compuertas de dichos transistores MOSFET para controlar sus estados de encendido/apagado. Un ejemplo de circuito de referencia de espacio de banda adecuado se describe en Dominik Gruber y otros, A Voltage Reference with On-Chip Trimmable Temperature Coefficient and Offset Voltage, MIXDES 2011,¹⁸ Conferencia Internacional "Diseño Mixto de Circuitos y Sistemas Integrados", 16-18 de junio de 2011, PP. 231-236 que se incorpora en la presente en su totalidad por referencia a la misma.

20 La duración mínima de fallo del umbral bajo y la duración mínima de fallo del umbral alto pueden ser fijas o variables, o una puede ser fija y la otra variable. Si es variable, la duración de la detección del fallo bajo (o alto) puede coordinarse con el nivel de tensión umbral bajo (o alto) o ser independiente de éste. En la FIGURA 5 se muestra una técnica ilustrativa para implementar un subcircuito de duración variable de detección de fallos, en el que la salida del amplificador diferencial 66 del detector de umbral bajo 60 se aplica a una puerta AND 69, así como a un circuito de retardo 68, de modo que una señal de disparo pasa a través de la puerta AND 69 sólo si es de duración suficiente para permanecer afirmada mientras que la misma señal de disparo se retrasa a través del retardo 68. Si se desea coordinar la duración de la detección de fallo bajo con el nivel de tensión umbral bajo, puede utilizarse la señal LV_{CC}_THRESHOLD como señal de control del retardo 68. De lo contrario, se puede utilizar una señal diferente. De manera similar, la salida del amplificador diferencial 74 del detector de umbral alto 70 se aplica a una puerta AND 79, así como a un circuito de retardo 78, de manera que una señal de disparo pasa a través de la puerta AND 79 sólo si tiene la duración suficiente para permanecer afirmada mientras que la misma señal de disparo se retrasa a través del retardo 78. Si se desea coordinar la duración de la detección de fallo alto con el nivel de tensión umbral alto, se puede utilizar la señal HV_{CC}_THRESHOLD como señal de control del retardo 78. De lo contrario, se puede utilizar una señal diferente. Los circuitos de retardo variable adecuados son bien conocidos en la técnica; véase, por ejemplo Jung-Lin Yang y otros, Tunable Delay Element for Low Power VLSI Circuit Design, IEEE nº 1-4244-0549-1/06, 2006, PP. 1-4 que se incorpora en la presente en su totalidad por referencia a la misma.

25 La realización de la FIGURA 5 es un ejemplo de un detector de fallos adaptable adecuado. Otros circuitos comparadores de tensión pueden modificarse convenientemente para proporcionar una detección adaptativa de fallos de acuerdo con la descripción expuesta en este documento de patente.

30 La FIGURA 6 es un diagrama de flujo que muestra una secuencia de funcionamiento ilustrativa 90 para el detector de fallos adaptativo 10 de la FIGURA 1. La detección de fallos puede habilitarse (bloque 91) de la forma que se desee, ya sea como parte del procedimiento de encendido o de reinicio o mediante un comando. Si se desea, pueden establecerse umbrales bajos y/o altos predeterminados en el momento de la activación. Mientras el dispositivo de circuito integrado monolítico está en funcionamiento, el detector de fallos puede configurarse de forma adaptativa a un umbral bajo, a un umbral alto o a ambos, según se desee, en función del modo de funcionamiento (bloque 92). Si no se superan ni el umbral bajo ni el umbral alto mientras el modo de funcionamiento está en vigor (bloque 93 - NO), la secuencia 90 vuelve a establecer de forma adaptativa un umbral bajo, un umbral alto o ambos, según se desee, en función del modo de funcionamiento (bloque 92). Sin embargo, si se supera el umbral bajo o el umbral alto mientras el modo de funcionamiento está en vigor (bloque 93 - SÍ), se activa la alarma de umbral bajo LV_{CC}_ALARM o la alarma de umbral alto HV_{CC}_ALARM según corresponda (bloque 94) para que el dispositivo de circuito integrado monolítico pueda tomar las medidas oportunas (bloque 95), como apagar el dispositivo, reiniciarlo, configurar un bit de registro para indicar un posible fallo u otra acción deseada. Para los dispositivos que continúan funcionando tras la detección del fallo, se restablece la alarma de umbral bajo LV_{CC}_ALARM o la alarma de umbral alto HV_{CC}_ALARM según corresponda (bloque 96) y la secuencia 90 vuelve a establecer de forma adaptativa un umbral bajo, un umbral alto o ambos, según se desee, en función del modo de funcionamiento (bloque 92).

Implementación ejemplar: Detección de fallos para un dispositivo seguro

La memoria digital no volátil puede utilizarse en dispositivos de circuitos integrados monolíticos para almacenar información sensible. La memoria flash, por ejemplo, muy utilizada en dispositivos de memoria segura, sistemas en un chip ("SOC") y matrices de puertas programables en campo ("FPGA"), puede utilizarse para almacenar punteros de instrucciones, datos sensibles, contraseñas, claves de cifrado y similares, en cualquier combinación. Ventajosamente para estas aplicaciones, la memoria flash es no volátil, reprogramable, programable una sola vez y de bajo consumo.

Por desgracia, muchos tipos de dispositivos de circuitos integrados seguros son vulnerables a los ataques de fallo de V_{CC} en los que un atacante varía la V_{CC} en un intento de explotar posibles debilidades en el diseño del dispositivo. En un ataque de fallo por subimpulso de V_{CC} , por ejemplo, un flip-flop dentro de la lógica del dispositivo puede cambiar de estado. Además, en esta ilustración ejemplar, esto puede hacer que la lógica de codificación, que comprueba si los comandos son legales, funcione mal y permita que se ejecute un comando ilegal. Esto no es deseable ya que la seguridad puede verse comprometida. Detectar V_{CC} fuera de la ventana de funcionamiento normal y activar una alarma o tomar otras medidas apropiadas es, por tanto, útil para la seguridad de la rebaba asegurada.

Para contrarrestar la amenaza de un ataque de fallo V_{CC} , un dispositivo de circuito integrado puede estar provisto de un detector de fallo adaptable como el detector de fallo adaptable 10 (FIGURA 1). El detector de fallos de V_{CC} adaptable puede monitorizar V_{CC} en cualquier ubicación deseada dentro del dispositivo de circuito integrado, aunque monitorizar tan cerca de la patilla V_{CC} externa del dispositivo de circuito integrado como sea práctico puede ser ventajoso en algunos dispositivos de circuito integrado para evitar los efectos de las impedancias del circuito interno en las formas de onda V_{CC} internas. Alternativamente, la supervisión de V_{CC} cerca de circuitos sensibles puede ser ventajosa en algunos dispositivos de circuitos integrados.

La FIGURA 7 es un diagrama esquemático de bloques de un dispositivo integrado monolítico seguro ilustrativo 100 que incluye circuitos como el acondicionador de tensión 101, la referencia interna 102, el detector adaptativo de fallos 103, el detector analógico 104, el reinicio y las interrupciones 105, la unidad procesadora y/o la lógica de control 106, el generador de reloj 107, el detector de manipulaciones 108, el controlador de entrada/salida 109, los módulos de servicio 110, las matrices de memoria 111 y las funciones de seguridad (por ejemplo, criptografía) 112. El detector de fallos adaptable 103 proporciona la señal de alarma de umbral bajo LV_{CC_ALARM} y/o la señal de alarma de umbral alto HV_{CC_ALARM} al detector de manipulaciones 108, que determina un curso de acción apropiado de acuerdo con el umbral violado y el modo de funcionamiento en vigor.

Implementación ejemplar: Detección de fallos para dispositivos no seguros

La FIGURA 8 es un diagrama esquemático de bloques de un dispositivo integrado monolítico ilustrativo 200 que es similar al dispositivo de circuito integrado monolítico seguro 100 (FIGURA 7) pero carece del detector de manipulaciones 108 y de las funciones de seguridad 112. El detector de fallos adaptable 103 proporciona la señal de alarma de umbral bajo LV_{CC_ALARM} y/o la señal de alarma de umbral alto HV_{CC_ALARM} a cualquier elemento funcional que se desee. Las señales de alarma de umbral LV_{CC_ALARM} y/o HV_{CC_ALARM} pueden proporcionarse, por ejemplo, al elemento de reinicio e interrupciones 105, que puede estar configurado para reiniciar el dispositivo o determinados elementos funcionales del mismo, o a la unidad procesadora y/o lógica de control 106, que puede estar configurada para informar del incidente a un dispositivo o circuito externo a través del control de entrada/salida 109.

REIVINDICACIONES

1. Un método (90) para detectar un fallo (30, 38, 39; 41, 42) en la tensión de alimentación (VCC) suministrada a un dispositivo de circuito integrado monolítico (100; 200) que tiene varios modos de funcionamiento y que comprende una pluralidad de circuitos funcionales (101 - 112) configurados para funcionar respectivamente en los diversos modos de funcionamiento, el método comprende:
 - 5 hacer funcionar el dispositivo (100; 200) en un primer modo de funcionamiento seleccionado entre los modos de funcionamiento;
configurar (92), mediante un circuito de detección del umbral de tensión de alimentación (50; 103) del dispositivo (100; 200) y en respuesta al primer paso de funcionamiento del modo, un umbral de detección configurable (LVCC, HVCC) como uno de una pluralidad de umbrales de detección asociados respectivamente a uno o más de los modos de funcionamiento, de acuerdo con el primer modo de funcionamiento, en el que el circuito de detección del umbral de tensión de alimentación (50; 103) configura el umbral de detección configurable (LVCC, HVCC) en respuesta a una señal de control proporcionada por una lógica de control (106) del dispositivo (100; 200), la señal de control indicativa de uno
10 actualmente activo de los diversos modos de funcionamiento; y
supervisar (93), mediante el circuito de detección del umbral de tensión de alimentación (50; 103), la tensión de alimentación (VCC) de un fallo (39; 41, 42) que viole el umbral de detección configurable (LVCC, HVCC) tal como se configuró en el paso de configuración del umbral de detección configurable (92).
 - 15 2. El método de acuerdo con la reivindicación 1, en donde:

el umbral de detección configurable (LVCC, HVCC) configurado en el paso de configuración del umbral de detección configurable (92) comprende un umbral de baja tensión (LVCC) para una duración mínima predeterminada (68); y
el primer fallo (39; 41) tiene una amplitud de tensión mínima inferior al umbral de baja tensión (LVCC) o el primer fallo (39; 41) tiene una amplitud de tensión mínima inferior al umbral de baja tensión (LVCC) durante una duración superior a la
20 duración mínima predeterminada.
 3. El método de acuerdo con la reivindicación 1, en donde:

el umbral de detección configurable (LVCC, HVCC) configurado en el paso de configuración del umbral de detección configurable (92) comprende un umbral de alta tensión (HVCC) para una duración mínima predeterminada (78); y
el primer fallo (42) tiene una amplitud de tensión máxima superior al umbral de alta tensión (HVCC) o el primer fallo (42) tiene una amplitud de tensión máxima superior al umbral de alta tensión (HVCC) durante una duración superior a la
25 duración mínima predeterminada (78).
 4. El método de acuerdo con la reivindicación 1, en el que la pluralidad de umbrales de detección (LVCC, HVCC) comprende una pluralidad de umbrales de detección bajos (LVCC) y una pluralidad de umbrales de detección altos (HVCC), comprendiendo además:

configurar (92), en respuesta adicional al primer paso de funcionamiento del modo, un umbral de detección configurable adicional (LVCC, HVCC) como uno de la pluralidad de umbrales de detección, de acuerdo con el primer modo de funcionamiento, siendo el umbral de detección configurable un umbral de detección bajo (LVCC), y el umbral de detección
30 configurable adicional un umbral de detección alto (HVCC); y
monitorizar adicionalmente (93) la tensión de alimentación (VCC) en busca de un fallo (42) que viole el umbral de detección configurable adicional (HVCC) configurado en el paso de configuración del umbral de detección configurable adicional (92).
 5. El método de acuerdo con la reivindicación 4, que además comprende:

35 detectar un primer fallo (39; 41, 42) en la etapa de supervisión (93), en la etapa de supervisión posterior (93) o en ambas;
y
configurar (94) una alarma en respuesta al primer escalón de detección de fallos.
 6. El método de acuerdo con la reivindicación 1, que además comprende:

45 hacer funcionar el dispositivo en un segundo modo de funcionamiento seleccionado entre los modos de funcionamiento, siendo el segundo modo de funcionamiento posterior y diferente al primer modo de funcionamiento;
configurar (92), en respuesta al segundo paso de funcionamiento del modo, un umbral de detección configurable posterior (LVCC, HVCC) como uno de la pluralidad de umbrales de detección, de acuerdo con el segundo modo de funcionamiento;
y
40 monitorizar (93) la tensión de alimentación (VCC) en busca de un fallo (30, 38, 39; 41, 42) que viole el umbral de detección configurable posterior (LVCC, HVCC) configurado en el paso de configuración del umbral de detección configurable posterior (92).
 7. Un dispositivo de circuito integrado monolítico (100; 200) con varios modos de funcionamiento, que comprende:

- una pluralidad de circuitos funcionales (101 - 112) configurados para operar respectivamente en los distintos modos de funcionamiento;
- lógica de control (106) configurada para proporcionar una señal de control indicativa de uno de los diversos modos de funcionamiento actualmente activo; y
- un circuito de detección del umbral de tensión de alimentación (50; 103) adaptado para configurarse, en respuesta a la señal de control indicativa de uno de varios modos de funcionamiento actualmente activos, en uno o varios de una pluralidad de umbrales de detección (LVCC, HVCC) asociados respectivamente a uno o varios de los modos de funcionamiento, estando el circuito de detección del umbral de tensión de alimentación (50; 103) acoplado a la lógica de control (106) y configurado en respuesta a la señal de control para proporcionar una alarma en una salida del mismo cuando la tensión de alimentación viole uno de los umbrales de detección (LVCC, HVCC) en función del modo de funcionamiento actualmente activo.
- 10 8. El dispositivo de circuito integrado monolítico de acuerdo con la reivindicación 7, en el que
- los umbrales de detección (LVCC, HVCC) comprenden umbrales de detección bajos (LVCC) y umbrales de detección altos (HVCC); y
- el circuito de detección del umbral de tensión de alimentación (50; 103) está configurado en uno de los umbrales de detección bajo (LVCC) y en uno de los umbrales de detección alto (HVCC) para el modo de funcionamiento actualmente activo.
- 15 9. El dispositivo de circuito integrado monolítico de acuerdo con la reivindicación 8, en el que el circuito de detección del umbral de tensión de alimentación (50; 103) comprende:
- un detector de umbral bajo (60) que tenga un circuito de referencia CMOS controlado por la señal de control; y
- 20 un detector de umbral alto (70) que tiene un circuito de referencia de espacio de banda controlado por la señal de control.
10. El dispositivo de circuito integrado monolítico de acuerdo con la reivindicación 9, en el que el circuito de detección de umbral de tensión de alimentación (50; 103) comprende además un circuito corrector de inestabilidad de encendido (80) que tiene una entrada acoplada a una salida del detector de umbral bajo (60), y una salida acoplada al detector de umbral alto (70) y configurado para bloquear (82) una señal de alarma procedente del detector de umbral alto (70) durante el encendido del circuito integrado monolítico.
- 25 11. El dispositivo de circuito integrado monolítico de acuerdo con la reivindicación 7, en el que el circuito de detección del umbral de tensión de alimentación (50; 103) comprende:
- un amplificador diferencial (66, 74) que tenga una salida, una entrada de polarización y una entrada de tensión de referencia variable que responda a la señal de control; y
- 30 un sujetador (67, 75) acoplado a la salida del amplificador diferencial (66, 74).
12. El dispositivo de circuito integrado monolítico de acuerdo con la reivindicación 11, que comprende además un circuito de referencia CMOS (61, 62, 63) que responde a la señal de control y tiene una salida acoplada a la entrada de tensión de referencia variable del amplificador diferencial (66).
- 35 13. El dispositivo de circuito integrado monolítico de acuerdo con la reivindicación 11, que comprende además un circuito de referencia de espacio de banda (73) que responde a la señal de control y tiene una salida acoplada a la entrada de tensión de referencia variable del amplificador diferencial (74).

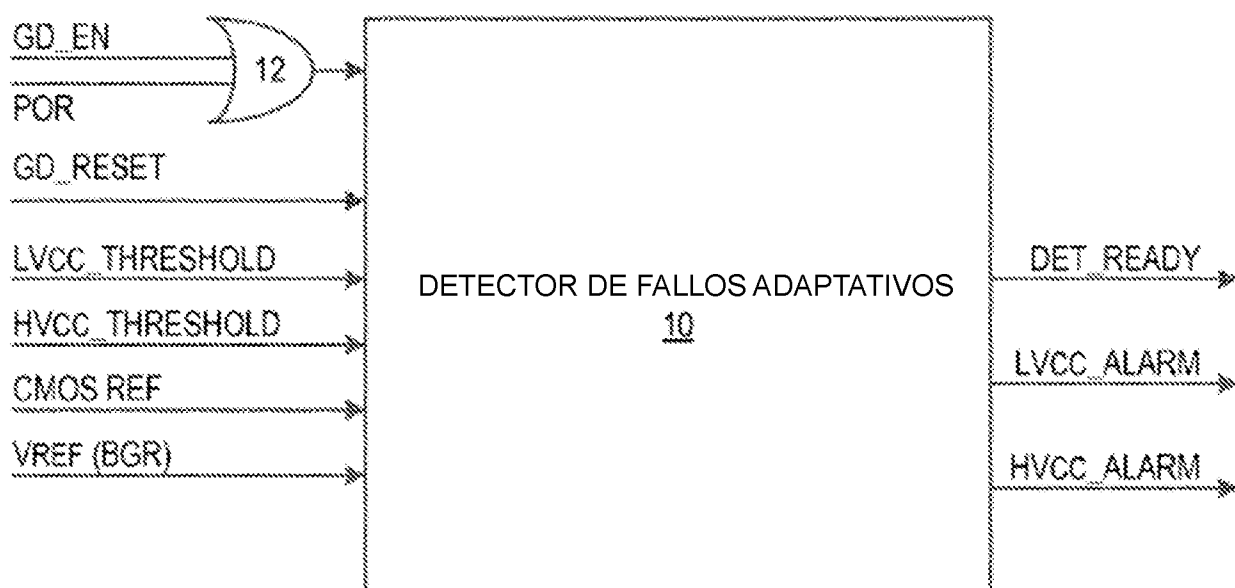


FIG. 1

PARÁMETRO DE UMBRAL	VALOR POR DEFECTO	VALOR ADAPTATIVO
NIVEL LV	1.4V	1.3V
NIVEL HV	2.05V	2.15V
ANCHO DE IMPULSO LV	10nS	20nS
ANCHO DE IMPULSO HV	10nS	20nS

FIG. 2

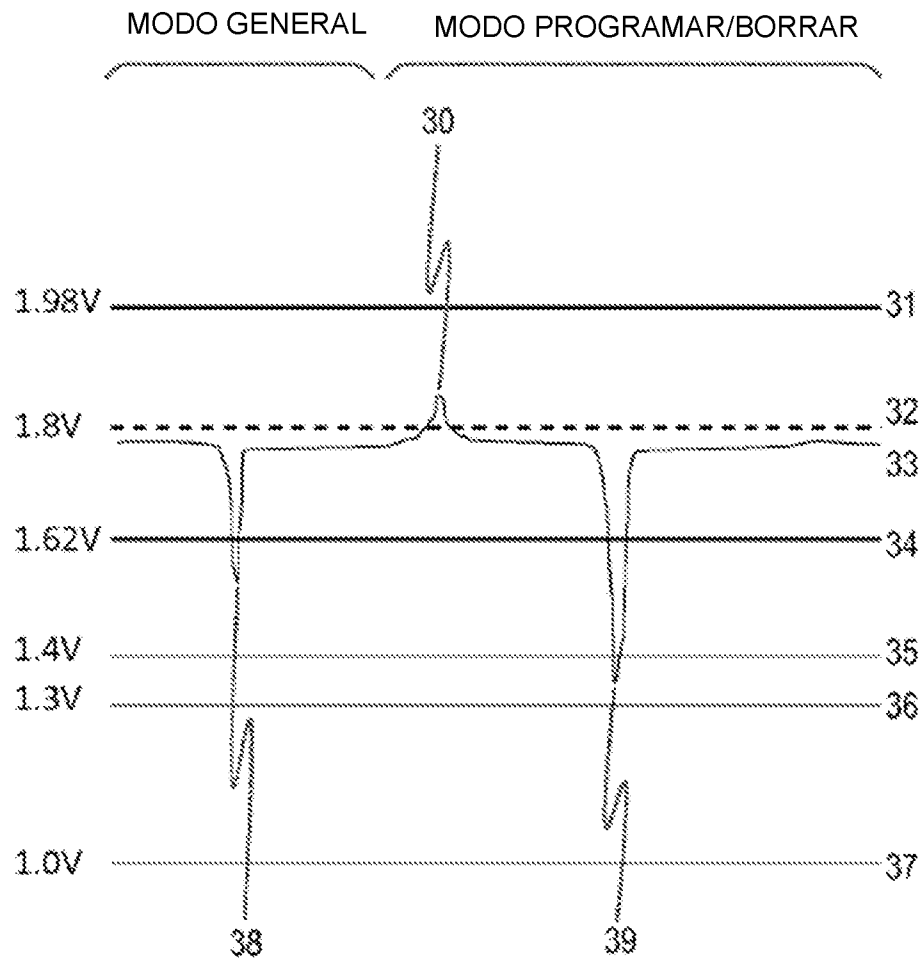


FIG. 3

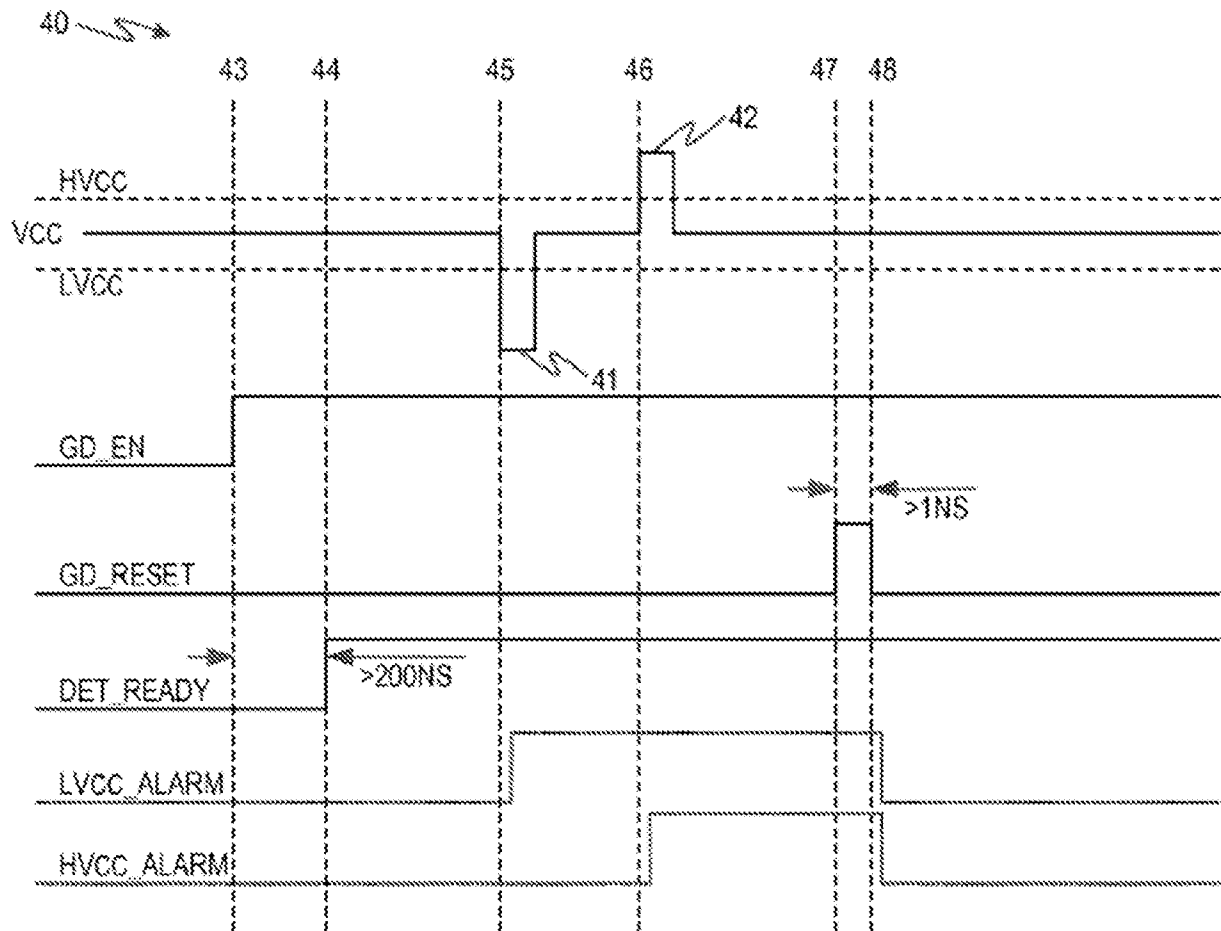


FIG. 4

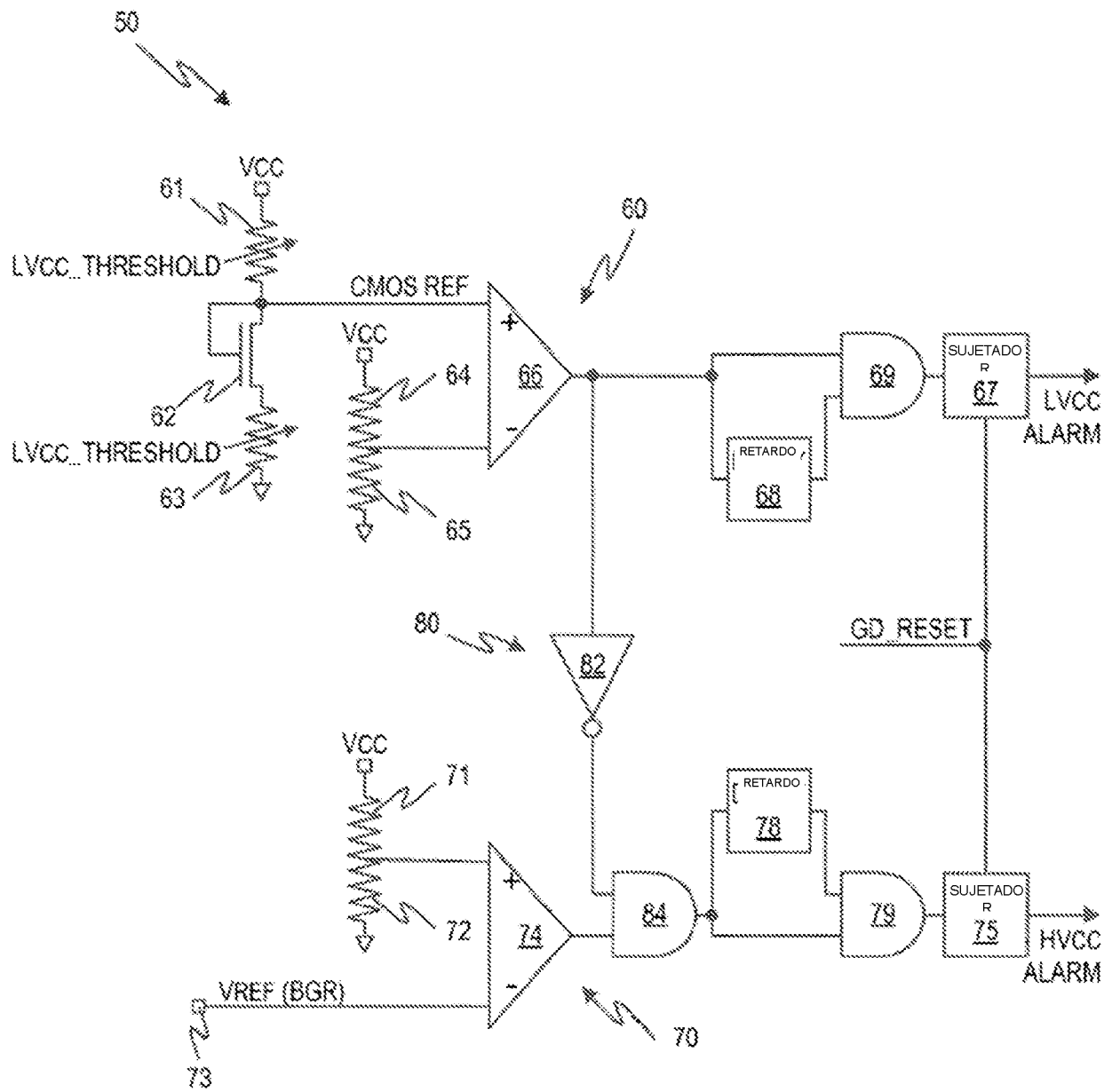


FIG. 5

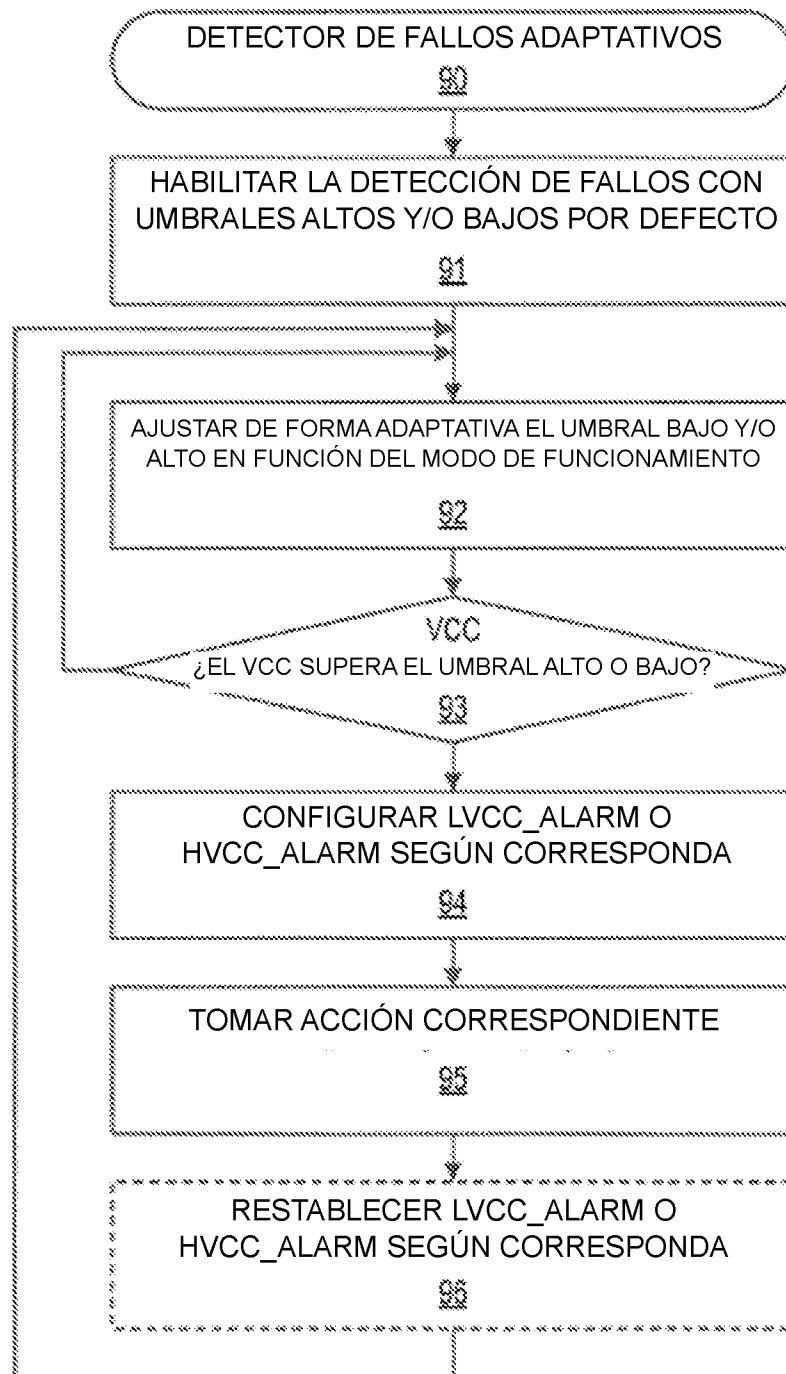


FIG. 6

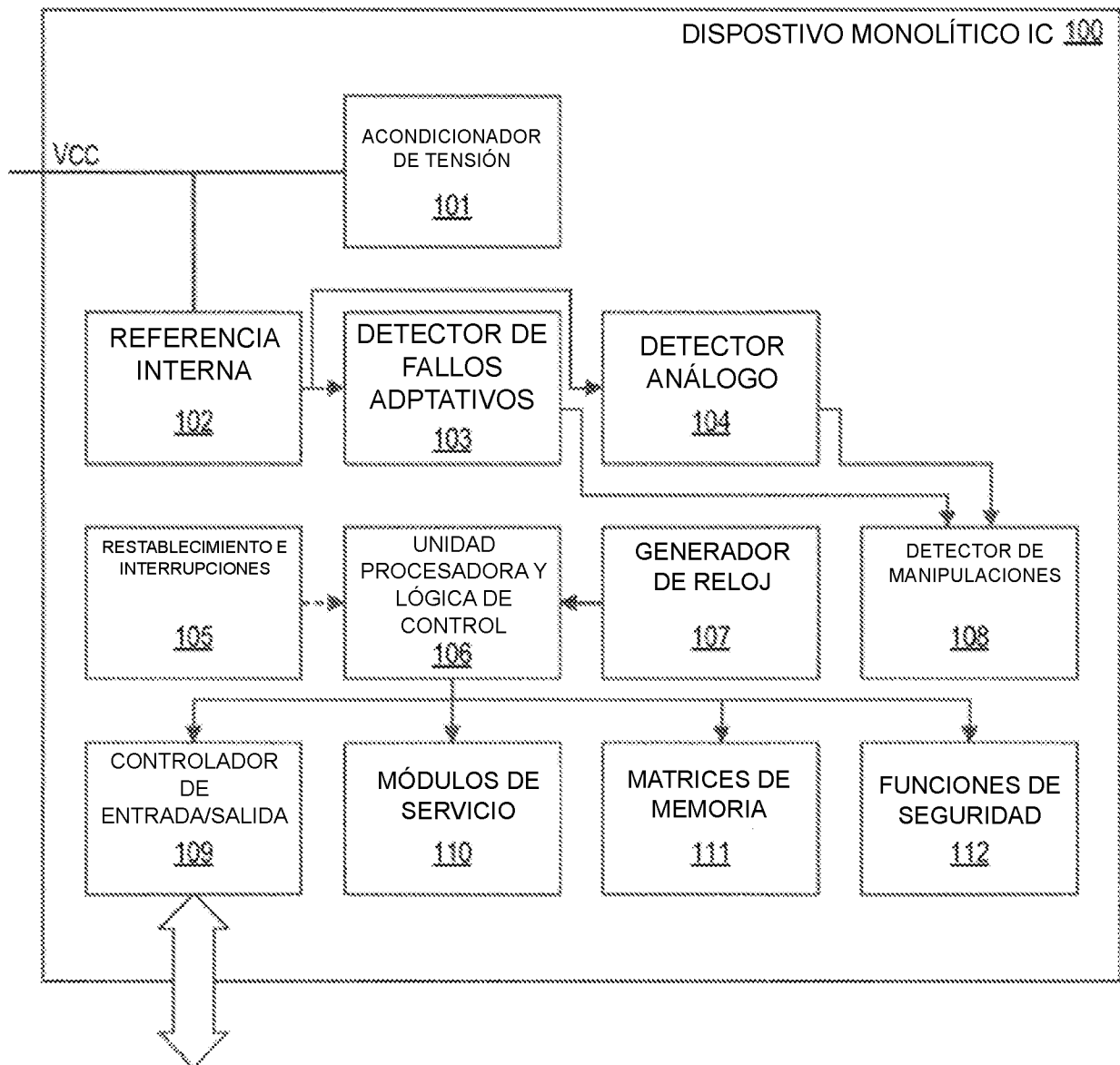


FIG. 7

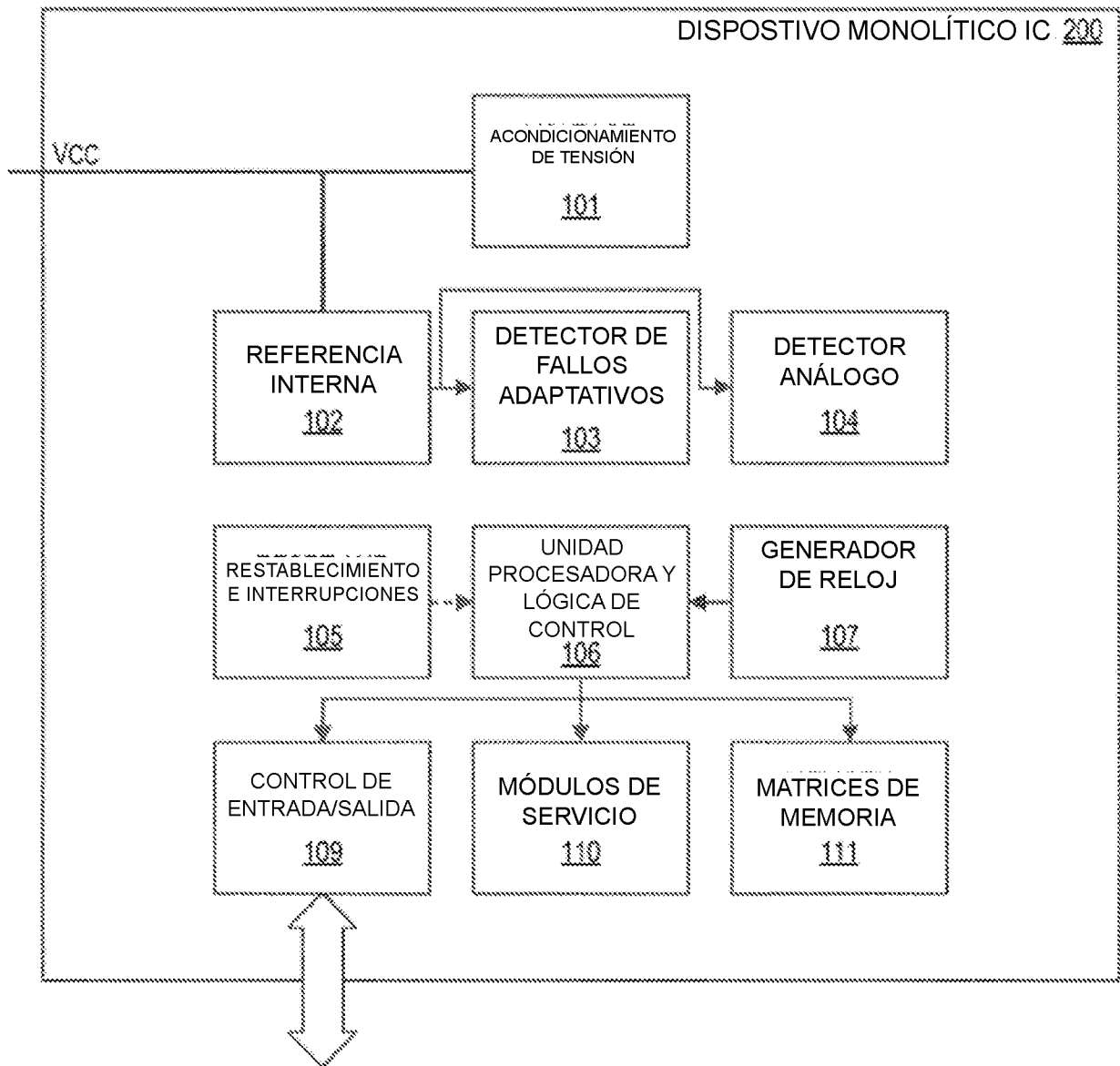


FIG. 8