(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 974 290**

(51) Int. Cl.:

***G01R 31/3193*** (2006.01)
***G01R 31/30*** (2006.01)
***G01R 31/28*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.11.2018 PCT/IL2018/051234**

(87) Fecha y número de publicación internacional: **23.05.2019 WO19097516**

(96) Fecha de presentación y número de la solicitud europea: **15.11.2018 E 18877539 (9)**

(97) Fecha y número de publicación de la concesión europea: **07.02.2024 EP 3710844**

(54) Título: **Medición del margen de un circuito integrado y dispositivo de predicción de fallos**

(30) Prioridad:

**15.11.2017 US 201762586423 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**26.06.2024**

(73) Titular/es:

**PROTEANTECS LTD. (100.0%)**
**2 Pal-Yam Ave.**
**3309502 Haifa, IL**

(72) Inventor/es:

**LANDMAN, EVELYN;**
**COHEN, SHAI;**
**DAVID, YAHEL;**
**FAYNEH, EYAL y**
**WEINTROB, INBAR**

(74) Agente/Representante:

**DEL VALLE VALIENTE, Sonia**

## DESCRIPCIÓN

Medición del margen de un circuito integrado y dispositivo de predicción de fallos

### Campo de la invención

La invención se refiere al campo de los circuitos integrados semiconductores.

### Antecedentes

Los circuitos integrados (CI) pueden incluir circuitos electrónicos analógicos y digitales en un sustrato semiconductor plano, tal como un chip de silicio. Unos transistores microscópicos se imprimen sobre el sustrato usando técnicas de fotolitografía para producir circuitos complejos de miles de millones de transistores en un área muy pequeña, lo que hace que el diseño moderno de circuitos electrónicos que utilizan CI sea de bajo coste y de alto rendimiento. Los CI se producen en líneas de ensamblaje de fábricas, denominadas fundiciones, que han mercantilizado la producción de CI, tales como CI de semiconductores complementarios de óxido metálico (CMOS, por sus siglas en inglés). Los CI digitales contienen miles de millones de transistores dispuestos en unidades funcionales y/o lógicas en el chip, con rutas de datos que interconectan las unidades funcionales que transfieren valores de datos entre las unidades funcionales. Como se utiliza en la presente memoria, el término "ruta de datos" significa una serie paralela de conexiones electrónicas, o rutas, para transferir señales de datos entre unidades funcionales/lógicas de un CI, y cada ruta de datos puede incluir un número específico de rutas de bits, tal como 64, 128, 256 o similares. Durante el proceso de diseño del CI, la temporización de las unidades funcionales se dispone de modo que cada unidad funcional puede completar usualmente el procesamiento requerido de esa unidad dentro de un solo ciclo de reloj. Puede usarse un factor de seguridad para tener en cuenta las diferencias de fabricación de los CI individuales y los posibles cambios, tales como degradaciones, sobre la vida útil planificada del CI.

La degradación de los transistores de un CI a lo largo del tiempo se denomina envejecimiento. Por ejemplo, la degradación de los transistores a lo largo del tiempo conduce lentamente a una disminución de las velocidades de conmutación, e incluso puede provocar fallos completos en el circuito, cuando superan los factores de seguridad del diseño. Usualmente, el proceso de diseño incorpora estos retardos en el diseño de manera que los CI no fallarán durante su vida útil normal, pero las condiciones medioambientales y de uso (tales como calor, tensión, corriente, humedad y/o similares) pueden acelerar el proceso de envejecimiento.

Los transistores del CI, tales como transistores bipolares, transistores de efecto de campo de semiconductores de óxido metálico (MOSFET, por sus siglas en inglés) y/o similares, pueden usarse en los CI digitales y pueden funcionar como conmutadores eléctricos. Por ejemplo, un MOSFET puede tener cuatro terminales, tales como el sustrato, la puerta, la fuente y el drenador, sin embargo típicamente la fuente y el sustrato están conectados eléctricamente. La tensión aplicada a la puerta puede determinar la cantidad de corriente que fluye entre la fuente y el drenador. Una capa delgada de material dieléctrico aísla eléctricamente la puerta, y el campo eléctrico aplicado a través de la puerta puede alterar la conductividad del canal semiconductor subyacente entre la fuente y el drenador.

Con el uso, los portadores de carga (tales como electrones para los MOSFET de canal negativo o n, o huecos para los MOSFET de canal positivo o p) que tienen más energía que el portador de carga medio pueden desviarse del canal conductor entre la fuente y el drenador, y quedar atrapados en el dieléctrico aislante. Este proceso, denominado inyección de portadores calientes (HCI, por sus siglas en ingles), puede eventualmente acumular carga eléctrica dentro de la capa dieléctrica y, por lo tanto, aumentar la tensión necesaria para hacer funcionar el transistor. A medida que aumenta la tensión umbral, el retardo de conmutación del transistor puede ser más grande.

Se produce otro mecanismo de envejecimiento cuando se aplica una tensión a la puerta, un fenómeno denominado inestabilidad de temperatura de polarización (BTI, por sus siglas en inglés). La BTI puede causar una acumulación de carga en el dieléctrico, entre otros problemas, aunque parte de este efecto desaparece espontáneamente después de eliminar la tensión de la puerta. Esta recuperación se produce en unos pocos microsegundos, lo que dificulta observar cuándo se somete a esfuerzo un transistor y a continuación los efectos resultantes se miden solo después de haber eliminado el esfuerzo.

Otro mecanismo de envejecimiento entra en juego cuando una tensión aplicada a la puerta puede crear defectos eléctricamente activos, conocidos como trampas, dentro del dieléctrico. Cuando las trampas llegan a ser demasiado numerosas, estas trampas de carga pueden unirse y formar un cortocircuito completo entre la puerta y el canal corriente. Este tipo de fallo se denomina ruptura de óxido o ruptura dieléctrica dependiente del tiempo. A diferencia de los otros mecanismos de envejecimiento, que causan una disminución gradual en el rendimiento, la ruptura del dieléctrico puede conducir a un fallo catastrófico del transistor, provocando que el CI funcione mal.

De forma adicional, un fenómeno llamado electromigración puede dañar las conexiones de cobre o aluminio que unen los transistores o los enlaza respecto al mundo exterior. La electromigración puede ocurrir cuando un aumento repentino de la corriente golpea átomos de metal sueltos de las conexiones eléctricas, y puede hacer que fluyan con los electrones. Esto merma el metal de algunos átomos corriente arriba, al tiempo que provoca una acumulación de

metal corriente abajo. El adelgazamiento corriente arriba del metal aumenta la resistencia eléctrica de la conexión, convirtiéndose a veces en un circuito abierto. La deposición corriente abajo puede provocar que el metal sobresalga de su pista designada.

Otro problema relacionado con la fiabilidad de los CI es un fenómeno llamado migración por estrés. Esto se usa para describir el flujo de átomos de metal bajo la influencia de estrés mecánico.

De forma adicional, cualquier defecto, tal como un fenómeno no modelado, defectos de fabricación aleatorios y/o similares, puede causar una degradación de la temporización de una ruta de señales a lo largo del tiempo. Algunos defectos pueden no aparecer durante el ensayo, la verificación, el funcionamiento inicial y/o similares, por ejemplo, el producto con la matriz y el CI puede pasar todos los procedimientos de selección en la etapa de ensayo. Por ejemplo, una vía que incluya defectos de fabricación, tales como una cobertura de metal incompleta, aumentará su resistencia a lo largo del tiempo, y en algún momento provocará un fallo de temporización de una ruta lógica. Por ejemplo, pueden aparecer defectos de fabricación aleatorios en cualquier lugar del CI e incorporar una gran variedad de tipos y niveles de defectos, por lo que los diseños pueden no ser capaces de incorporar factores de seguridad para mitigar estos defectos. Por otro lado, los aspectos de las realizaciones de las técnicas descritas pueden ser capaces de predecir el fallo de cada CI individual basándose en el muestreo de huellas en las pistas apropiadas del CI, y mitigar el fallo mediante un reemplazo anticipativo, acciones correctivas y preventivas, notificaciones a los usuarios, compensaciones en el CI para aumentar la vida útil con el tiempo y/o similares.

La patente US 9.760.672 de Taneja y col. describe un sensor de temporización de ruta crítica que detecta fallos de temporización en la configuración desde una ruta crítica funcional hasta un flip-flop de la ruta. La ruta crítica funcional lleva datos de prueba durante el modo de prueba y datos normales durante el funcionamiento normal del dispositivo. La entrada D y la salida Q del flip-flop de la ruta se comparan mediante una puerta OR-exclusiva (XOR) y se muestrean mediante un flip-flop de captura temprana que está temporizado por un reloj retardado, realizándose el muestreo de D y Q justo después de temporizar el flip-flop de la ruta. Cuando el tiempo de la configuración falla, D y Q difieren justo después del flanco de reloj y se detecta un fallo de temporización.

La patente US 9.564.884 de Quinton y col. describe sensores de temporización de rutas críticas funcionales de conmutación que miden los retardos en rutas críticas funcionales de conmutación que reciben continuamente patrones de un generador de patrones de envejecimiento. El desgaste se acelera. Un controlador de ajuste del margen de retardo hace un barrido del margen de retardos hasta que se producen fallos para medir los retardos. El margen de retardo se ajusta entonces en sensores de temporización de rutas críticas funcionales que añaden el margen de retardo a rutas críticas funcionales que transportan datos de usuario o controles de chip durante el funcionamiento normal.

La patente US 9.536.038 de Quinton y col. describe el software CAD que examina los retardos de las rutas en un diseño de ingenieros de diseño y selecciona primero las rutas más largas. A continuación se examinan todas las rutas que convergen con estas rutas más largas buscando retardos, y se selecciona una ruta convergente más rápida para cada una de las rutas más largas. Las rutas más largas se ordenan de nuevo en función del retardo convergente más rápido, y se seleccionan rutas con rutas convergentes más lentas para que sean rutas críticas funcionales (FCP, por sus siglas en inglés). Se añaden sensores de temporización de rutas críticas funcionales a cada FCP para probar la configuración de tiempo con un margen de retardo añadido.

La patente US 9.564.883 de Quinton y col. describe los sensores de temporización de rutas críticas funcionales de conmutación que miden retardos en las rutas críticas funcionales de conmutación que son réplicas de rutas críticas reales o representaciones de rutas de retardo en el peor de los casos. Un flip-flop de conmutación o un registro de desplazamiento con retroalimentación lineal (LFSR, por sus siglas en inglés) dirige patrones de prueba de densidad de transición alta para las rutas críticas funcionales de conmutación. Cuando un retardo de la ruta crítica funcional de conmutación no cumple con el requisito de configuración de temporización para un siguiente registro, los sensores de temporización de rutas críticas funcionales de conmutación señalan un controlador para aumentar la tensión de trabajo interno del dispositivo (VDD, por sus siglas en inglés).

Los ejemplos anteriores de la técnica relacionada y las limitaciones de los mismos pretenden ser ilustrativos y no exclusivos. Otras limitaciones de la técnica relacionada resultarán evidentes para los expertos en la técnica tras una lectura de la memoria descriptiva y un estudio de las figuras.

**Resumen**

Las siguientes realizaciones y aspectos de las mismas se describen e ilustran junto con sistemas, herramientas y métodos que pretenden ser ejemplares e ilustrativos, no limitantes en su alcance.

Se proporciona un circuito integrado (CI) semiconductor según la reivindicación independiente 1. Se definen realizaciones adicionales en las reivindicaciones dependientes correspondientes. La descripción y los dibujos también presentan aspectos, ejemplos, implementaciones y realizaciones no reivindicadas adicionales para la mejor comprensión de las realizaciones reivindicadas.

El CI comprende: una ruta de datos que comprende rutas de bits paralelas, terminando cada una de las rutas de bits paralelas con un flip-flop; un combinador de rutas de señales, que comprende una pluralidad de rutas de entrada y una salida, basándose la salida en una combinación de señales respectivas recibidas en cada una de las rutas de entrada, en donde cada una de las rutas de entrada está conectada a una entrada de cada uno de los diferentes flip-flops de la ruta de datos, de manera que cada una de las señales recibidas en las rutas de entrada son una señal respectiva recibida por el flip-flop respectivo de la ruta de datos. El CI comprende un circuito de retardo que tiene una salida y una entrada conectadas eléctricamente al combinador de rutas de señales, estando el circuito de retardo configurado para aplicar, en un tiempo diferente, respectivos diferentes retardos a una señal recibida en la entrada del circuito de retardo, para proporcionar, en la salida del circuito de retardo, respectivas señales retardadas diferentes de los diferentes retardos. El CI comprende un circuito de comparación dispuesto para proporcionar salidas de comparación basándose cada una en una comparación de la salida del combinador de rutas de señales y una diferente de las señales retardadas, en donde las salidas de comparación se proporcionan en al menos una señal de datos de comparación a al menos un circuito de mitigación. El circuito de mitigación es al menos un circuito del grupo que consiste en: un circuito de notificación; un circuito de medición de retardos de temporización; un circuito de transmisión de datos; un circuito de compensación de antienvejecimiento del CI; y un circuito de análisis de fallos.

En algunas realizaciones, el combinador de rutas de señales es uno o más del grupo que consiste en un combinador lógico XOR, un combinador de paridad de Hamming y un multiplexor.

En algunas realizaciones, el tiempo de retardo variable se establece en un múltiplo entero de incrementos iguales a un período de reloj del CI dividido por un tamaño del vector de la firma, y en donde el tamaño del vector de la firma está entre 1 y 100.000.

En algunos ejemplos, el circuito de mitigación es un circuito de transmisión de datos conectado electrónicamente a un servidor computarizado, en donde el servidor computarizado está configurado para recibir múltiples instancias de la señal de datos de comparación, realizar un análisis de predicción de fallos de las señales de datos de comparación y enviar una notificación a un módulo de mitigación cuando el análisis de predicción de fallos predice el fallo del CI dentro de un tiempo predefinido.

En algunos ejemplos, al menos algunas de las señales de datos de comparación se generan en múltiples valores del tiempo de retardo variable.

En algunos ejemplos, al menos algunas de las señales de datos de comparación se generan a partir de múltiples ejemplos de uno o más valores a partir de múltiples valores del tiempo de retardo variable.

En algunos ejemplos, el análisis de predicción de fallos comprende uno o más de un análisis de aprendizaje automático, un análisis de tendencias, un análisis de seguimiento de múltiples objetos y un análisis multivariante.

En algunos ejemplos, el análisis de predicción de fallos comprende recibir señales de datos de comparación de múltiples CI diferentes.

En algunos ejemplos, el análisis de predicción de fallos comprende recibir resultados de análisis de predicción de fallos de múltiples CI diferentes.

En una realización, el CI comprende además: un primer circuito de almacenamiento interno, conectado eléctricamente a la salida del combinador de rutas de señales y dispuesto para proporcionar la salida del combinador de rutas de señales almacenadas como una primera entrada al circuito de comparación; y un segundo circuito de almacenamiento interno, conectado eléctricamente a la señal retardada y dispuesto para proporcionar la señal retardada como una segunda entrada al circuito de comparación.

En determinadas realizaciones, el combinador de rutas de señales es un combinador de primera ruta de señales dispuesto para recibir una pluralidad de señales de una primera fuente de datos y el circuito de comparación es un primer circuito de comparación. A continuación, el CI puede comprender además: un combinador de segunda ruta de señales, que comprenda una pluralidad de rutas de entrada y una salida, basándose la salida del combinador de segunda ruta de señales en una combinación de señales respectivas recibidas en cada una de las rutas de entrada, recibiéndose las señales de una segunda fuente de datos; un multiplexor, configurado para recibir la salida del combinador de primera ruta de señales, la salida del combinador de segunda ruta de señales y una señal de selección y para emitir de forma selectiva la salida del combinador de primera ruta de señales o la salida del combinador de segunda ruta de señales basándose en la señal de selección, proporcionándose la salida del multiplexor como la entrada al circuito de retardo; un segundo circuito de comparación dispuesto para proporcionar una salida de segunda comparación basándose en una comparación de la salida del combinador de segunda ruta de señales y la señal retardada; y una puerta OR dispuesta para recibir como entradas la salida de la primera comparación y la salida de la segunda comparación y para proporcionar una salida como la señal de datos de comparación al, al menos, un circuito de mitigación.

Opcionalmente, el CI comprende además: un circuito de almacenamiento de la primera comparación, dispuesto para recibir la salida de la primera comparación y controlado por una primera señal de reloj; un circuito de almacenamiento de la segunda comparación, dispuesto para recibir la salida de la segunda comparación y controlado por una segunda señal de reloj; y en donde el circuito de almacenamiento de la primera comparación está dispuesto para proporcionar la salida de la primera comparación como una primera entrada a la puerta OR y el circuito de almacenamiento de la segunda comparación está dispuesto para proporcionar la salida de la segunda comparación como una segunda entrada a la puerta OR.

En algunos ejemplos, cada una de la pluralidad de rutas de entrada del combinador de rutas de señales está configurada para recibir una de: una señal de una fuente de datos respectiva en el CI; una señal de un circuito de memoria; y una señal de uno de una pluralidad de circuitos lógicos agrupados por una habilitación de reloj.

Sin ser conforme a las reivindicaciones, pero útil para comprender la invención, puede considerarse un método para usar un circuito integrado (CI) semiconductor, comprendiendo el método: combinar las señales respectivas recibidas en cada una de una pluralidad de rutas de entrada en un combinador de rutas de señales para proporcionar una salida; retardar la salida del combinador de rutas de señales durante un tiempo de retardo variable en un circuito de retardo para emitir una señal retardada; y comparar la salida del combinador de rutas de señales y la señal retardada para proporcionar una salida de comparación y proporcionar la salida de comparación en una señal de datos de comparación a al menos un circuito de mitigación.

**Breve descripción de las figuras**

Las realizaciones ilustrativas se ilustran en las figuras referenciadas. Las dimensiones de los componentes y las características mostradas en las figuras se eligen generalmente por conveniencia y para una presentación más clara y no necesariamente se muestran a escala. Las figuras se enumeran a continuación.

La Figura 1 muestra esquemáticamente un sistema computarizado para la medición del margen del CI y la predicción de fallos;

la Figura 2 muestra diagramas de flujo de métodos para la medición del margen del CI y la predicción de fallos;

la Figura 3, la Figura 3A y la Figura 3B muestran diagramas de circuitos basados en XOR respectivos para la medición del margen del CI y la predicción de fallos;

la Figura 4 muestra un diagrama de circuitos basado en MUX para la medición del margen del CI y la predicción de fallos;

la Figura 5 muestra un diagrama de circuitos para el modo antienvejecimiento del CI;

la Figura 6 muestra un diagrama de temporización de un retardo de señal para la medición del margen del CI y la predicción de fallos;

la Figura 7 muestra un gráfico de errores frente al tiempo del ciclo para un primer experimento;

la Figura 8 muestra un gráfico de errores frente al tiempo del ciclo para un segundo experimento;

la Figura 9 muestra un diagrama de temporización de dos retardos de señal para la medición del margen del CI y la predicción de fallos;

la Figura 10 muestra un gráfico de errores frente al tiempo del ciclo para un tercer experimento; y

la Figura 11 muestra un diagrama del mapa del margen de una unidad.

**Descripción detallada**

En la presente memoria se describen métodos y dispositivos para determinar y predecir un fallo futuro del circuito integrado individual. También se describe un circuito de medición del margen de retardo de temporización para un CI, desde su primera operación y/o a lo largo del tiempo (por ejemplo, durante cualquier período de tiempo desde o posterior a su primera operación). Se coloca un circuito dedicado (que puede ser detector), tal como un circuito de predicción de fallos (FPC, por sus siglas en inglés) o un circuito de medición del margen y de predicción de fallos (MFPC, por sus siglas en inglés), en puntos seleccionados a lo largo de una o más rutas de datos en un circuito integrado digital (tal como uno o más FPC o MFPC por ruta de datos), donde cada circuito dedicado combina múltiples rutas de datos individuales en un menor número de rutas de prueba. Al dividir cada señal de prueba en dos y aplicar un circuito de retardo a una de las rutas de señales divididas, puede adquirirse una huella o firma de los retardos de cada ruta de la ruta de datos durante cada ciclo de reloj de la unidad funcional. Como se utiliza en la presente memoria, el término “huella” y/o “firma” significa el perfil de intensidades de señal, tales como un vector, serie y/o similares, que

se obtiene de una medición de márgenes de retardo de temporización de una combinación de señales de una ruta de datos. Para cada ciclo de reloj de la unidad funcional, la ruta de datos de salida puede tener un valor de datos diferente. Por lo tanto, durante cada ciclo de reloj, puede probarse una combinación diferente de las rutas lógicas dentro de la unidad funcional, produciendo una huella diferente. Al recopilar un gran número de huellas a lo largo del tiempo, puede analizarse un conjunto de datos de huellas. El análisis de los conjuntos de datos de huellas puede determinar el rendimiento y/o predecir el fallo futuro del CI individual.

En términos generales, puede considerarse un circuito integrado (CI) semiconductor que comprenda: un combinador de rutas de señales, que comprenda una pluralidad de rutas de entrada (por ejemplo, para recibir señales en una fuente de datos o ruta de datos, desde un circuito de memoria y/o desde circuitos lógicos agrupados por una habilitación de reloj) y una salida, basándose la salida en una combinación de señales respectivas recibidas en cada una de las rutas de entrada; un circuito de retardo que tenga una entrada conectada eléctricamente a la salida del combinador de rutas de señales, retardando el circuito de retardo una señal de entrada durante un tiempo de retardo variable para emitir una señal retardada; y un circuito de comparación dispuesto para proporcionar una salida de comparación basándose en una comparación de la salida del combinador de rutas de señales y la señal retardada, en donde la salida de comparación se proporciona en una señal de datos de comparación a al menos un circuito de mitigación. La combinación del combinador de rutas de señales, el circuito de retardo y el circuito de comparación puede proporcionar un FPC o un MFPC.

También puede considerarse un método para usar tal CI (en el que el uso puede comprender uno de más de funcionamiento, análisis y configuración, por ejemplo). Por ejemplo, esto puede incluir un método para usar un circuito integrado (CI) semiconductor. El método puede comprender: combinar las señales respectivas recibidas en cada una de una pluralidad de rutas de entrada en un combinador de rutas de señales para proporcionar una salida; retardar la salida del combinador de rutas de señales durante un tiempo de retardo variable en un circuito de retardo para emitir una señal retardada; y comparar la salida del combinador de rutas de señales y la señal retardada para proporcionar una salida de comparación y proporcionar la salida de comparación en una señal de datos de comparación a al menos un circuito de mitigación.

También puede considerarse que las etapas de combinar, retardar y comparar puedan repetirse para cada uno de una pluralidad de tiempos de retardo. De esta manera, puede proporcionarse una pluralidad de salidas de comparación. De este modo, puede determinarse una característica de identificación (es decir, una firma o huella digital) para el CI basándose en la pluralidad de salidas de comparación. Repitiendo este proceso en diferentes ciclos de reloj, pueden determinarse múltiples de tales huellas. A continuación, las huellas pueden rastrearse en diferentes tiempos, por ejemplo, rastreando cambios en la huella a lo largo del tiempo (usando intervalos al menos tan largos como la cantidad de tiempo que se tarda en determinar una huella única y preferiblemente más larga).

También pueden proporcionarse características de método opcionales adicionales correspondientes a las etapas implementadas por cualquiera de las características descritas con referencia al CI. Los ejemplos de estas pueden explicarse a continuación. Las realizaciones específicas también se explicarán a continuación, pero también se hará referencia adicional a significados o términos generalizados de la descripción.

Obsérvese que una ruta de datos es un ejemplo de un estilo de diseño que puede manejarse mediante el FPC o el MFPC, otros ejemplos pueden ser circuitos de memoria (el FPC/MFPC se ubica en la salida de la memoria) y otros circuitos lógicos agrupados con respecto a una determinada habilitación de reloj.

Opcionalmente, los aspectos de las realizaciones descritas en la presente memoria pueden aplicarse a cualquier problema de fiabilidad del rendimiento del CI, tal como el envejecimiento, defectos latentes que se manifiestan en el diseño y provocan la degradación, diferencias de fabricación dentro de/entre los CI, diferencias de fabricación entre fábricas y/o similares. Las técnicas descritas pueden encontrar cambios en los retardos de temporización de cualquier fuente o causa, predecir un fallo futuro antes de que el fallo del CI provoque un fallo de dispositivo/sistema, y permitir la acción correctiva y preventiva antes del fallo del CI específico. Si bien los problemas de fiabilidad, tales como el envejecimiento, la electromigración y/o similares, se usan aquí como ejemplos, las técnicas también pueden aplicarse a defectos latentes, tales como defectos aleatorios, defectos sistemáticos, defectos desconocidos y/o similares.

Opcionalmente, el retardo puede cambiarse en pasos de pequeños tiempos, produciendo uno o más barridos de retardos de tiempo y huellas asociadas en cada retardo de tiempo diferente. El barrido puede analizarse para determinar el funcionamiento del CI individual, predecir un fallo futuro del CI y/o similares.

Opcionalmente, uno o más conjuntos de datos (por ejemplo, de señales en el CI) pueden analizarse combinatoriamente para determinar los retardos operativos de cada ruta de la ruta de datos (o ruta de señal equivalente), cada ruta de procesamiento lógico de la unidad funcional y/o similares.

Opcionalmente, pueden analizarse estadísticamente uno o más conjuntos de datos para predecir un fallo futuro del CI. Por ejemplo, una tendencia de degradación del CI puede analizarse en uno o más márgenes de retardo medidos usando el circuito de predicción de fallos, tal como analizar un cambio de margen de retardo mínimo a lo largo del tiempo.

Opcionalmente, uno o más conjuntos de datos pueden analizarse usando aprendizaje automático para monitorizar el fallo del CI, predecir un fallo futuro del CI y/o similares.

Opcionalmente, uno o más conjuntos de datos pueden analizarse para diseñar un CI futuro.

Opcionalmente, uno o más barridos pueden analizarse combinatoriamente para determinar los retardos operativos de cada ruta de la ruta de datos, cada ruta de procesamiento lógico de la unidad funcional y/o similares.

Opcionalmente, uno o más barridos pueden analizarse estadísticamente para predecir un fallo futuro del IC. Por ejemplo, un análisis de regresión de uno o más barridos determina los cambios en los retardos de temporización, y una extrapolación a un valor de fallo del retardo de temporización determina el tiempo hasta el fallo.

Opcionalmente, uno o más barridos pueden analizarse usando aprendizaje automático para monitorizar el fallo del CI, predecir un fallo futuro del CI y/o similares.

Opcionalmente, uno o más barridos de tiempo de retardo pueden analizarse para diseñar un CI futuro, donde el CI futuro se diseña para evitar los fallos de los CI anteriores.

Opcionalmente, uno o más barridos se analizan usando el aprendizaje automático al inicio de la vida del chip, por ejemplo, la firma de los márgenes de retardo de temporización o la huella del CI al inicio de la vida. La firma o huella pueden usarse para la detección/selección de valores atípicos del chip, es decir, un CI específico recibe una identidad única y la firma en comparación con otros CI que permiten detectar anomalías en una fabricación a gran escala.

A continuación se hace referencia a la Figura 1 y la Figura 2, que muestran esquemáticamente un sistema informatizado 100 y diagramas (200 y 210) de flujo de métodos, respectivamente, para la predicción de fallos del CI y la medición de márgenes de rutas lógicas en las pruebas del CI (aparato de pruebas o nivel del sistema). El sistema 100 comprende un CI 150, un ordenador 101A y una conexión 140 de interfaz de datos que conecta los dos. El CI 150 comprende múltiples unidades funcionales (como en 151, 152, 153 y similares) y rutas de datos (como en 141, 142A, 142B, 143A, 143B y similares, que pueden incluir lógica sintetizada) entre ellas. El CI 150 comprende circuitos de medición de margen y predicción de fallos (MFPC; como en 131, 132, 133 y similares) para capturar señales de rutas de datos (como en 142A, 143A y similares), y determinar temporizaciones de retardo de al menos algunas señales desde la ruta de datos respectiva. Los MFPC 131, 132 o 133 combinan 201 señales desde la ruta de datos y prueban 202 uno o más retardos de las señales combinadas. El CI 150 comprende una interfaz de datos para conectarse a la conexión 140 de interfaz de datos y enviar 202 las temporizaciones de retardo al ordenador 101A. Los datos de temporización de retardo recopilados para múltiples señales de las rutas de datos y/o para múltiples valores de retardo, tal como el cambio 204 del retardo, pueden considerarse la huella de las temporizaciones de retardo.

El ordenador 101A comprende uno o más procesadores 101B de hardware, una interfaz 120 de usuario y un medio 102 de almacenamiento no transitorio legible por ordenador. El medio de almacenamiento comprende un código de programa, tal como un receptor 102A de datos del MFPC, un analizador 102B de envejecimiento del CI, un predictor 102C de fallos del CI y/o similares, comprendiendo el código de programa instrucciones que, cuando se ejecutan en el procesador o procesadores 101B de hardware, hacen que el procesador o procesadores 101B de hardware reciban 211 los datos de retardo de la señal (es decir, las huellas) usando una interfaz 110 de datos, tal como usando el receptor 102A de datos del MFPC. El analizador 102B de envejecimiento del CI analiza 212 las huellas, y el predictor 102C de fallos del CI notifica 213 a un operador un estado, una predicción de fallo, una acción preventiva y o similares, tal como usando la interfaz 120 de usuario.

Opcionalmente, las temporizaciones de retardo son analizadas por un circuito (no mostrado) del CI 150 para determinar cuándo las modificaciones 206 del reloj y/o lógicas en el CI 150 mejoran la vida útil del CI 150 antes del fallo. Opcionalmente, las temporizaciones de retardo son analizadas por un circuito (no mostrado) del CI 150 y se emite una notificación 206 del estado o la predicción de fallos.

Opcionalmente, la huella de la temporización de retardo puede generarse en las pruebas del CI (aparato de pruebas o sistema) para extraer el mapa de margen de tiempo cero de las rutas de datos en una determinada unidad.

La huella puede analizarse en un tiempo de operación inicial y monitorizarse a lo largo de la vida del CI para determinar cuándo puede producirse un fallo previsto. Por ejemplo, un análisis del gradiente de degradación del defecto puede determinar el tiempo futuro de un fallo del CI. Por ejemplo, analizar el margen mínimo de una huella, representar el margen mínimo a lo largo del tiempo y extrapolar el gráfico a un margen de retardo de cero determina el tiempo previsto de fallo.

A continuación se hace referencia a la Figura 3, que muestra un diagrama de circuitos basado en XOR para la predicción de fallos del CI. Un componente XOR (XOR1) combina las señales de una ruta de datos, tales como 64, 128, 256, 512 o el número similar de señales en una única señal XOR1_out. XOR1_out se alimenta a un primer flip-flop FF2 y una línea de retardo D2. El XOR1_out retardado se alimenta a un segundo flip-flop FF1. FF1 y FF2 son

activados por un reloj clk_3, y sus salidas XOR combinadas con XOR2. XOR2_out es una lógica 1 para cada retardo donde uno de XOR1_out y XOR1_out_d2 es lógica 1 en el tiempo de clk_d1.

Por lo tanto, múltiples instancias de clk_d1 y/o múltiples valores de D1 pueden determinar los datos de retardo de la temporización del retardo a lo largo de las rutas de datos de la FU1 lógica combinatoria (de la rama de la matemática "combinatoria") y, por lo tanto, la huella de los retardos de temporización. Al analizar estos retardos de temporización a lo largo del tiempo, el MFPC puede detectar cuál de las rutas de FU1 se degrada y/o envejece más rápido, y puede provocar el fallo del CI 150.

La señal de salida de XOR1 puede considerarse una compresión de las señales de entrada que preserva los retardos mínimos del margen de temporización de las señales de entrada de la ruta de datos. La salida de XOR2 puede ser logic-1 cuando el margen mínimo de una señal de entrada es menor que el retardo asociado a D2. Por lo tanto, XOR1 puede ser un verificador de paridad, es decir, la salida es lógica 1 cuando la paridad de las señales de entrada es lógica 1. Cada flanco de subida de la señal comprimida (salida XOR1) puede asociarse a un flanco de subida de una de las señales de entrada. Para el caso simple en el que el margen mínimo de retardo de temporización esté asociado solo a una entrada, las últimas transiciones de subida o de bajada de la salida de XOR1 representan el margen mínimo. Este concepto puede demostrarse mediante una prueba matemática, descrita a continuación, así como mediante simulaciones basadas en eventos. Por ejemplo, se pueden demostrar casos especiales por simulación, donde el margen de varias señales es menor que D2, múltiples señales conmutadas simultáneamente y/o similares.

En los términos generales considerados anteriormente, el CI puede comprender además: un primer circuito de almacenamiento interno, conectado eléctricamente a la salida del combinador de rutas de señales y dispuesto para proporcionar la salida del combinador de rutas de señales almacenada como una primera entrada al circuito de comparación; y un segundo circuito de almacenamiento interno, conectado eléctricamente a la señal retardada y dispuesto para proporcionar la señal retardada como una segunda entrada al circuito de comparación. Sin embargo, tal configuración es opcional, como se explicará ahora.

A continuación se hace referencia a la Figura 3A, que muestra una versión diferente de un diagrama de circuitos basado en XOR para la predicción de fallos del CI, en comparación con la mostrada en la Figura 3. La ruta de datos mostrada en la Figura 3A tiene prácticamente la misma estructura que la mostrada en la Figura 3. En esta versión, un componente XOR, XOR1a, combina las señales de la ruta de datos, tal como 64, 128, 256, 512 o el número similar de señales, en una única señal de salida, $XOR1a_{out}$. $XOR1a_{out}$ se alimenta como una primera entrada a un segundo circuito XOR, XOR2a, y en paralelo a una línea de retardo D2, cuya salida proporciona una segunda entrada al segundo circuito XOR, XOR2a. La señal de salida retardada del segundo circuito XOR, XOR2a, $XOR2a_{out}$, se alimenta a un flip-flop FF1a. El flip-flop FF1a es activado por un reloj (clk1a). La segunda señal de salida $XOR2_{out}$ es una lógica 1 para cada retardo donde las dos entradas del segundo circuito XOR, XOR2a, están en un estado lógico diferente en el tiempo de clk1a.

A continuación se hace referencia a la Figura 3B, que muestra otra versión diferente de un diagrama de circuitos basado en XOR para la predicción de fallos del CI, en comparación con la mostrada en la Figura 3. En esta versión, se proporcionan dos circuitos de predicción de fallos basados en XOR que usan un circuito de línea de retardo. En otras palabras, se proporcionan dos rutas de datos, cada una de las cuales puede ser conforme a la mostrada en la Figura 3 o la Figura 3A. El primer circuito de predicción de fallos comprende: un primer componente XOR, XOR1a, que es accionado por un conjunto de señales de entrada paralelas de una primera ruta de datos (como se ha explicado anteriormente con referencia a la Figura 3 o la Figura 3A); un segundo componente XOR, XOR2a; y un primer flip-flop FF1a que está cronometrado por una primera señal de reloj clk1a. El segundo circuito de predicción de fallos comprende: un tercer componente XOR, XOR1b, que es accionado por un conjunto de señales de entrada paralelas de una segunda ruta de datos (como se explica con referencia a la Figura 3 o la Figura 3A anteriormente); un cuarto componente XOR, XOR2b; y un segundo flip-flop FFlb que está cronometrado por una segunda señal de reloj clklb. Una línea de retardo común D2 da a los dos circuitos de predicción de fallos un multiplexor MUX que selecciona, en un modo de compartición de tiempo, si la salida del primer componente XOR, XOR1a, o la salida del tercer componente XOR, XOR1b, se proporciona como una entrada a la línea de retardo común D2. Esto se controla usando una señal de selección: In/out sel. La configuración de cada uno de los dos circuitos de predicción de fallos es, por lo demás, como se muestra en la Figura 3A. La salida del primer flip-flop FF1a cronometrada por la primera señal de reloj clk1a y la salida del segundo flip-flop FFlb cronometrada por la segunda señal de reloj clklb se proporcionan como entradas a una puerta OR para generar una señal de salida HT-out. Cuando el multiplexor MUX conecta la salida del primer componente XOR, XOR1a, a la entrada de la línea de retardo D2, la señal de salida HT-out es una lógica 1 para cada retardo donde las dos entradas del segundo componente XOR, XOR2a, están en un estado lógico diferente en el tiempo de la primera señal de reloj clk1a. Cuando el multiplexor MUX conecta la salida del tercer componente XOR, XOR1b, a la entrada de la línea de retardo D2, la señal de salida HT-out es una lógica 1 para cada retardo donde las dos entradas del cuarto componente XOR, XOR2b, están en un estado lógico diferente en el tiempo de la segunda señal de reloj clklb.

En términos generales, se puede considerar además que el combinador de rutas de señales es un combinador de primera ruta de señales dispuesto para recibir una pluralidad de señales de una primera fuente de datos (que puede ser una ruta de datos u otro conjunto de señales como se explica en la presente memoria) y el circuito de comparación

es un primer circuito de comparación. Entonces, se puede considerar que el CI comprende además un combinador de segunda ruta de señales, que comprende una pluralidad de rutas de entrada y una salida, basándose la salida del combinador de segunda ruta de señales en una combinación de señales respectivas recibidas en cada una de las rutas de entrada, recibiéndose las señales de una segunda fuente de datos. Además, se puede proporcionar un multiplexor, configurado para recibir la salida del combinador de primera ruta de señales, la salida del combinador de segunda ruta de señales y para emitir de forma selectiva la salida del combinador de primera ruta de señales o la salida del combinador de segunda ruta de señales basándose en una señal de selección recibida. La salida del multiplexor puede proporcionarse como la entrada al circuito de retardo (de manera que el circuito de retardo es común para los combinadores tanto de primera como de segunda ruta de señales). El CI puede comprender además un segundo circuito de comparación dispuesto para proporcionar una salida de segunda comparación basándose en una comparación de la salida del combinador de segunda ruta de señales y la señal retardada (que, de este modo, puede ser común a los circuitos tanto de la primera como de la segunda comparación). Una puerta OR puede estar dispuesta además para recibir como entradas la salida de la primera comparación y la salida de la segunda comparación y para proporcionar una salida como la señal de datos de comparación al, al menos, un circuito de mitigación. Con referencia al aspecto del método, este puede comprender además: combinar respectivas señales recibidas en cada una de una pluralidad de rutas de entrada en un combinador de segunda ruta de señales para proporcionar una salida, recibiéndose las señales de una segunda fuente de datos; recibir la salida del combinador de primera ruta de señales, la salida del combinador de segunda ruta de señales y una señal de selección en un multiplexor y emitir de forma selectiva la salida del combinador de primera ruta de señales o la salida del combinador de segunda ruta de señales basándose en la señal de selección, proporcionándose la salida del multiplexor como la entrada al circuito de retardo de manera que la etapa de retardo comprende retardar la salida del combinador de primera ruta de señales o la salida del combinador de segunda ruta de señales durante el tiempo de retardo variable en el circuito de retardo para emitir la señal retardada; comparar la salida del combinador de segunda ruta de señales y la señal retardada para proporcionar una salida de segunda comparación; y recibir, en una puerta OR, la salida de primera comparación y la salida de segunda comparación como entradas y emitir la señal de datos de comparación como una salida de la puerta OR al, al menos, un circuito de mitigación.

Opcionalmente, un circuito de almacenamiento de la primera comparación, controlado por una primera señal de reloj, puede disponerse para recibir la salida de primera comparación. A continuación, un circuito de almacenamiento de la segunda comparación, controlado por una segunda señal de reloj (que puede ser igual o diferente de la primera señal de reloj) puede disponerse para recibir la salida de segunda comparación. El circuito de almacenamiento de primera comparación está dispuesto, de forma ventajosa, para proporcionar la salida de la primera comparación como una primera entrada a la puerta OR y el circuito de almacenamiento de segunda comparación está dispuesto para proporcionar la salida de la segunda comparación como una segunda entrada a la puerta OR.

A continuación se hace referencia a la Figura 4, que muestra un diagrama de circuitos basado en MUX para la predicción de fallos del CI. Un multiplexor (Mux_sel) se usa para seleccionar una o más de las rutas de datos, y a continuación detectar una huella de temporización de retardo como se describe en la presente memoria. La ventaja con el MFPC basado en MUX es que la única señal se selecciona para la temporización de retardo en un tiempo, por lo que el fallo puede detectarse con menos datos (tal como con un circuito de análisis dedicado en el CI). Opcionalmente, puede usarse un MFPC híbrido basado en MUX/XOR que combine algunas de las ventajas de cada tipo de MFPC.

A continuación se hace referencia a la Figura 5, que muestra un diagrama de circuitos para el modo antienvejecimiento del CI. La figura muestra una técnica de antienvejecimiento que desactiva el circuito XOR cuando el circuito MFPC no está habilitado, es decir, el reloj del MFPC se desconecta cíclicamente. Cuando el circuito está deshabilitado, un retardo lógico constante aumentará la degradación del circuito, tal como debido a los efectos de la inestabilidad por polarización negativa (NBTI, por sus siglas en inglés). Para mitigar la degradación por NBTI, el circuito XOR se conmuta siempre que el reloj del MFPC se desconecte cíclicamente. De forma alternativa, la degradación del margen se monitoriza en cada una de las señales por separado. La Figura 5 es solo un ejemplo de realizaciones alternativas de correcciones de circuitos que pueden realizarse para compensar la degradación y/o el envejecimiento del circuito CI. Pueden usarse muchos otros circuitos ilustrativos.

Las técnicas descritas en la presente memoria pueden expandirse a otros tipos de rutas/señales lógicas, longitudes de rutas y diferentes tipos de elementos electrónicos de generación y muestreo. Por ejemplo, las rutas de fase, las rutas lógicas basadas en un dispositivo de almacenamiento sensible a nivel, las rutas lógicas de reloj desconectado cíclicamente, las señales lógicas de temporización de caída del flip-flop (FF) y/o similares. Por ejemplo, las realizaciones pueden detectar un fallo de retención (retardo mín.) que es causado por una degradación de retardo en la ruta del reloj. En este ejemplo, una nueva ruta de retardo (tal como D4) se ubica entre el reloj de FF1 y de FF2 de manera que el valor de retardo D4 retarda el reloj de FF2.

El MFPC puede encenderse o activarse siempre por una señal de habilitación. Por ejemplo, una señal de habilitación representa una OR lógica de las señales de habilitación correspondientes al grupo de los FF que son muestreados por el MFPC. Cuando la habilitación es baja, el MFPC puede entrar en un modo de detección de antienvejecimiento del CI, donde se usa un reloj dedicado para conmutar el MFPC para mitigar los efectos de envejecimiento por NBTI.

Cuando el MFPC cubre grandes áreas lógicas (FU) del CI, el MFPC se puede usar como una firma del margen de retardo de temporización o huella del CI en la primera operación. Con el tiempo, el MFPC puede medir la firma del margen en diferentes momentos para analizar y detectar el gradiente de tiempo de la degradación/envejecimiento del CI. Diferentes funciones de gradiente pueden estar relacionadas con diferentes tipos de defectos y modos de degradación.

Opcionalmente, la firma comprende múltiples márgenes de retardo superpuestos, y se identifican varios márgenes críticos de retardo de temporización como que tienen diferentes gradientes de tiempo cada uno, y cada uno se analiza por separado para predecir un fallo futuro del CI. Por ejemplo, los métodos de correlación espaciotemporal no lineal se usan para rastrear múltiples márgenes de retardo de temporización simultáneamente desde una serie de firmas o huellas, representando cada firma o huella un vector unidimensional de todos los retardos de temporización superpuestos. Por ejemplo, se realiza una transformación de múltiples vectores unidimensionales para producir una representación de datos en dos o más dimensiones. Por ejemplo, Laube y col. publicado en 2002, "Analyzing Relative Motion within Groups of Trackable Moving Point Objects", en Lecture Notes in Computer Science (Egenhofer y col. - editores - Geographic Information Science, GIScience 2002), vol. 2478 (Springer, Berlín, Heidelberg), páginas 132-144.

Cuando el rendimiento de los circuitos integrados semiconductores se degrada a lo largo del tiempo, la progresión de los defectos físicos puede aumentar gradualmente el tiempo de retardo de los circuitos CI. El CI puede fallar cuando el tiempo de retardo excede el tiempo del ciclo del reloj del CI. Las técnicas existentes de detección de defectos pueden detectar defectos después de que se produzca el fallo, pero cuando se predice un fallo eminente, puede realizarse un mantenimiento anticipativo. Esto es especialmente importante para aplicaciones en las que el coste de un fallo es alto (tal como vehículos autónomos), el coste de reemplazo es alto (tal como el fallo del CI de un satélite), el coste de un fallo para la imagen de un producto es alto (tal como una experiencia de usuario negativa creada por un fallo) y/o similares. Una realización de un circuito integrado (CI) utilizando las técnicas descritas en la presente memoria incluye un circuito de predicción de fallos y un sistema que puede alertar de un fallo inminente antes de que ocurra el fallo.

Por ejemplo, en el sentido generalizado explicado anteriormente, el tiempo de retardo variable puede establecerse en un múltiplo entero de incrementos iguales a un período del reloj del CI dividido por un factor (un "tamaño del vector de la firma"), que es preferiblemente de 1 a 100.000.

En algunas realizaciones, el circuito de predicción de fallos comprende un par de componentes de almacenamiento (por ejemplo, flip-flops) que reciben una salida de señal de datos desde un gran número de rutas del CI, tales como una ruta de datos, rutas de memoria, rutas lógicas y/o similares. Para reducir la sobrecarga, la señal de datos se reduce usando códigos de Hamming, códigos de paridad, otras técnicas de corrección de errores y/o similares antes de almacenarse en los dos componentes de almacenamiento. Los dos componentes de almacenamiento difieren entre sí en las temporizaciones de entrada de la señal de datos, las temporizaciones de entrada de la señal del reloj, la fase de señales de entrada, los umbrales lógicos de entrada de la señal de datos y/o similares. Por ejemplo, se usa un circuito de temporización variable para retardar la señal a uno de los flip-flops.

El FPC o el MFPC incluye además componentes electrónicos que determinan (a) coincidencia o falta de coincidencia de las salidas desde los dos componentes de almacenamiento, y (b) lo cerca que el retardo entre salidas no coincidentes está del tiempo de ciclo del reloj del CI.

En funcionamiento, después de que se haya determinado la coincidencia o la falta de coincidencia de las salidas de señal (tal como usando un componente XOR), el circuito de predicción de fallos incrementa la temporización de entrada, la temporización de entrada de la señal del reloj o los umbrales lógicos de entrada de uno de los componentes de almacenamiento, y la coincidencia o la falta de coincidencia de las salidas se determina de nuevo. Este ciclo puede repetirse con pequeños incrementos.

Se mantiene un registro de la longitud relativa del retardo detectado en comparación con el tiempo del ciclo del reloj, así como del incremento de los componentes de almacenamiento utilizados. El análisis, tal como detección de tendencias, análisis combinatorio, aprendizaje automático, análisis de regresión, detección de anomalías y/o similares, puede realizarse sobre los datos registrados para estimar cuándo la degradación del CI puede llegar a un momento en el que el CI falle, tal como cuando el retardo de la ruta lógica más corta excede el tiempo de ciclo posterior del reloj.

Esta medición y/o estimación puede utilizarse de varias maneras. Puede emitirse una alerta al usuario del sistema donde está implementado el CI indicando bien el margen (cómo de cerca está el retardo del tiempo de ciclo del reloj del CI) o bien el tiempo estimado de fallo. Además, el agente puede indicar un cambio operativo del CI, tal como la reducción de la tensión o de la velocidad del reloj, que puede posponer el fallo y prolongar la vida útil del CI.

Al monitorizar continuamente circuitos lógicos en la salida de la ruta de datos usando un pequeño número de componentes, pueden conservarse recursos, tales como el área del CI, la energía y/o similares, en relación con las técnicas existentes.

Por ejemplo, las señales de entrada se comprimen para generar un código de Hamming (comprimido en el espacio de Hamming). El código de Hamming puede usarse para un proceso de detección, corrección y/o predicción de errores de mayor orden. Por ejemplo, un circuito basado en XOR se usa para combinar todas las señales de una ruta de datos en una ruta de dos señales unificadas que implemente una operación lógica de módulo 4. Además o como alternativa pueden usarse otros tipos de código (fuente) de compresión.

En los términos generales explicados anteriormente, puede entenderse que el combinador de rutas de señales (o al menos uno de los combinadores de rutas de señales) comprende al menos uno de un combinador lógico XOR (como se muestra en la Figura 3 o la Figura 3A), un combinador de paridad de Hamming y un multiplexor.

La técnica puede expandirse a otros tipos de rutas lógicas y elementos secuenciales de muestreo, por ejemplo:

- rutas de fase
- rutas lógicas basadas en un dispositivo de almacenamiento sensible a nivel
- rutas lógicas de reloj desconectado cíclicamente
- rutas lógicas basadas en la caída de señales de una ruta de datos
- entradas y salidas de memorias

El circuito de predicción de fallos puede estar siempre encendido o puede ser activado por una señal de habilitación que represente una OR lógica de las señales de una ruta de datos. Cuando la entrada de habilitación es baja, el circuito de predicción de fallos usa un reloj dedicado para conmutar el circuito para mitigar los efectos de envejecimiento.

Los circuitos integrados pueden implementar un gran número de circuitos lógicos síncronos y sensibles a la temporización. Cuando el retardo del circuito aumenta debido a la degradación física, se produce entonces una infracción de la temporización, y la infracción puede afectar la funcionalidad del circuito. La degradación física puede ser causada por efectos de envejecimiento, o debido a defectos que se desarrollan durante el uso. El circuito de predicción de fallos rastrea el margen de retardo lógico a lo largo del tiempo, y puede predecir un fallo debido a la degradación del retardo físico.

En los términos generales explicados anteriormente, se puede considerar, por lo tanto, que el circuito de mitigación es al menos un circuito del grupo que consiste en: un circuito de notificación (por ejemplo, configurado para producir la notificación 206 o 213); un circuito de medición (o estimación) del retardo de temporización (por ejemplo, para proporcionar una salida de retardo de temporización); un circuito de transmisión de datos; un circuito de compensación de antienvejecimiento del CI (por ejemplo, como se explicó con referencia a la Figura 5 anteriormente); y un circuito de análisis de fallos.

Si el circuito de mitigación es un circuito de transmisión de datos, puede conectarse electrónicamente a un servidor computarizado. El servidor computarizado está configurado de forma ventajosa para recibir múltiples ejemplos de la señal de datos de comparación (por ejemplo, con respecto a diferentes tiempos y/o diferentes fuentes de datos). El servidor computarizado puede realizar de este modo un análisis de predicción de fallos de las señales de datos de comparación. Opcionalmente, puede enviar una notificación a un módulo de mitigación (tal como un circuito de compensación de antienvejecimiento del CI) cuando el análisis de predicción de fallos predice el fallo del CI dentro de un tiempo predefinido. Al menos algunas de las señales de datos de comparación pueden generarse en múltiples valores del tiempo de retardo variable y/o al menos algunas de las señales de datos de comparación pueden generarse a partir de múltiples ejemplos de al menos un valor de múltiples valores del tiempo de retardo variable. Opcionalmente, el análisis de predicción de fallos comprende al menos uno de un análisis de aprendizaje automático, un análisis de tendencias, un análisis de seguimiento de múltiples objetos y un análisis multivariante. De forma ventajosa, el análisis de predicción de fallos comprende recibir señales de datos de comparación y/o resultados de análisis de predicción de fallos de múltiples CI diferentes.

El circuito de predicción de fallos monitoriza continuamente, buscando el efecto favorable, una gran cantidad de circuitos lógicos, tales como señales de una ruta de datos en la salida de una unidad funcional de un CI, usando un área de CI pequeña y energía.

En algunas realizaciones, puede usarse un algoritmo informático para determinar la población de los circuitos de predicción de fallos dentro de una unidad por una cobertura predefinida. Puede usar datos de diseño tales como circuitos de memoria y circuitos de flip-flop dentro de la unidad. El algoritmo informático también puede usarse para ubicar automáticamente los circuitos FPC o MFPC por las señales de desconectado cíclico del reloj de la unidad y para establecer automáticamente el tamaño de la señal de entrada por FPC o MFPC para un rendimiento óptimo (cobertura máxima de la instancia con un número mínimo de circuitos FPC o MFPC).

En algunas realizaciones, pueden calibrarse los retardos dentro del circuito de predicción de fallos. Esto puede hacerse para tener una ruta de correlación muy rápida a los datos de diseño y proporcionar resultados precisos del margen en tiempo cero (durante la prueba). Una metodología de calibración puede utilizar funciones con estimador Pre-Si basadas en matrices de sensores (agentes) en Post-Si para traducir el margen medido del circuito FPC o MFPC en Pre-Si para el margen del peor caso de los márgenes de los puntos finales (FF) monitorizados.

En términos generales, se puede considerar que esto incluye medir o estimar un retardo de temporización para el CI (particularmente en la operación inicial o de tiempo cero), basándose en la señal de datos de comparación proporcionada al circuito de mitigación. El retardo de temporización puede basarse en una pluralidad de salidas de comparación (que pueden estar en una única señal de datos de comparación o una pluralidad de señales de datos de comparación), determinadas por ejemplo repitiendo las etapas de combinar, retardar y comparar cada uno de una pluralidad de tiempos de retardo.

En algunas realizaciones, el retardo a través de X1..Xn + XorIA + Xor2A se equilibra respecto a un retardo aplicado al reloj usado para el flip-flop de salida (D3) para hacer que el desplazamiento de calibración sea mínimo.

En algunas realizaciones, los datos del margen de temporización de un circuito lógico a gran escala dentro de una unidad o una matriz extraída en el tiempo cero, tal como circuitos lógicos digitales y/o similares, pueden rastrearse y compararse a lo largo del tiempo. El seguimiento puede detectar y/o predecir un fallo de temporización debido al cambio en el retardo y/o la degradación de envejecimiento del CI. Con referencia ahora a la Figura 11, se muestra un diagrama del mapa del margen de una unidad. Este es un ejemplo de un mapa del margen de una unidad que representa la huella del margen de una unidad al inicio de la vida (el margen está representado por un retardo del buffer equivalente). La firma se puede usar para la detección/selección de valores atípicos del chip. En otras palabras, un CI específico recibe una identidad única y la firma se compara con otros CI, lo que permite detectar anomalías en una fabricación a gran escala. El mapa del margen puede rastrearse a lo largo del tiempo para medir la firma de margen en diferentes tiempos para analizar y detectar el gradiente de tiempo de la degradación o envejecimiento del CI. Diferentes funciones de gradiente pueden estar relacionadas con diferentes tipos de defectos y modos de degradación.

En algunas realizaciones, los datos del margen de una matriz pueden recopilarse y usarse para procesos de clasificación de matrices y de detección de anomalías. Esto se hace recopilando los datos del margen de una unidad dentro de una matriz y usando algoritmos ML para construir una función de estimador basada en una matriz de sensores. Se describen más detalles en la solicitud de patente provisional US62/675.986 titulada "INTEGRATED CIRCUIT PROFILING AND ANOMALY DETECTION", presentada el 16 de abril de 2018, cuyo contenido se publicó de forma efectiva en el marco de la publicación de la solicitud de patente US2021/0173007 el 10 de junio de 2021.

En algunas realizaciones, los datos de margen pueden analizarse por una aplicación de ejecución específica para generar un binomio de frecuencia/energía basada en la aplicación.

A continuación, se muestran ganancias matemáticas que pueden depender de la suposición de que todas las rutas son independientes. Para simplificar, la prueba se realiza usando el circuito descrito en la Figura 3. La prueba es también válida para el circuito descrito en la Figura 3A bajo la suposición de que XOR2a es simétrico. Esta suposición puede relajarse en casos de al menos algunas rutas dependientes cuando sea necesario, con las correcciones apropiadas. En cualquier tiempo, indicado *t*, se designa el margen de ruta $x_i^t$ (ruta i en el tiempo t) $m_i^t$. A continuación, el ciclo de reloj se designa T.

Teorema 1: En el tiempo t

A. Para $D2 < \min_{1 \le i \le k} m_i^t = m^t{}_{mín}$', la salida de XOR2 es constantemente 0'

B. Para $D2 > m^t{}_{mín}$', la salida de XOR2 puede ser 1' con alguna probabilidad P.

**Teorema 2:** Para el segundo caso del teorema 1 ($D2 > m^t{}_{mín}$), la probabilidad P es mayor que $\max_{j \in K^*} 2q_j(1-q_j)$, donde $K^* = \{j > 0 | D2 > m_j^t\}$.

**Conclusión:** Dado que por alguna degradación $m^{t1}{}_{mín} > m^{t2}{}_{mín}$', donde $t_2 > t_1$. Entonces, para *D*2 de manera que $m^{t1}{}_{mín} > D2 > m^{t2}{}_{mín}$', la salida de XOR2 es 0' en el tiempo $t_1$ y 1' con alguna probabilidad en $t_2$.

Demostración del Teorema 1

Caso A: Como ninguna de las entradas de XOR1 cambia en la ventana de tiempo $(T - m^t_{min}, T]$ se deduce que FF1 y FF2 contienen el mismo valor, por lo que la salida de XOR2 es 0'.

Caso B: Se representa XOR1 en 3 XOR: XORa, XORb y XORc. Sus entradas son las siguientes:

- XORa: una constante 0', más todas las rutas i para las cuales $m_i^t < D2$.
- XORb: una constante 0', más todas las rutas i para las cuales $m_i^t < D2$.
- XORc: las salidas de XORa y XORb.

Luego, en la ventana de tiempo [$T$ - $D_2$, $T$],

- La salida de XORa puede cambiarse con alguna probabilidad, ya que las entradas pueden cambiarse durante ese tiempo.
- La salida de XORb es constante.

Por lo tanto, la salida de XORc (que es en realidad la salida de XOR1) puede cambiarse en la ventana de tiempo ($T$ - $D2$, $T$] con alguna probabilidad y, por lo tanto, la salida de XOR2 puede ser 1'.

Demostración del Teorema 2

Se usa la misma representación de XOR1 que en la comprobación del Teorema 1. Entonces, la probabilidad P en la que la salida de XOR2 es 1' es la probabilidad en la que la salida de XORa se cambia en dos ciclos secuenciales. Esa probabilidad es $2q_{out}(1 - q_{out})$ donde $q_{out}$ es la probabilidad de que la salida de XORa sea 0'.

Ahora, se representa XORa en 2 XOR: XORa1 y XORa2. Sus entradas son las siguientes:

- XOa1: La señal x para la cual $q_x(1 - q_x)$ es la máxima entre todas las entradas de XORa y la salida de XORa2. Obsérvese que la salida de XORa1 es en realidad la salida de XORa.
- XORa2: todas las entradas de XORa excepto la señal x (para la que $q_x(1 - q_x)$ es la máxima).

A continuación, por el Lema 1, se deduce que $q_{a1}(1 - q_{a1})$, (donde $q_{a1}$ es la probabilidad de que la salida de XORa1 sea 0') es mayor que $q_x(1 - q_x)$.

Por lo tanto, como la salida de XORa1 es realmente la salida de XORa, se obtiene el Teorema 2.

**Lema 1:** Sean $a$ y $b$ las señales para las cuales las probabilidades de 0' son $q_a$ y $q_b$ respectivamente. Luego, $q_c(1 - q_c) \geq \max q_a(1 - q_a), q_b(1 - q_b)$, donde $q_c$ representa la probabilidad de que la salida de $XOR(a, b)$ sea 0'.

Demostración del Lema 1

Se supone sin ánimo de generalizar que $q_a(1 - q_a) = \max q_a(1 - q_a), q_b(1 - q_b)$. Entonces, mediante álgebra simple, se deduce que $q_a(1 - q_a) = \frac{1}{4}(1 - \Delta_a^2)$, donde $\Delta_a = 1 - 2q_a$.

Además, por la definición de XOR se deduce que: $q_c = q_a q_b + (1 - q_a)(1 - q_b)$. Por lo tanto, por el álgebra anterior se deduce que $q_c(1 - q_c) = \frac{1}{4}(1 - \Delta_c^2)$, donde $\Delta_c = 1 - 2q_c$.

Además, por la definición de $q_c$, puede mostrarse que $\Delta_c = 1 - 2(2q_a q_b - q_a - q_b + 1) = -1 - 4q_a q_b + 2q_a + 2q_b = 1 + 2q_b)$. Por lo tanto, dado que $|-1 + 2q_b| < 1$, se deduce que $\Delta_c^2 \leq \Delta_a^2$. Por tanto, se obtiene el Lema 1.

En cualquier intervalo de tiempo, el MFPC basado en MUX puede considerarse un caso especial del MFPC basado en XOR. Por lo tanto, la siguiente demostración matemática de la versión basada en XOR se mantiene para la versión basada en MUX.

Resultados experimentales

A continuación se presentan los resultados de los experimentos de simulación.

Ahora se hace referencia a la Figura 6, que muestra un diagrama de temporización de un retardo de señal para la predicción de fallo del CI. La definición de señal puede ser *Di~ U(Xi, Xi+di)*, y *P{V(Si) = 1, tj}= P{V(Si) = 0, tj}= 1/2*. La Figura 6 muestra una descripción de simulación basada en eventos, con la siguiente configuración de simulación:

- XOR1 estaba monitorizando 256 rutas de entrada
- La longitud de los datos de cada ruta fue de $10^4$ ciclos de reloj
- El tiempo de ciclo de reloj se definió como 100 unidades de tiempo
- Se generó una señal Si para cada ruta [*i*] (descripción detallada en la siguiente página)
- Cada ruta [*i*], se definió por dos constantes [*Xi*] y [*di*] que determinan el retardo por cada ciclo de reloj
- Se extrajo [*Xi*] para cada ruta mediante una distribución uniforme entre 25 - 50 unidades de tiempo
- Se extrajo *[di]* para cada ruta mediante una distribución uniforme entre 0 - 25 unidades de tiempo
- Para la señal i, el tiempo de conmutación en cada ciclo se extrajo uniformemente en el intervalo de *(Xi, Xi+di)*
- El margen de señal i, es entonces [100 - *Xi* - *di*]

El experimento se llevó a cabo para cada valor de D2, donde D2 se definió en unidades de tiempo, y el valor de retardo D2 se recorrió en valores a una resolución necesaria para resolver los márgenes de retardo de temporización separados en la firma, tales como resoluciones de fracciones de los tiempos de período de reloj. Para cada valor D2, se pueden contar las transiciones de salida XOR2, y el número de recuentos se representa frente al umbral del margen de valor de temporización. El umbral del margen del eje X puede ser 100-D2, y el eje Y puede ser el número de [1] en la salida de XOR2 observada para un cierto valor de D2:

$$\mathrm{XOR2} = 1 \text{ iff } \mathrm{XOR1(t = 100)} \neq \mathrm{XOR1(t=D2)}.$$

A continuación se hace referencia a la Figura 7, que muestra un gráfico de errores frente al tiempo del ciclo para un primer experimento. La línea continua representa la salida de MFPC en el tiempo cero (sin degradación), y la línea discontinua representa la salida de MFPC después de la degradación. El margen mínimo fue igual a 25 unidades de tiempo, tal como [100-75] y MaxD2 en el fallo fue de 75 unidades de tiempo. En el escenario de degradación, el margen de una ruta se redujo en 15 unidades de tiempo (el margen se distribuye uniformemente, y el valor máximo se movió en 15 unidades de tiempo), el MFPC detecta el cambio en el margen. Aquí, el margen mínimo fue igual a 10 unidades de tiempo, tal como [100-75-15] y MaxD2 en el fallo fue de 90 unidades de tiempo. El gráfico muestra que los recuentos en la salida de XOR2 se reducen gradualmente a cero. Para cada D2 en el intervalo de [75-90]:

$$\mathrm{P(XOR2=1)=P(cambio,retardo>D2)=0{,}5*(90-(100-D2))/(di+15)}.$$

A continuación se hace referencia a la Figura 8, que muestra un gráfico de errores frente al tiempo del ciclo para un segundo experimento. La línea continua representa la salida de MFPC en el tiempo cero (sin degradación), y la línea discontinua representa la salida de MFPC después de la degradación. El margen mínimo de todas las rutas con [*Xi+di* > 70] (margen<30) aumentó en 15 unidades de tiempo, y esto se realizó para 5 rutas de señal. El margen mínimo fue igual a 25 unidades de tiempo, tal como [100-75] y MaxD2 en el fallo fue de 75 unidades de tiempo. El MFPC detecta el cambio en el margen, donde el margen mínimo fue igual a 10 unidades de tiempo, tal como [100-75-15] y MaxD2 en el fallo fue de 90 unidades de tiempo. Los recuentos en la salida de XOR2 se reducen gradualmente a cero. La probabilidad de fallo se incrementó con el número de rutas.

A continuación se hace referencia a la Figura 9 (diagrama superior), que muestra un diagrama de temporización de dos retardos de señal para la predicción de fallos del CI. Las múltiples señales se conmutan simultáneamente, con igual retardo y valor lógico en cada ciclo. Las señales duplicadas se implementan con el margen más pequeño. Se muestra el valor máximo de [*Xi+di*], donde el retardo de las rutas duplicadas aumentó en 15 unidades de tiempo. Ambas rutas implementan la misma degradación.

A continuación se hace referencia a la Figura 10, que muestra un gráfico de errores frente al tiempo del ciclo para un tercer experimento. La línea continua representa que no hay degradación, la línea discontinua (similar a la línea continua) representa un primer escenario de degradación (Figura 9 línea superior), y la línea discontinua punteada representa un segundo escenario de degradación en el que el retardo de una de las rutas duplicadas aumentó en una cantidad adicional de 5 unidades de tiempo (Figura 9 línea inferior). Obsérvese que los retardos de la señal de réplica son menores en 5 unidades de tiempo con respecto a la señal de base. Las dos rutas son lógicamente idénticas, pero

implementan degradaciones de temporización diferentes. El margen mínimo fue igual a 25 unidades de tiempo, tal como [100-75]. En un primer escenario de degradación (línea discontinua), el sistema puede no detectar el cambio en el margen. MaxD2 en el fallo es igual a 75 unidades de tiempo para ambos escenarios. En un segundo escenario de degradación (línea discontinua punteada), el sistema detecta el cambio en el margen. MaxD2 en el fallo fue de 95 unidades de tiempo.

A lo largo de esta solicitud, varias realizaciones de esta invención pueden presentarse en un formato de intervalo. Debe entenderse que la descripción en formato de intervalo es simplemente por conveniencia y brevedad y no debe interpretarse como una limitación inflexible del alcance de la invención. Por consiguiente, debe considerarse que la descripción de un intervalo describe específicamente todos los posibles subintervalos, así como valores numéricos individuales dentro de ese intervalo. Por ejemplo, se debe considerar que la descripción de un intervalo tal como de 1 a 6 describe específicamente subintervalos tales como de 1 a 3, de 1 a 4, de 1 a 5, de 2 a 4, de 2 a 6, de 3 a 6, etc., así como números individuales dentro de ese intervalo, por ejemplo, 1, 2, 3, 4, 5 y 6. Esto se aplica independientemente de la amplitud del intervalo.

Siempre que se indique un intervalo numérico en la presente memoria, se pretende incluir cualquier número citado (fraccionario o integral) dentro del intervalo indicado. Las frases "variando/varía entre" un primer número indicado y un segundo número indicado y "que varía/varía de" un primer número indicado "a" un segundo número indicado se usan indistintamente en la presente memoria y pretenden incluir el primer y segundo números indicados y todos los números fraccionales e integrales entre ellos.

En la descripción y las reivindicaciones de la solicitud, cada una de las palabras "comprende" "incluye" y "tiene" y formas de las mismas, no están necesariamente limitadas a elementos en una lista con la que pueden asociarse las palabras. Además, en caso de incoherencias entre esta solicitud y cualquier documento al que se haga referencia en esta solicitud, se entenderá que prevalece la presente solicitud.

Para aclarar las referencias en esta descripción, se observa que el uso de sustantivos como nombres comunes, nombres propios, denominaciones, y/o similares no pretenden implicar que las realizaciones de la invención se limitan a una sola realización, y muchas configuraciones de los componentes descritos pueden usarse para describir algunas realizaciones de la invención, mientras que otras configuraciones pueden derivarse de estas realizaciones en diferentes configuraciones.

Para mayor claridad, no se muestran ni describen todas las características rutinarias de las implementaciones descritas en la presente memoria. Por supuesto, debe apreciarse que en el desarrollo de cualquier implementación real de este tipo, se deben realizar numerosas decisiones específicas de implementación para lograr los objetivos específicos del desarrollador, tal como el cumplimiento de las restricciones relacionadas con la aplicación y el negocio, y que estos objetivos específicos variarán de una implementación a otra y de un desarrollador a otro. Además, se apreciará que dicho esfuerzo de desarrollo podría ser complejo y llevar mucho tiempo, pero sería una tarea rutinaria de ingeniería para los expertos en la técnica que tengan conocimiento de esta descripción.

Basándose en las enseñanzas de esta descripción, se espera que un experto en la técnica sea capaz de poner en práctica fácilmente la presente invención. Se considera que las descripciones de las diversas realizaciones proporcionadas en la presente memoria proporcionan una información amplia y detalles de la presente invención para permitir a un experto en la técnica ponerla en práctica. Además, las diversas características y realizaciones de la invención descritas anteriormente están contempladas específicamente para usarlas solas, así como en diversas combinaciones.

Se pueden usar herramientas de diseño y diseño de circuitos convencionales y/o contemporáneos para implementar la invención. Las realizaciones específicas descritas en la presente memoria, y en particular los diversos espesores y composiciones de diversas capas, son ilustrativas de realizaciones ilustrativas y estas opciones de implementación específicas no deben considerarse limitantes de la invención. Por consiguiente, se pueden proporcionar varios ejemplos para los componentes descritos en la presente memoria como un solo ejemplo.

Si bien generalmente se supone la presencia de circuitos y estructuras físicas, es bien sabido que en el diseño y la fabricación de semiconductores modernos, se pueden incorporar estructuras físicas y circuitos en una forma descriptiva legible por ordenador adecuada para su uso en etapas de diseño, prueba o fabricación posteriores, así como en circuitos integrados semiconductores fabricados resultantes. Por consiguiente, también se describen codificaciones legibles por ordenador y representaciones de las mismas, ya sean incorporadas en medios o combinadas con instalaciones de lectura adecuadas para permitir la fabricación, prueba o refinamiento de diseño de los circuitos y/o las estructuras correspondientes. Las estructuras y funcionalidad que se presentan como componentes discretos en las configuraciones ilustrativas pueden implementarse como una estructura o componente combinados. Se contempla que la invención incluya circuitos, sistemas de circuitos, métodos relacionados y codificaciones de medios legibles por ordenador de dichos circuitos, sistemas y métodos, todos como se describe en la presente memoria, y como se define en las reivindicaciones adjuntas. Como se utiliza en la presente memoria, un medio legible por ordenador incluye al menos un disco, una cinta u otro semiconductor magnético, óptico (por ejemplo, tarjetas de memoria flash, ROM) o medio electrónico y una red de cable o inalámbrica u otro medio de comunicación.

La descripción detallada anterior ha descrito solo algunas de las muchas implementaciones posibles de la presente invención. Por esta razón, esta descripción detallada está prevista a modo de ilustración, y no como limitaciones. Las variaciones y modificaciones de las realizaciones descritas en la presente memoria pueden realizarse basándose en la descripción establecida en la presente memoria. El alcance de la invención está definido por las reivindicaciones adjuntas.

Las realizaciones de la presente invención pueden usarse para fabricar, producir y/o ensamblar circuitos integrados y/o productos basados en circuitos integrados.

Los aspectos de la presente invención se describen en la presente memoria con referencia a ilustraciones de diagramas de flujo y/o diagramas de bloques de métodos, aparatos (sistemas) y productos de programas informáticos según realizaciones de la invención. Se entenderá que cada bloque de las ilustraciones del diagrama de flujo y/o los diagramas de bloques, y las combinaciones de bloques en las ilustraciones del diagrama de flujo y/o los diagramas de bloques, pueden implementarse mediante instrucciones de programa legibles por ordenador.

El diagrama de flujo y los diagramas de bloques en las figuras ilustran la arquitectura, la funcionalidad y el funcionamiento de posibles implementaciones de sistemas, métodos y productos de programas informáticos según diversas realizaciones de la presente invención. A este respecto, cada bloque en el diagrama de flujo o diagramas de bloques puede representar un módulo, segmento o porción de instrucciones, que comprenda una o más instrucciones ejecutables para implementar las funciones lógicas especificadas. En algunas implementaciones alternativas, las funciones indicadas en el bloque pueden ocurrir fuera del orden indicado en las figuras. Por ejemplo, dos bloques mostrados en sucesión pueden, de hecho, ejecutarse de manera sustancialmente concurrente, o los bloques a veces pueden ejecutarse en el orden inverso, dependiendo de la funcionalidad involucrada. También se observará que cada bloque de los diagramas de bloques y/o la ilustración del diagrama de flujo, y las combinaciones de bloques en los diagramas de bloques y/o la ilustración del diagrama de flujo, pueden implementarse mediante sistemas basados en hardware específico que realicen las funciones o actos especificados o lleven a cabo combinaciones de hardware específico e instrucciones informáticas.

## REIVINDICACIONES

1. Un circuito integrado (CI) semiconductor que comprende:

una ruta de datos que comprende rutas de bits paralelas, terminando cada una de las rutas de bits paralelas con un flip-flop (FF);
un combinador de rutas de señales (XOR1, XOR1a, MUX), que comprende una pluralidad de rutas de entrada (X1_d - Xk_d, X1 - Xn) y una salida (XOR1_OUT, XOR1a$_{out}$, Mux_OUT), basándose la salida en una combinación de señales respectivas recibidas en cada una de las rutas de entrada, en donde cada una de las rutas de entrada está conectada a una entrada de cada uno de los diferentes flip-flops de la ruta de datos, de manera que cada una de las señales recibidas en las rutas de entrada son una señal respectiva recibida por el flip-flop respectivo de la ruta de datos;
un circuito de retardo (D2) que tiene una salida (XOR_1 OUT d2, Mux_OUT_d2) y una entrada que está conectada eléctricamente a la salida del combinador de rutas de señales, estando el circuito de retardo configurado para aplicar, en momentos diferentes, respectivos diferentes retardos a una señal recibida en la entrada del circuito de retardo, para proporcionar, en la salida del circuito de retardo, respectivas señales de retardo diferentes de los diferentes retardos; y
un circuito de comparación (XOR2, XOR2a) dispuesto para proporcionar salidas de comparación basándose cada una en una comparación de la salida del combinador de rutas de señales y una diferente de las señales retardadas, en donde las salidas de comparación se proporcionan, en al menos una señal de datos de comparación, a al menos un circuito de mitigación, en donde el circuito de mitigación es al menos un circuito del grupo que consiste en: un circuito de notificación, un circuito de medición de retardo de temporización, un circuito de transmisión de datos, un circuito de compensación antienvejecimiento del CI y un circuito de análisis de fallos.

2. El CI de la reivindicación 1, en donde el combinador de rutas de señales es al menos uno del grupo que consiste en un combinador lógico XOR (XOR1, XOR1a), un combinador de paridad de Hamming y un multiplexor (MUX).

3. El CI de la reivindicación 1 o la reivindicación 2, que comprende además:

un primer circuito (FF2) de almacenamiento interno, conectado eléctricamente a la salida del combinador de rutas de señales y dispuesto para proporcionar la salida del combinador de rutas de señales almacenadas como una primera entrada al circuito de comparación; y
un segundo circuito (FF1) de almacenamiento interno, conectado eléctricamente a la señal retardada y dispuesto para proporcionar la señal retardada almacenada como una segunda entrada al circuito de comparación.

4. El CI de una cualquiera de las reivindicaciones 1 a 3, en donde el combinador de rutas de señales es un combinador de primera ruta de señales (XOR1a) dispuesto para recibir una pluralidad de señales de una primera fuente de datos y en donde el circuito de comparación es un circuito de primera comparación (XOR2a), comprendiendo el CI además:

un combinador de segunda ruta de señales (XOR1b), que comprende una pluralidad de rutas de entrada y una salida, basándose la salida del combinador de segunda ruta de señales en una combinación de señales respectivas recibidas en cada una de las rutas de entrada, recibiéndose las señales de una segunda fuente de datos;
un multiplexor, configurado para recibir la salida del combinador de primera ruta de señales, la salida del combinador de segunda ruta de señales y una señal de selección (in/out sel) y para emitir de forma selectiva la salida del combinador de primera ruta de señales o la salida del combinador de segunda ruta de señales basándose en la señal de selección, proporcionándose la salida del multiplexor como la entrada al circuito de retardo (D2);
un circuito de segunda comparación (XOR2b) dispuesto para proporcionar una salida de la segunda comparación basándose en una comparación de la salida del combinador de segunda ruta de señales y la señal retardada; y
una puerta OR dispuesta para recibir como entradas la salida de la primera comparación y la salida de la segunda comparación y para proporcionar una salida (HT out) como la señal de datos de comparación al, al menos, un circuito de mitigación.

5. El CI de la reivindicación 4, que comprende además:

un circuito de almacenamiento de primera comparación (FF1a), dispuesto para recibir la salida de la primera comparación y controlado por una primera señal de reloj (clk1a);
un circuito de almacenamiento de segunda comparación (FF1b), dispuesto para recibir la salida de la segunda comparación y controlado por una segunda señal de reloj (clk1b); y

en donde el circuito de almacenamiento de primera comparación está dispuesto para proporcionar la salida de la primera comparación como una primera entrada a la puerta OR y el circuito de almacenamiento de segunda comparación está dispuesto para proporcionar la salida de la segunda comparación como una segunda entrada a la puerta OR.

6. El CI de una cualquiera de las reivindicaciones 1 a 3, en donde los diferentes retardos aplicados por el circuito de retardo son múltiplos enteros de incrementos iguales a un período de reloj del CI dividido por un tamaño de vector de la firma, y en donde el tamaño de vector de la firma está entre 1 y 100.000.

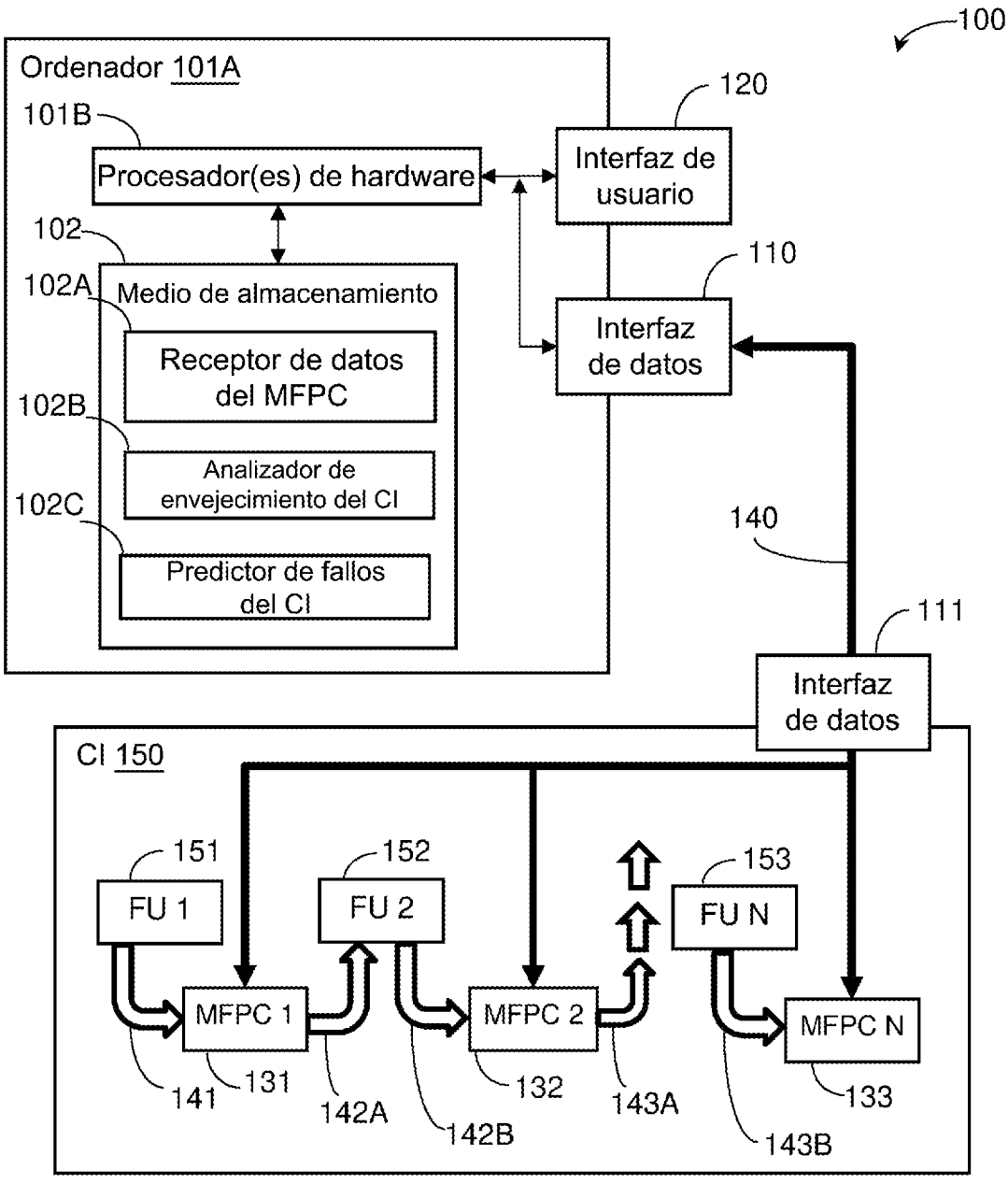
100
Ordenador 101A
101B
Procesador(es) de hardware
102
102A
Medio de almacenamiento
Receptor de datos del MFPC
102B
Analizador de envejecimiento del CI
102C
Predictor de fallos del CI
120
Interfaz de usuario
110
Interfaz de datos
140
111
Interfaz de datos
CI 150
151
FU 1
152
FU 2
153
FU N
MFPC 1
MFPC 2
MFPC N
141
131
142A
142B
132
143A
143B
133

Figura 1

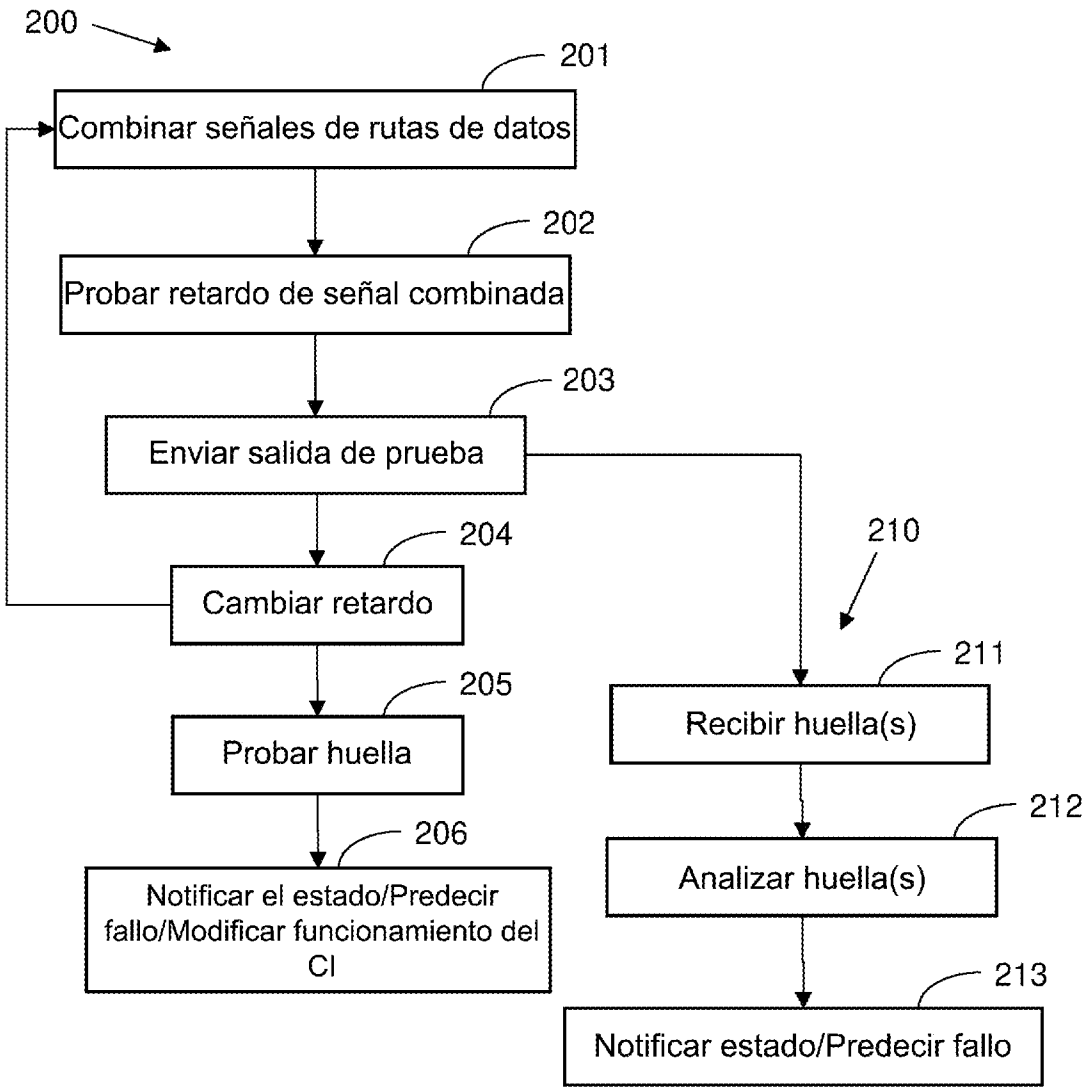
200
201
Combinar señales de rutas de datos
202
Probar retardo de señal combinada
203
Enviar salida de prueba
204
Cambiar retardo
205
Probar huella
206
Notificar el estado/Predecir fallo/Modificar funcionamiento del CI
210
211
Recibir huella(s)
212
Analizar huella(s)
213
Notificar estado/Predecir fallo

Figura 2

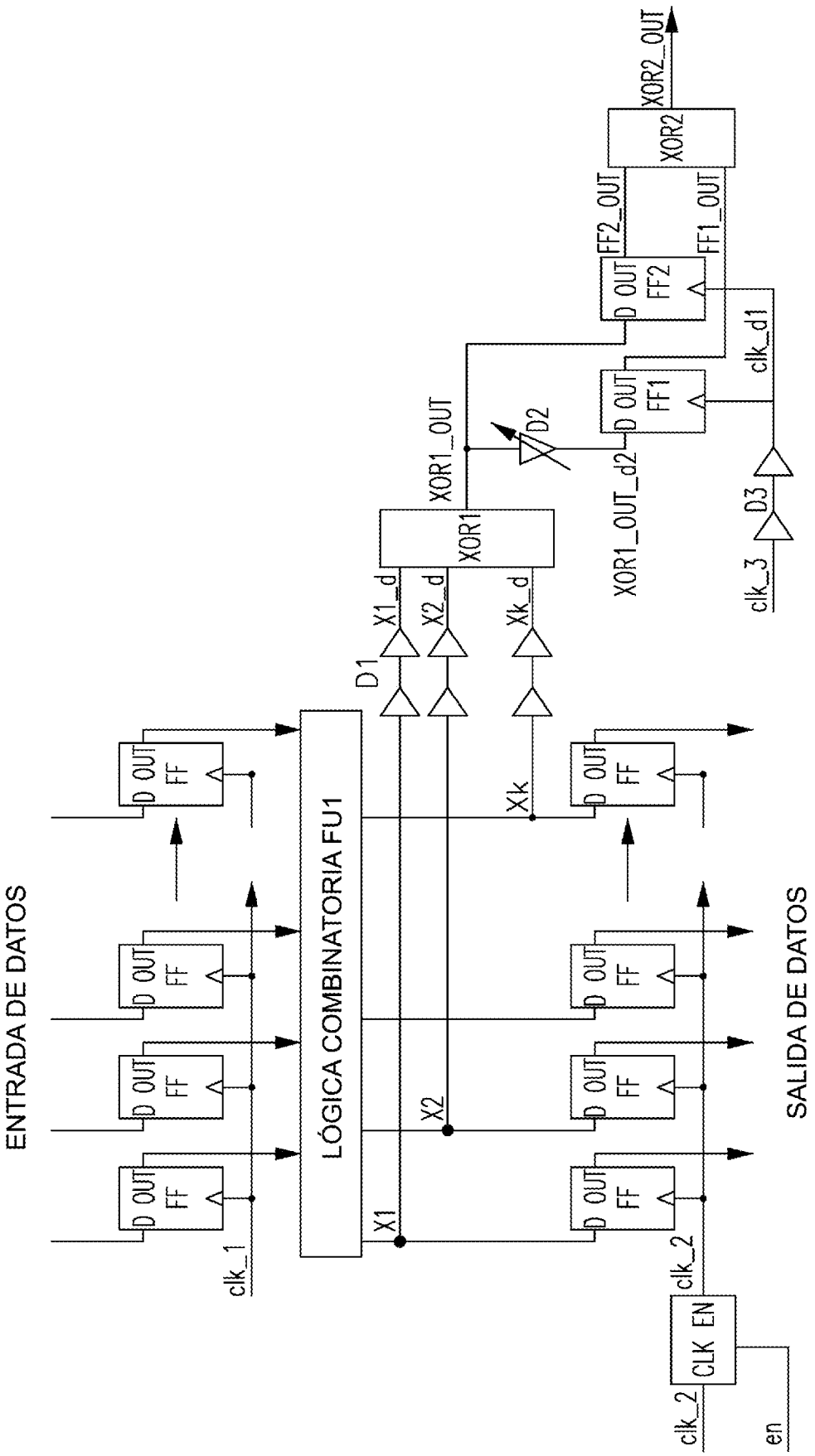
ENTRADA DE DATOS
LÓGICA COMBINATORIA FU1
SALIDA DE DATOS
D OUT FF
clk_1
clk_2
CLK EN
en
X1
X2
Xk
D1
X1_d
X2_d
Xk_d
XOR1
XOR1_OUT
D2
XOR1_OUT_d2
D3
clk_3
clk_d1
FF1
FF2
FF1_OUT
FF2_OUT
XOR2
XOR2_OUT

Figura 3

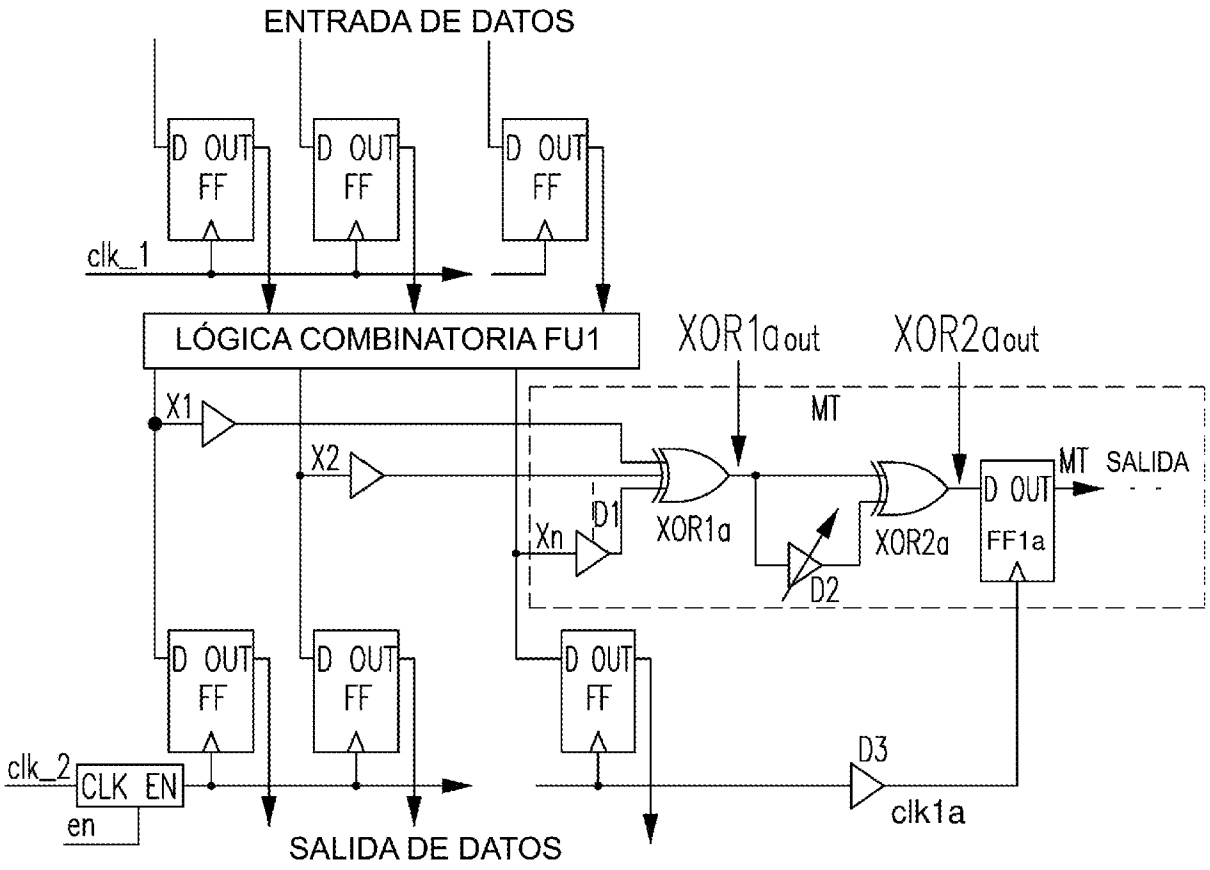


Figura 3A

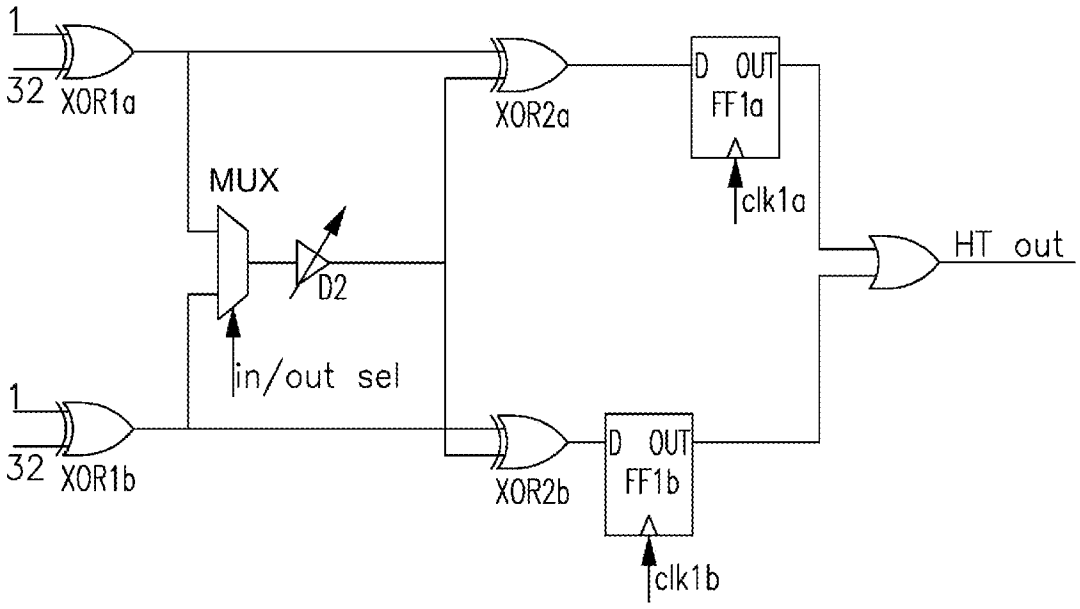


Figura 3B

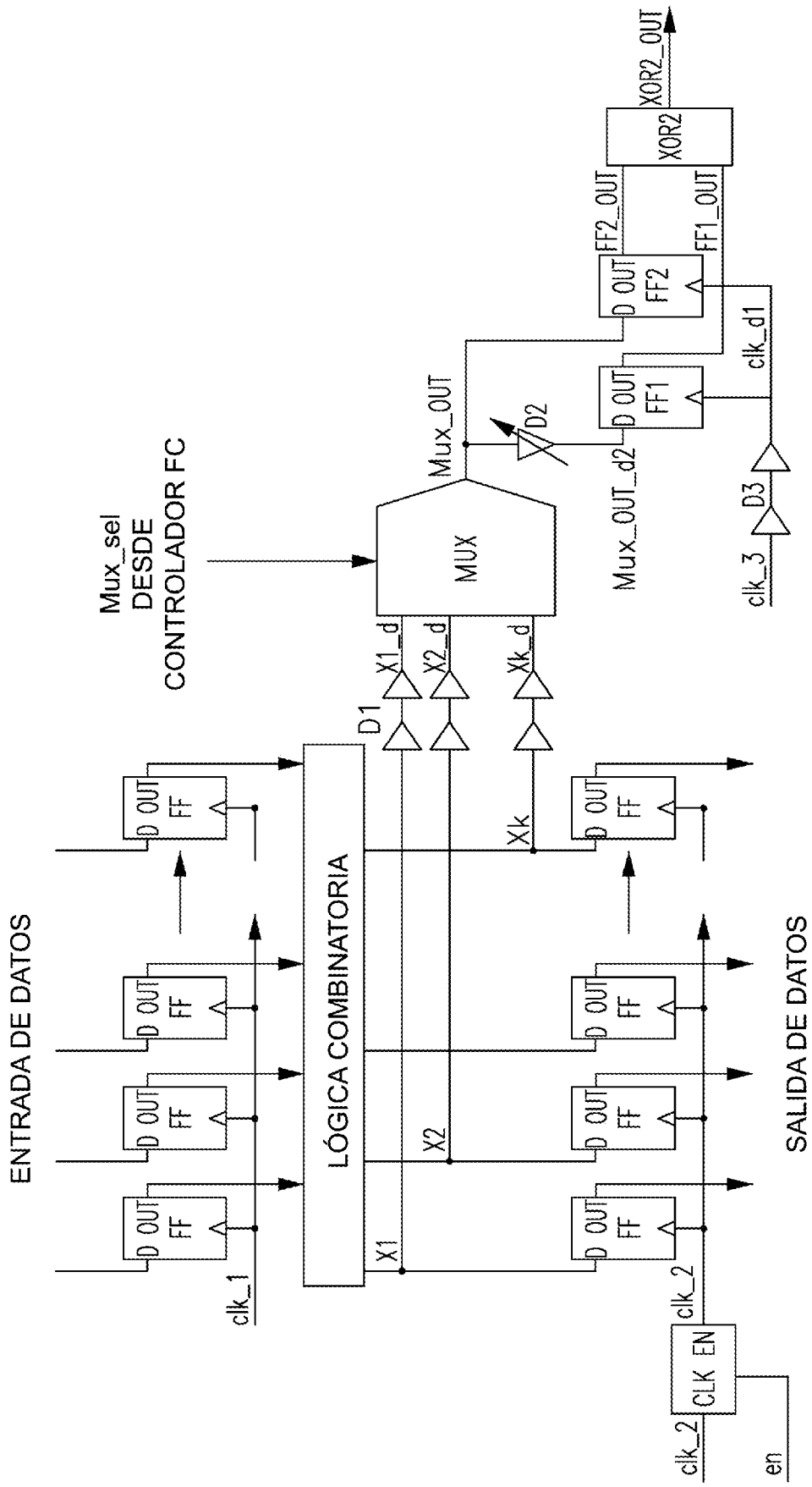
ENTRADA DE DATOS
Mux_sel
DESDE
CONTROLADOR FC
LÓGICA COMBINATORIA
MUX
Mux_OUT
Mux_OUT_d2
D1
D2
D3
X1
X2
Xk
X1_d
X2_d
Xk_d
D OUT FF
FF1
FF2
XOR2
FF1_OUT
FF2_OUT
XOR2_OUT
clk_1
clk_2
clk_3
clk_d1
CLK EN
en
SALIDA DE DATOS

Figura 4

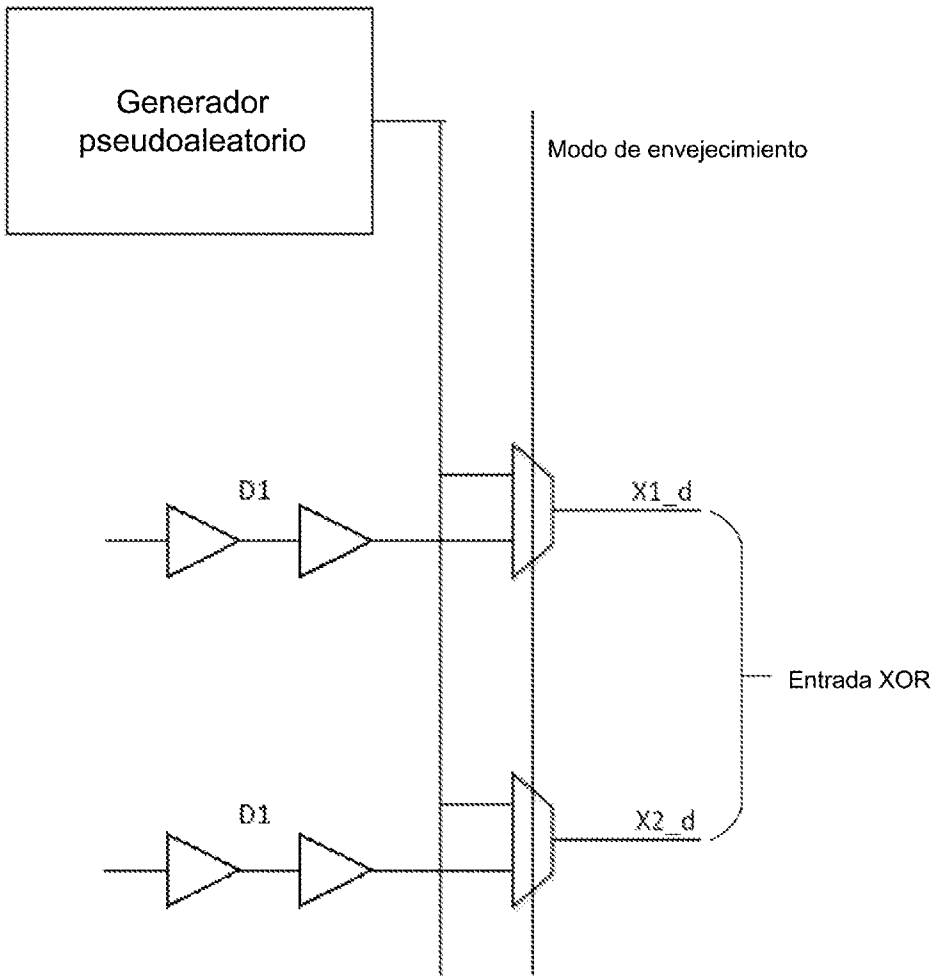


Figura 5

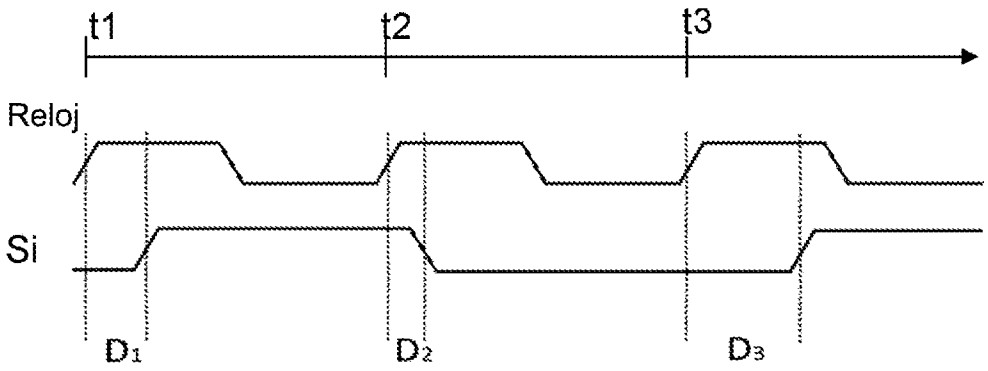


Figura 6

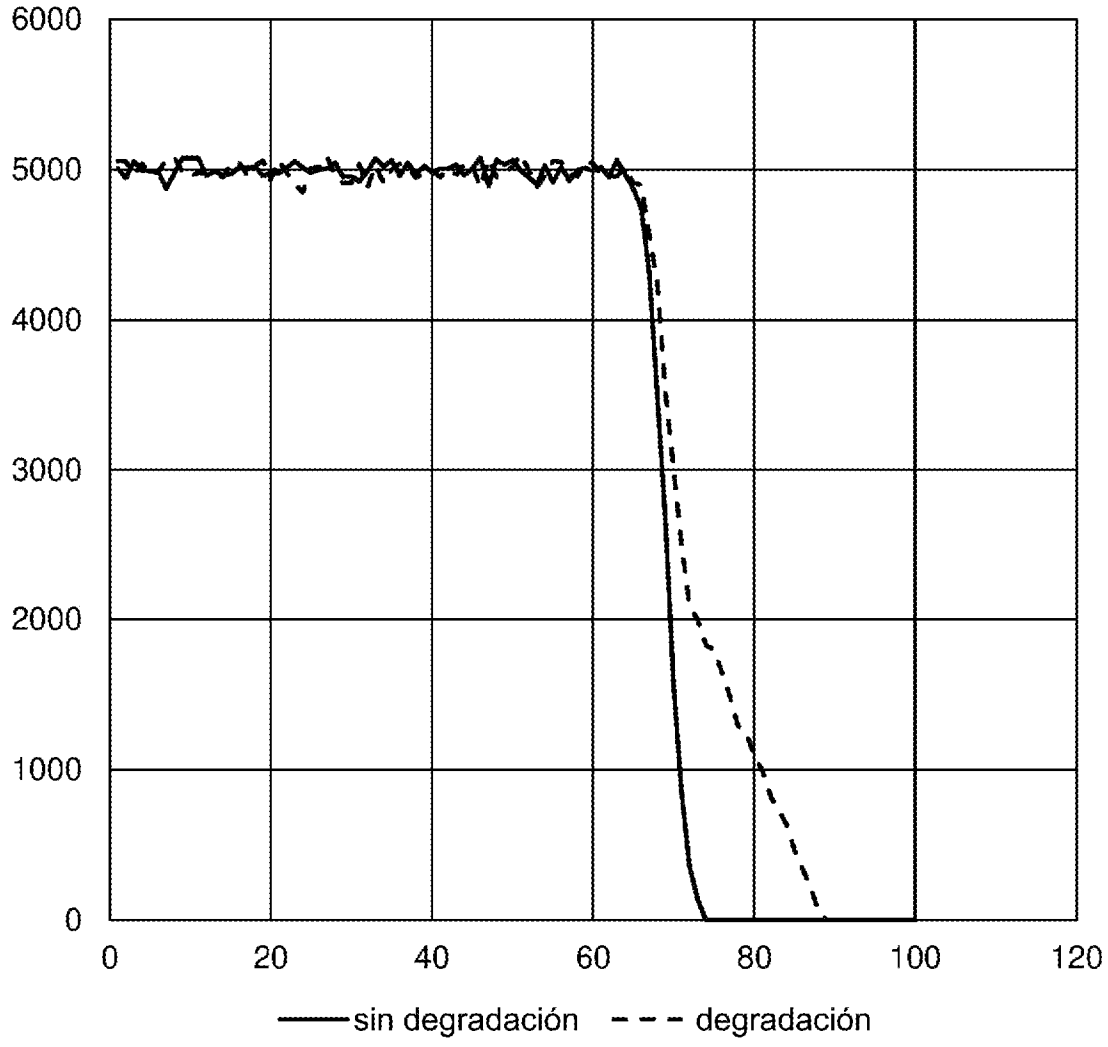
6000
5000
4000
3000
2000
1000
0
0
20
40
60
80
100
120
sin degradación
degradación

Figura 7

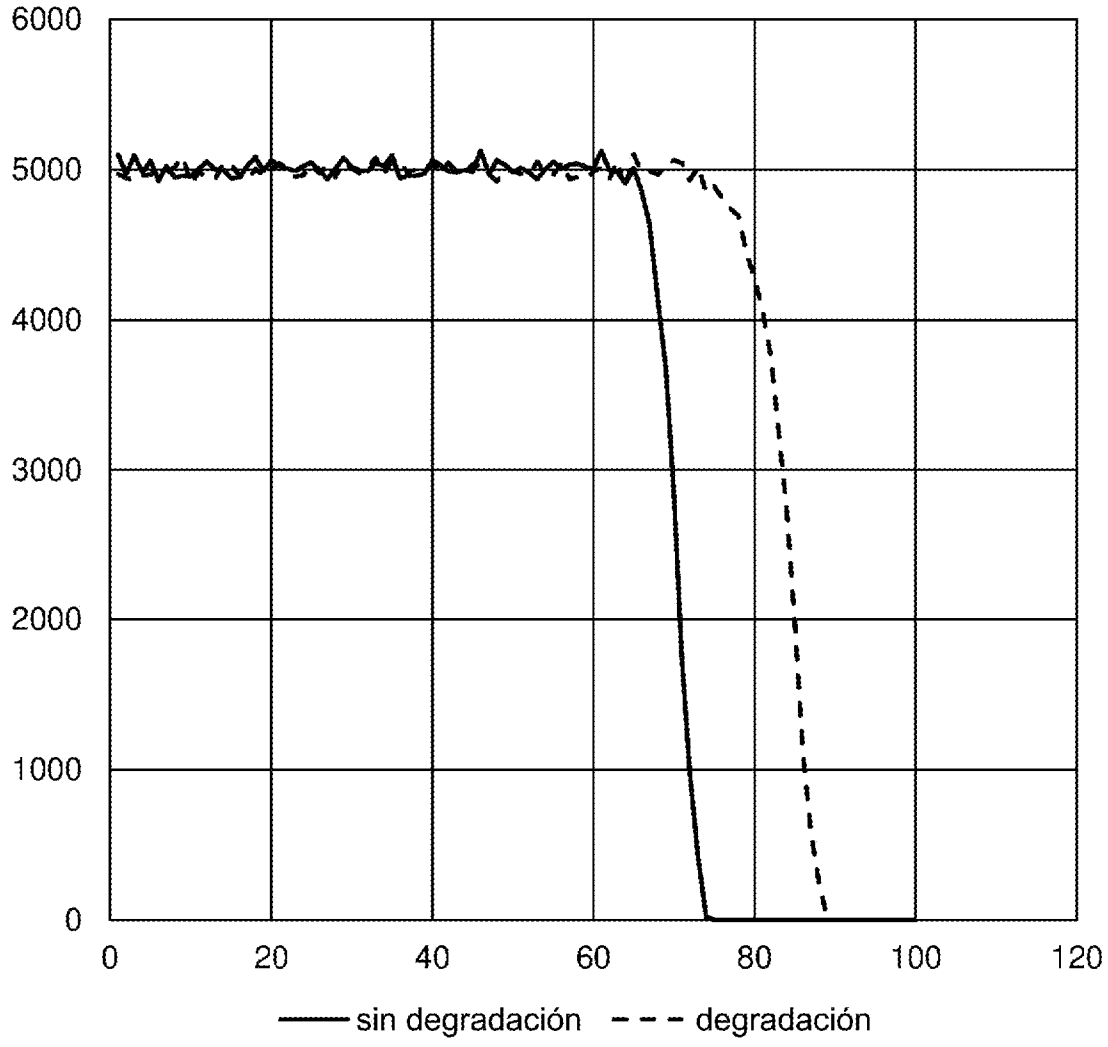
6000
5000
4000
3000
2000
1000
0
0
20
40
60
80
100
120
sin degradación
degradación

Figura 8

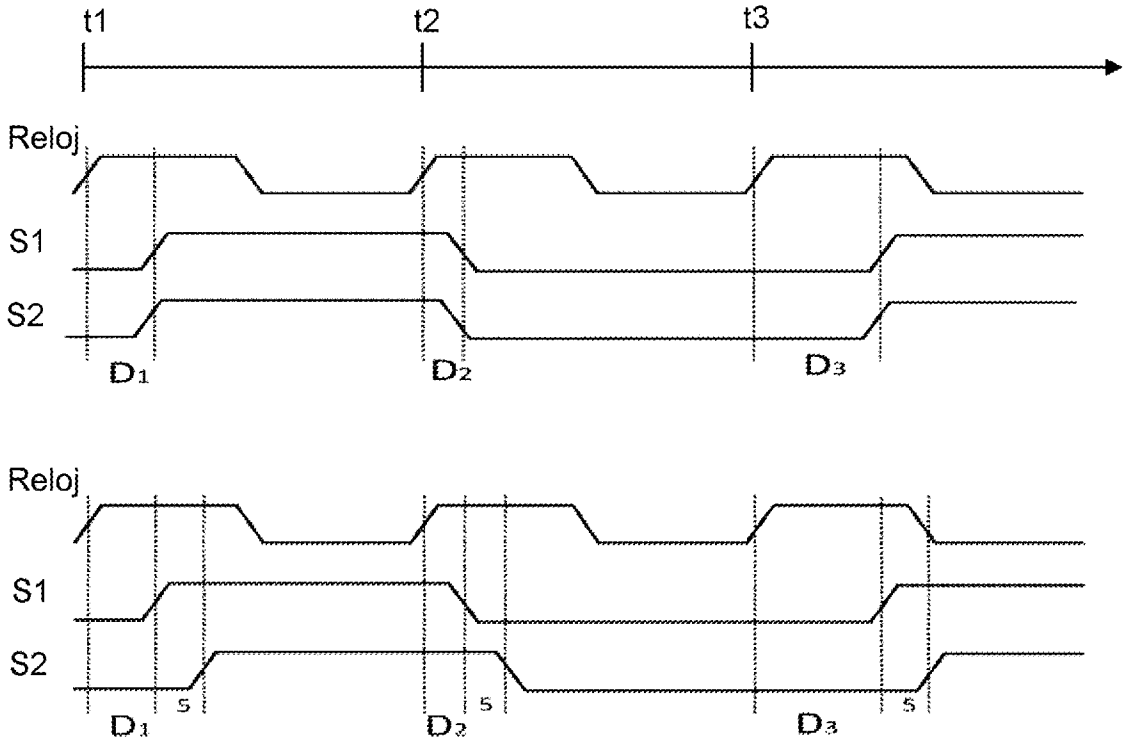


Figura 9

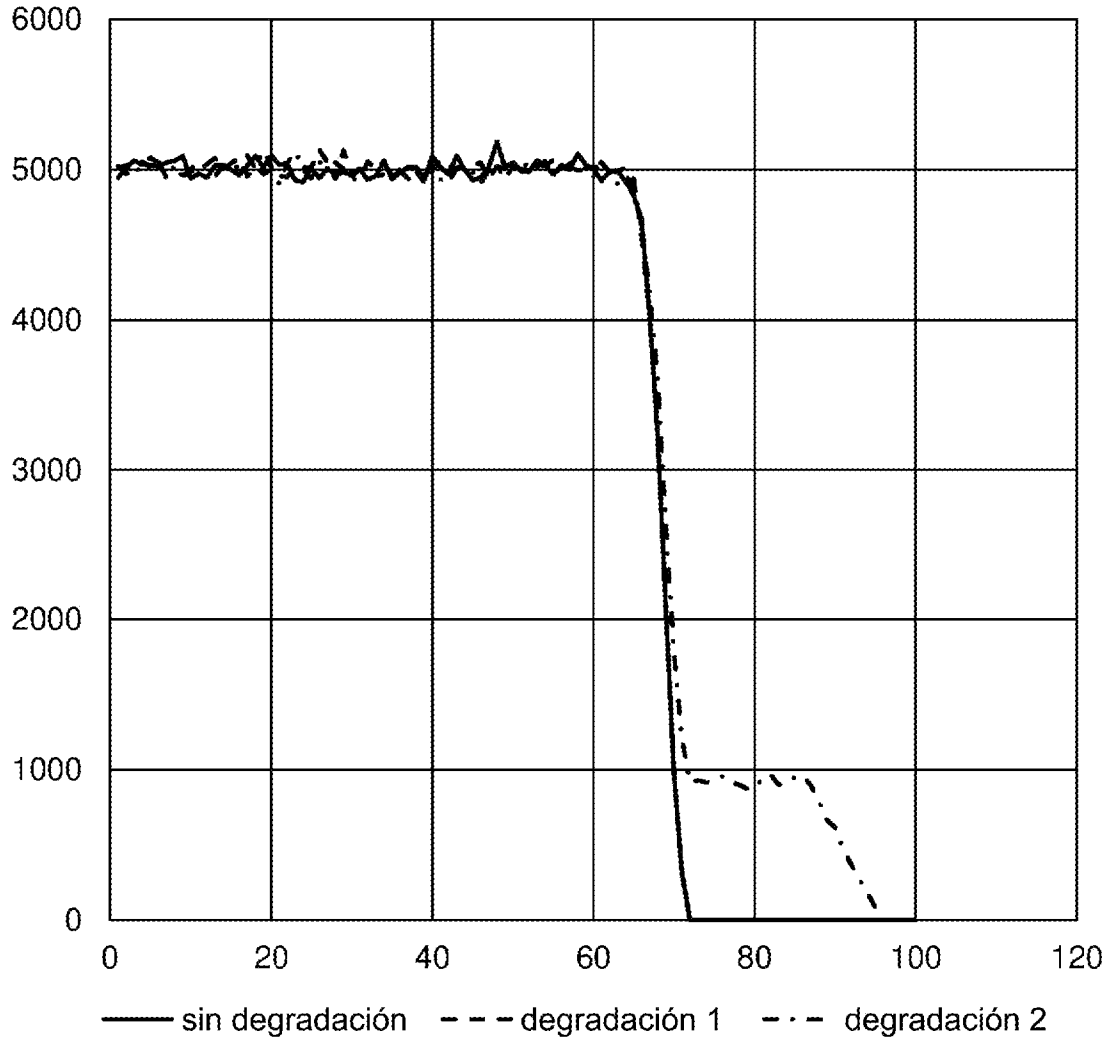
6000
5000
4000
3000
2000
1000
0
0
20
40
60
80
100
120
sin degradación
degradación 1
degradación 2

Figura 10

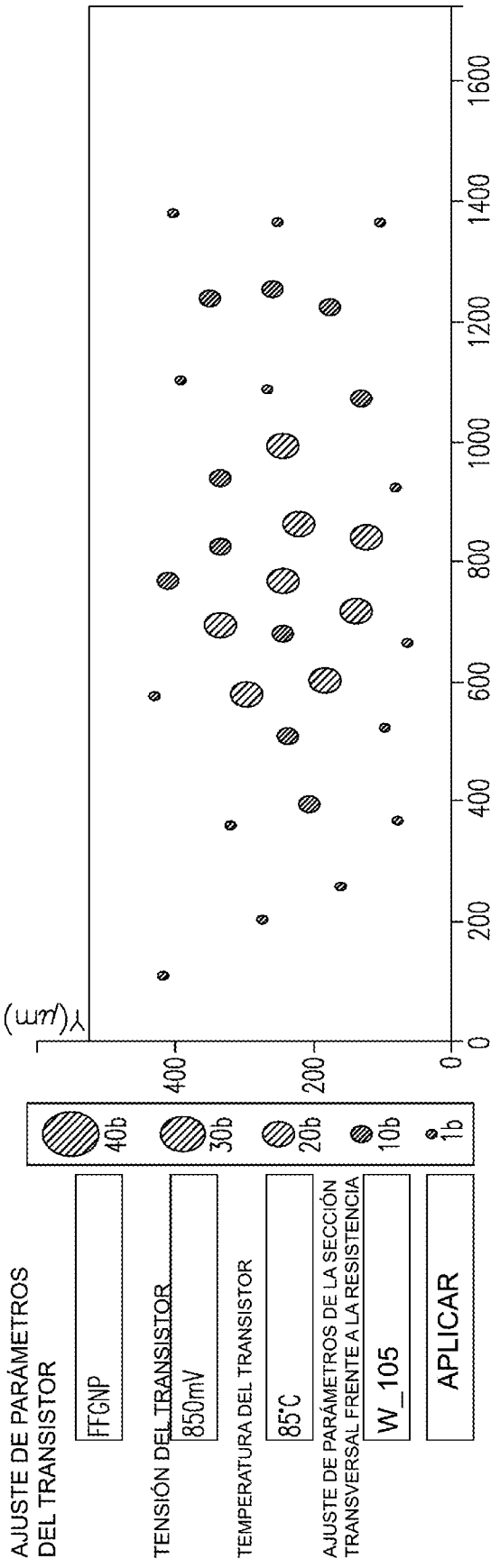
AJUSTE DE PARÁMETROS DEL TRANSISTOR
FFGNP
TENSIÓN DEL TRANSISTOR
850mV
TEMPERATURA DEL TRANSISTOR
85°C
AJUSTE DE PARÁMETROS DE LA SECCIÓN TRANSVERSAL FRENTE A LA RESISTENCIA
W_105
APLICAR
40b
30b
20b
10b
1b
Y(μm)
0
200
400
0
200
400
600
800
1000
1200
1400
1600

Figura 11