(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 768 874**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/57 (2013.01)
G01R 31/3181 (2006.01)
G01R 31/3183 (2006.01)
G01R 31/3193 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.09.2016 E 16188213 (9)**

(97) Fecha y número de publicación de la concesión europea: **27.11.2019 EP 3163491**

(54) Título: **Mecanismo informatizado para evaluación de vulnerabilidad en disposiciones con interceptores**

(30) Prioridad:

02.11.2015 US 201514929423

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.06.2020

(73) Titular/es:

WINBOND ELECTRONICS CORP. (100.0%)
No. 8 Keya 1st Rd., Daya District, Central Taiwan Science Park
Taichung City, Taiwan. , TW

(72) Inventor/es:

TEPER, VALERY

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Mecanismo informatizado para evaluación de vulnerabilidad en disposiciones con interceptores

Antecedentes

La presente divulgación generalmente se refiere a fallos en circuitos integrados, y más específicamente a medidas de detección de fallos en diseños de circuitos integrados.

La prueba de circuitos integrados de vulnerabilidad de seguridad como dispositivos físicos es excesivamente costosa, tanto en el trabajo y consecuencias como el tiempo de comercialización, dado que la reparación de fallos detectados requiere ciclos iterativos de cinta completa.

Se puede encontrar información básica en "Fault Simulation and Emulation Tools to Augment Radiation-Hardness Assurance Testing", IEEE TRANSACTIONS ON NUCLEAR SCIENCE de Heather Quinn y col. y en el documento US 2013/096902.

Sumario

La invención se define en la reivindicación independiente. Las reivindicaciones dependientes definen realizaciones preferidas. Una realización ejemplar del objeto divulgado es un mecanismo informatizado para la evaluación de vulnerabilidad en un diseño que tiene unidades de circuito como interceptores, que comprende recibir un diseño con interceptores incorporados en posiciones preestablecidas, prácticamente induciendo fallos en la disposición al modelar un fenómeno físico que afecta los tiempos en la disposición, detectar violaciones de tiempo en la disposición que responden a los fallos inducidos en función de las discrepancias entre los tiempos y las especificaciones proporcionadas para determinar la vulnerabilidad de la disposición a los fallos de acuerdo con los fallos detectados, y en el que el procedimiento se realiza en al menos un aparato informatizado configurado para realizar el procedimiento.

En otra realización ejemplar del objeto divulgado, el fenómeno físico es un haz láser virtual que tiene una intensidad representada por un factor de tiempo y un diámetro según el cual la disposición se divide en particiones de células y redes, escaneando el haz la disposición por las particiones y alterando en las particiones los tiempos especificados de las células y redes de acuerdo con el factor de tiempo, y en el que detectar violaciones de tiempo en la disposición comprende detectar en cada partición discrepancias entre los tiempos de las células y las redes y las especificaciones proporcionadas de los mismos, y en el que determinar la vulnerabilidad de la disposición a los fallos es de acuerdo con las violaciones de tiempo detectadas fuera de los interceptores.

En alguna otra realización ejemplar del objeto divulgado, el fenómeno físico es una irradiación electromagnética modelada.

Breve descripción de los dibujos

Algunas realizaciones o características ejemplares no limitativas del objeto divulgado se ilustran en los siguientes dibujos.

Estructuras idénticas o duplicadas o equivalentes o similares, elementos o partes que aparecen en uno o más dibujos generalmente están etiquetados con el mismo número de referencia y pueden no etiquetarse y/o describirse repetidamente.

Las dimensiones de los componentes y las características que se muestran en las figuras se eligen por conveniencia o claridad de presentación y no necesariamente se muestran a escala o perspectiva real. Por conveniencia o claridad, algunos elementos o estructuras no se muestran o se muestran solo parcialmente y/o con diferentes perspectivas o desde diferentes puntos de vista.

Las referencias a elementos presentados anteriormente están implícitas sin citar necesariamente más el dibujo o la descripción en la que aparecen.

La figura 1A ilustra esquemáticamente un diseño de células en el que algunas de las cuales son interceptoras, de acuerdo con realizaciones ejemplares del objeto divulgado;
La figura 1B ilustra esquemáticamente la disposición de la figura 1A con una representación de un rayo láser que irradia la disposición, de acuerdo con realizaciones ejemplares del objeto divulgado;
La figura 1C ilustra esquemáticamente una aproximación rectangular de un haz circular, de acuerdo con realizaciones ejemplares del objeto divulgado;
La figura 2A ilustra esquemáticamente y concisamente un diseño similar al diseño de la figura 1C con particiones, cada partición denotada como una partición 118, basado en repeticiones del cuadrado 116, de acuerdo con realizaciones ejemplares del objeto divulgado;
La figura 2B ilustra esquemáticamente y concisamente la disposición y las particiones a partir de la figura 2A con indicaciones de particiones que son susceptibles de intrusión de acuerdo con la evaluación de las intercepciones de fallos, de acuerdo con realizaciones ejemplares del objeto divulgado; y
La figura 2C describe esquemáticamente las operaciones en la evaluación de la intercepción de fallos, de acuerdo

con realizaciones ejemplares del objeto divulgado.

Descripción detallada

En el contexto de la presente divulgación y, a menos que se especifique lo contrario, los circuitos se expresan en construcciones de descripción de hardware y/o por modelos en los que el funcionamiento de los mismos puede simularse o analizarse de otro modo con herramientas adecuadas, tales como, por ejemplo, Verilog o VHDL.

Igualmente, a menos que se especifique lo contrario, las operaciones aplicadas a los circuitos se aplican virtualmente a los circuitos virtuales.

En el contexto de la presente divulgación, sin limitar, referirse a entidades o fenómenos u ocurrencias 'virtuales' implica una suplantación o imitación o modelado de las entidades o fenómenos u ocurrencias, respectivamente.

En el contexto de la presente divulgación, sin limitar, un "diseño" es un diseño de un circuito electrónico con la colocación de los componentes y las interconexiones entre ellos.

En el contexto de la presente divulgación, sin limitar, un 'interceptor de fallos', o brevemente un 'interceptor', implica una unidad de circuito tal como una célula o un bloque que comprende algunos elementos lógicos de operación diseñada y/o propiedades que responden a la interferencia con la misma o la perturbación de la misma que exhiben funcionalidades o propiedades diferentes a las de circunstancias normales no perturbadas. Por lo tanto, al comparar o evaluar las respuestas de los interceptores a las respuestas normalmente esperadas, se pueden identificar intrusiones, es decir, interceptado.

Un interceptor puede ser un circuito independiente entre otras unidades lógicas y/o puede estar interconectado con otras unidades o circuitos.

En el contexto de la presente divulgación, sin limitar, referirse a la inyección de fallos implica efectuar o inducir o provocar fallos o mal funcionamiento en un circuito.

En el contexto de la presente divulgación, sin limitar, una 'célula' implica una unidad de lógica o circuitería, como una célula estándar de ASIC o un bloque en FPGA o cualquier otra unidad de una biblioteca determinada.

Cuando una célula se establece en un diseño, entonces, generalmente, la célula está asociada con las interconexiones de la misma, en el que las interconexiones pueden referirse a una 'red'.

Generalmente, una célula está asociada con parámetros pertenecientes a la lógica o circuitería de la misma y, al menos opcionalmente, parámetros u otra información relacionada con las redes o redes parciales (subredes), que especifican datos operativos de la célula y/o redes, como los tiempos, retrasos u otros datos relacionados con la progresión de una señal a lo largo de una ruta de conexiones. Los parámetros son o pueden ser proporcionados por la práctica de la técnica, como en el archivo de formato de retardo estándar (SDF) o en el archivo de restricciones de diseño de sinopsis (SDC).

Los términos citados anteriormente denotan también inflexiones y conjugados de los mismos.

Un problema técnico tratado por el objeto divulgado es evaluar la intercepción de fallos en circuitos integrados en una fase de diseño pre-silicio.

Una solución técnica de acuerdo con el objeto divulgado es incorporar interceptores de fallos en el diseño de la disposición, posteriormente inyectando o efectuando fallos en la disposición y determinando la extensión de la detección de los fallos.

Los fallos pueden ser debidos o generados por varios fenómenos o incidentes con diversas cantidades y localidades que pueden interrumpir el funcionamiento adecuado de los circuitos electrónicos e inducir o generar fallos. Por ejemplo, tales fenómenos pueden ser la irradiación con un rayo láser que está enfocado y localizado de manera estrecha y puede ser de intensidad o densidad de energía sustancialmente alta. O, por ejemplo, tales fenómenos pueden ser la aplicación de un campo electromagnético o un campo eléctrico o magnético que está menos localizado que un rayo láser y puede ser de menor densidad de campo que un rayo láser. O, por ejemplo, tales fenómenos pueden ser cualquier otro fenómeno como el calentamiento que generalmente se disipa y, por lo tanto, está menos localizado al menos que un rayo láser.

Una característica que puede ser común a los fallos, al menos parcialmente, está aumentando o alterando la disposición de electrones y/o emisiones que pueden afectar negativamente el funcionamiento de los elementos electrónicos que, generalmente al menos, están finamente ajustados y coordinados con elementos conectados.

En algunas realizaciones, para aumentar la confiabilidad de la intercepción de fallos, la cantidad y/o intensidad de los fenómenos para generar los fallos son variadas, por ejemplo, la intensidad de un rayo láser aumenta o la temperatura disminuye.

Generalmente, en la fase de diseño, un fallo se hace perceptible al alterar la respuesta de tiempo atribuida a un elemento lógico, cuanto mayor es la intensidad de los fenómenos para generar el fallo, mayor es la discrepancia temporal debido a capacidades y/o inducciones y/o movimientos brownianos.

Por ejemplo, cuanto mayor es la intensidad del láser atribuido, más rápido es el tiempo de respuesta ya que aparentemente hay más electrones emitidos que reducen las impedancias y menor es el enfriamiento, es decir, disminución del calentamiento, cuanto más lento es el tiempo de respuesta, ya que hay menos electrones libres en relación con las condiciones ordinarias.

Un posible efecto técnico del objeto divulgado es un circuito electrónico tolerante a fallos, al menos en el sentido de interceptar intrusiones.

Otro posible efecto técnico del objeto divulgado es un circuito electrónico tolerante a fallos, al menos en el sentido de tener y/o aumentar la probabilidad de que ocurran fallos inofensivos en los interceptores en lugar de que ocurran fallos dañinos en otras partes de los circuitos electrónicos.

A continuación se presenta una descripción general no limitativa de la práctica de la presente divulgación. El resumen describe la práctica ejemplar de realizaciones de la presente divulgación, proporcionando una base constructiva para realizaciones variantes y/o alternativas y/o divergentes, algunas de las cuales se describen posteriormente.

La figura 1 ilustra esquemáticamente, de acuerdo con realizaciones ejemplares del objeto divulgado, un diseño 100 de células como instancias de una célula 102 en el que algunas de las células son interceptoras y en el que cada interceptor se denota como un interceptor 104 y se marca como 'detector CM'.

Se observa que cualquier instancia de la célula 102 no es necesariamente igual o equivalente a cualquier otra célula 102; igualmente, se observa que cualquier interceptor 104 de instancia no es necesariamente igual o equivalente a cualquier otro interceptor 104.

El diseño 100 representa cualquier diseño de cualquier extensión y de cualquier célula, y la cantidad y ubicaciones y/o disposición de los interceptores en la disposición representan cualquier asignación o configuración adecuada y/o factible de interceptores en la disposición. La determinación de las asignaciones y disposiciones de interceptores en un diseño se analizan más adelante.

A modo de ejemplo, un rayo láser escanea un diseño como para entrometerse o inferir el funcionamiento de los circuitos en la disposición mediante un procedimiento de escaneo similar a las técnicas de la técnica.

La figura 1B ilustra esquemáticamente la disposición 100 con una representación de un rayo láser designado como un haz 112 que tiene un diámetro indicado como un diseño 100 de irradiación de diámetro 114, de acuerdo con realizaciones ejemplares del objeto divulgado.

La figura 1C ilustra esquemáticamente una aproximación rectangular de un haz circular, de acuerdo con realizaciones ejemplares del objeto divulgado.

Como la disposición generalmente está formado por células rectangulares, el haz 112 es aproximado y representado por un cuadrado 116. Por consiguiente, la exploración por el haz 112 se aproxima repitiendo gradualmente el cuadrado 116 sobre la disposición 100.

La figura 2A ilustra esquemáticamente y concisamente la disposición 100 con particiones basadas en repeticiones de representaciones rectangulares de un haz circular como el cuadrado 116 similar a la figura 1C, de acuerdo con realizaciones ejemplares del objeto divulgado.

Las repeticiones incrementales de la disposición 100 de división del cuadrado 116 en particiones denotaron de forma ejemplar un '*S_00*' a *'S_31',* en el que cada una de las particiones pertenece o está asociada con células y redes y viceversa, como se ejemplifica arbitrariamente en la Tabla-1 a continuación, en el que algunas células ejemplares se muestran en la figura 1C en el cuadrado 116 respectivo al haz 112.

Tabla-1

Partición	Redes
S-00	NET3, NET36, AND21, ...
S_01	N563, NET4355, NOR324, ...
S_31	N42, MUX2, XOR34, ...

Como el cuadrado 116 divide la disposición 100 en particiones basadas en el tamaño del mismo, es probable que las

redes se corten o desconecten arbitrariamente. Por lo tanto, en algunas realizaciones, la asociación de particiones con redes se lleva a cabo de acuerdo con algunas pautas o restricciones, como asignar cualquiera de los cuadrados 116 a una red que pueda pertenecer a la misma y/o evitar redundancias de redes en particiones.

La figura 2B ilustra esquemáticamente y concisamente la disposición y las particiones a partir de la figura 2A con indicaciones de particiones que son susceptibles de intrusiones de acuerdo con la evaluación de las intercepciones de fallos como se describe en la figura 2C descrita a continuación, de acuerdo con realizaciones ejemplares del objeto divulgado.

La figura 2C describe esquemáticamente las operaciones 200 en la evaluación de la intercepción de fallos, de acuerdo con realizaciones ejemplares del objeto divulgado.

En la operación 202, se establece un diámetro de un haz virtual que imita un haz láser, tal como se usa en la técnica para la intrusión o el análisis de caja negra de circuitos como el ASIC.

Opcionalmente, el diámetro representa un diámetro o una extensión de otros medios, como una sección transversal de una irradiación electromagnética.

En la operación 204, la intensidad del haz se establece como un factor de tiempo que representa el efecto sobre los tiempos y los retrasos y/o la progresión de la señal en una célula o una red.

Una razón potencial para representar la intensidad por un factor de temporización se debe al efecto del haz sobre la cantidad y/o disposición de electrones, como el efecto fotoeléctrico.

Opcionalmente, el factor de tiempo representa la intensidad y/o densidad de energía de una irradiación electromagnética.

Por brevedad y a menos que se especifique lo contrario, la referencia a un rayo como un rayo láser representa, *mutatis mutandis,* cualquier medio disruptivo.

En la operación 206, un diseño compuesto por interceptores y provisto para evaluación de vulnerabilidad se divide en particiones de acuerdo con el diámetro. Generalmente, una partición cubre una o más células y/o una o más redes o subredes, aunque una partición puede no cubrir ningún componente.

En la operación 208, las células y redes o partes de las mismas pertenecientes a cada partición se obtienen o derivan de la disposición de la disposición.

En la operación 210, se selecciona una partición. Generalmente aunque sin limitar, se selecciona una partición desde una esquina de la disposición como primera partición en una secuencia que viene, por ejemplo, una partición denotada como *'S_00'* en la figura 2A.

En la operación 212, los parámetros de tiempo de las células y redes pertenecientes a la partición se modifican por el factor de tiempo, modelando así, al menos hasta cierto punto, el efecto del haz que irradia la partición.

La intensidad del haz, tal como se modela, generalmente afecta la desaceleración del funcionamiento o la respuesta de las células y/o redes de la partición, aunque no se impide la aceleración de la operación o respuesta de las células y/o redes de la partición.

La operación 212 también se etiqueta como ***A*** para referencia de una continuación de la figura 2C en una página posterior.

En la operación 214, el análisis de tiempo de las células y redes pertenecientes a la partición se realiza para determinar el efecto virtual del haz tal como se modela o imita.

Las operaciones 200 proceden en una página siguiente en una ubicación etiquetada como ***B,*** como se muestra también con una flecha 216 discontinua.

En la operación 218, se verifica si se ha detectado una violación de tiempo en el análisis. Si no se detectó la violación del tiempo, el control se transfiere a la operación 224; de lo contrario, el control se transfiere a la operación 220.

En la operación 220, se verifica si la violación de tiempo ocurrió en un interceptor. Si la violación de tiempo ocurrió en un interceptor, entonces el control se transfiere a la operación 224; de lo contrario, el UE avanza a la operación 222.

En la operación 222, como la violación de tiempo ocurrió pero no en un interceptor, la partición seleccionada actualmente, inclusiva de las células y redes en el mismo, está marcado como susceptible de intrusión. La partición está marcada por cualquier técnica, como el etiquetado, la clasificación, puntuación o cualquier otra técnica, como registrarse o grabar en una lista o base de datos.

El marcado de una partición como susceptible de intrusión se ejemplifica figurativamente en cualquier partición 118 en la figura 2B que se oscurece con respecto a cualquiera de la partición 118 en la figura 2A.

Se observa que, si bien la infracción de tiempo en una partición se considera vulnerabilidad, La violación de tiempo en un interceptor se considera neutral o inmaterial ya que los interceptores no son parte de los circuitos de la disposición *per se,* y aparte de las violaciones de intercepción, los interceptores son efectiva o prácticamente inertes o inactivos en lo que respecta al funcionamiento previsto de la disposición.

En la operación 224, alcanzado desde la operación 218 o 220, se verifica si todavía hay particiones pendientes que no se manejaron.

Si hay particiones pendientes, controle las transferencias a la operación 226 en el que se selecciona la siguiente partición pendiente, y controle las transferencias a la operación 212 etiquetadas también como 'A' para una iteración en la partición seleccionada actualmente como se indica mediante una flecha 228 discontinua; en caso contrario, si no hay más particiones pendientes, la evaluación finaliza al menos en lo que respecta al presente paso o ejecución de las operaciones 200 (operación 230).

En consecuencia, en algunas realizaciones, la disposición se decide o determina como vulnerable si se detectan infracciones de tiempo fuera de los interceptores, opcionalmente basado en la cantidad y/o conteo de tales violaciones, por ejemplo, violaciones menores no contribuyen a la decisión de vulnerabilidad. Opcional o alternativamente, se realizan algunas operaciones o procedimientos adicionales, como la reiteración y/o algunos procedimientos terminales.

En algunas realizaciones, las operaciones 200 se repiten o reiteran con diferentes configuraciones. Por ejemplo, el haz se imita o modela para escanear virtualmente la disposición en intensidades progresivamente incrementadas para modelar intrusiones más potentes. Igualmente, el diámetro del rayo puede alterarse y el rayo se imita o modela para escanear virtualmente la disposición en particiones de diferente tamaño o tamaños.

En algunas realizaciones, después de que las operaciones 200 hayan terminado, se realizan algunos procedimientos terminales. Por ejemplo, se evalúa la vulnerabilidad de la disposición y, en consecuencia, los interceptores se agregan y/o mueven en la disposición y, opcionalmente, se eliminan los interceptores. Generalmente, en algunas realizaciones, después de tales modificaciones, la vulnerabilidad de la disposición se evalúa nuevamente como con las operaciones 200 como se describió anteriormente.

Se observa que las infracciones de tiempo generalmente se determinan dentro de cierta tolerancia o tolerancias. Generalmente, las tolerancias de temporización varían entre ubicaciones en un diseño de acuerdo con las puertas o elementos lógicos y conexiones entre ellas y la longitud de las conexiones. En algunos casos, las tolerancias varían según el reloj y/o el tiempo de propagación de las señales entre los elementos del diseño, y posiblemente también según la naturaleza de los elementos en el que algunos elementos pueden ser más sensibles a las variaciones de temporización y otros pueden ser más robustos o resistentes a tales variaciones.

El orden y/o las funciones de las operaciones 200 se proporcionan a modo de ejemplo y pueden variar o modificarse.

Por ejemplo, establecer el factor de temporización puede preceder al ajuste del diámetro, o la obtención de redes de particiones correspondientes (operación 208) se puede realizar por separado para cada partición seleccionada, o establecer un diámetro e intensidad del haz se puede hacer en combinación o en paralelo.

Mientras que el haz escanea la disposición con el diámetro, en algunas realizaciones, se generan fallos menos localizados y/o generales en la disposición, y para identificar los fallos, las particiones pueden verificarse como o como en las operaciones 200 de acuerdo con las particiones o la granularidad del haz, en el que los tamaños de las particiones o extensiones de la granularidad dependen del diámetro del haz.

En algunas realizaciones, las particiones no son necesariamente cuadradas o rectangulares. Por ejemplo, se pueden usar particiones hexagonales que, al menos potencialmente, representan áreas circulares mejor que las rectangulares.

En algunas realizaciones, se permite cierta superposición entre particiones, como para una mejor separación de la funcionalidad de las células y las redes.

Se observa que las infracciones de tiempo se proporcionan como fallos ejemplares, y otros fallos pueden detectarse y analizarse detectadas de manera similar o variada y bajo el ámbito de la presente divulgación. Por ejemplo, se pueden detectar y analizar corrientes o tensiones anómalas o estados inestables y se puede determinar y evaluar la vulnerabilidad de la disposición, *mutatis mutandis,* como con respecto al tiempo.

Generalmente, existe una compensación entre las cantidades de interceptores y/o la densidad de los mismos en un diseño y entre otros factores o restricciones.

Aunque, ingenuamente, tener tantos interceptores como aspirantes es beneficioso, sin embargo, tener numerosos interceptores puede aumentar el tamaño del diseño y/o el consumo de energía y/o la generación de calor y/o enfrentar otros aspectos perjudiciales como la complejidad del diseño o no dejar suficiente 'bienes raíces'.

Por lo tanto, en algunas realizaciones, se determina un equilibrio o compensación entre el número de interceptores y la funcionalidad de los mismos, como por una disposición adecuada de interceptores y, opcionalmente, teniendo en cuenta qué secciones del diseño son más sensibles y/o vulnerables que otras.

En algunas realizaciones, algunos programas y/o pautas heurísticas están diseñados y/o implementados para la disposición de interceptores, opcionalmente en combinación con otras técnicas.

En algunas realizaciones, la disposición de los interceptores en un diseño se expresa de forma cualitativa y/o cuantitativa. Por ejemplo, una expresión como *(número de particiones con al menos 1 interceptor*/*(número total de particiones),* o una expresión como *(número de particiones en las que se ha identificado una violación de temporización)*/*(número total de particiones).*

Adicionalmente, en algunas realizaciones, las expresiones cuantitativas como las anteriores pueden usarse como funciones de objetivo para determinar la disposición de los interceptores en una disposición, posiblemente con ajustes y/o ajustes por otros factores como la sensibilidad o la complejidad.

Cabe señalar que, además y/o como alternativa a la detección y análisis de fallos con respecto a los interceptores y al resto de la disposición, en algunas realizaciones, la respuesta de los interceptores a las intrusiones se utiliza para determinar si la disposición se entrometió y, opcionalmente, en qué región de la disposición.

Con una disposición densa suficiente de los interceptores, posiblemente teniendo en cuenta las limitaciones y restricciones mencionadas anteriormente, la probabilidad o la confiabilidad de la detección de intrusos por parte de los interceptores puede aumentar o al menos lograrse satisfactoriamente y, opcionalmente, con mejor localización de la detección de intrusos.

El objetivo de los procedimientos de la presente solicitud es lograr un circuito, por ejemplo, como en un microchip o como cualquier otra implementación, como un ASIC o una parte de un producto VLSI, en el que el circuito es seguro contra intrusiones al menos prácticamente y/o en un grado considerable o adecuado.

Para lograr el objetivo, Se utilizan varias herramientas de diseño electrónico, por ejemplo, codificación por lenguaje de transferencia de registro (RTL), compilando o convirtiendo el código en la lista de elementos básicos de la red lógica y asignando mediante una biblioteca de células estándar digital específica para tecnología de planta/procedimiento de fabricación de microchips (FAB) y colocación de las células en una disposición.

Adicionalmente, los interceptores se incorporan en la disposición en función de al menos análisis de tiempo y otras funciones adicionales como las expresiones cuantitativas mencionadas anteriormente, que implican operaciones iterativas para obtener al menos un diseño aparentemente seguro con suficiente seguridad en el sentido de protección contra intrusiones y/o detección de intrusiones antes de que se produzca un daño.

Evidentemente y con claridad, los mecanismos y operaciones descritos anteriormente están mucho más allá de las capacidades de los humanos, incluso con ayuda de lápiz y papel o calculadoras, y solo puede llevarse a cabo mediante maquinaria como procesadores electrónicos que utilizan dispositivos de memoria integrados y/o separados, entrada/salida y/u otras funcionalidades como las comunicaciones. Por lo tanto, indudablemente, los mecanismos y procedimientos divulgados en el presente documento están vinculados a una máquina para su implementación.

Por consiguiente, las operaciones 200 y las fases de diseño de un diseño tal como la disposición 100 se llevan a cabo mediante un sistema informatizado que opera al menos un procesador.

Por lo tanto, según la presente divulgación, se proporciona un mecanismo informatizado para la evaluación de vulnerabilidad en un diseño que tiene unidades de circuito como interceptores, que comprende al menos un aparato informatizado configurado para realizar operaciones que incluyen recibir un diseño con interceptores incorporados en posiciones preestablecidas, prácticamente induciendo fallos en la disposición al modelar un fenómeno físico que afecta los tiempos en la disposición, detectar violaciones de tiempo en la disposición que responden a los fallos inducidos en función de las discrepancias entre los tiempos y las especificaciones proporcionadas de los mismos, y determinar la vulnerabilidad de la disposición a los fallos según los fallos detectados.

En algunas realizaciones, el fenómeno físico es un rayo láser virtual que tiene una intensidad representada por un factor de tiempo y un diámetro según el cual la disposición se divide en particiones de células y redes. El rayo escanea la disposición con el diámetro para dividir la disposición en particiones y altera los tiempos especificados de las células y las redes de las particiones de acuerdo con el factor tiempo. En el que, la operación de detectar violaciones de tiempo en la disposición comprende detectar en cada partición discrepancias entre los tiempos de las células y las redes y las especificaciones proporcionadas de las mismas. En el que, la operación para determinar la vulnerabilidad de la disposición a los fallos se realiza de acuerdo con las violaciones de tiempo detectadas fuera de los interceptores.

En algunas realizaciones, virtualmente induciendo fallos en la disposición al modelar un fenómeno físico que afecta los tiempos en la disposición y luego detectando violaciones de tiempo en la disposición que responden a los fallos inducidos y luego determinando la vulnerabilidad de la disposición a los fallos según los fallos detectados se repite al menos una vez más con diferentes intensidades que afectan de manera diferente los tiempos en la disposición.

En algunas realizaciones, virtualmente induciendo fallos en la disposición al modelar un fenómeno físico que afecta los tiempos en la disposición y luego detectando violaciones de tiempo en la disposición que responden a los fallos inducidos y luego determinando la vulnerabilidad de la disposición a los fallos según los fallos detectados se repite al

menos una vez más con diferentes extensiones del fenómeno físico modelado que afectan de manera diferente los tiempos en la disposición.

En algunas realizaciones, las posiciones de los interceptores en la disposición se modifican en respuesta a la determinación de la vulnerabilidad de la disposición a los fallos y la repetición adicional del mecanismo para una mayor verificación de la vulnerabilidad de la disposición a los fallos.

En algunas realizaciones, la cantidad de interceptores en la disposición se modifica en respuesta a la determinación de la vulnerabilidad de la disposición a los fallos y la repetición adicional del mecanismo para una mayor verificación de la vulnerabilidad de la disposición a los fallos.

En algunas realizaciones, las posiciones y la cantidad de los interceptores en la disposición se modifican en respuesta a la determinación de la vulnerabilidad de la disposición a los fallos y la repetición adicional del mecanismo para una mayor verificación de la vulnerabilidad de la disposición a los fallos.

En algunas realizaciones, determinar la vulnerabilidad de la disposición a los fallos de acuerdo con los fallos detectados se basa en las detecciones de violaciones de temporización en los interceptores.

En algunas realizaciones, el fenómeno físico modelado es una irradiación electromagnética modelada.

En algunas realizaciones, el fenómeno físico modelado es un calentamiento modelado.

En el contexto de algunas realizaciones de la presente divulgación, a modo de ejemplo, y sin limitación, términos como 'operar' o 'ejecutar' implican también capacidades, como 'operable' o 'ejecutable', respectivamente.

Términos conjugados como, a modo de ejemplo, 'una propiedad de la cosa' implica una propiedad de la cosa, a menos que sea claramente evidente por el contexto de los mismos.

Los términos 'procesador' o 'ordenador', o sistema de los mismos, se usan en el presente documento como contexto ordinario de la técnica, como un procesador de uso general o un microprocesador, procesador RISC o DSP, posiblemente comprende elementos adicionales como memoria o puertos de comunicación. Opcional o adicionalmente, los términos 'procesador' o 'ordenador' o derivados de los mismos denotan un aparato que es capaz de llevar a cabo un programa provisto o incorporado y/o es capaz de controlar y/o acceder al aparato de almacenamiento de datos y/u otro aparato como puertos de entrada y salida. Los términos 'procesador' o 'ordenador' denotan también una pluralidad de procesadores u ordenadores conectados, y/o vinculados y/o comunicados de otra manera, posiblemente compartiendo uno o más recursos como una memoria.

El término aparato informatizado o un sistema informatizado o un término similar denota un aparato que comprende uno o más procesadores operables u operando de acuerdo con uno o más programas.

El diagrama de flujo y los diagramas de bloques ilustran la arquitectura, funcionalidad o una operación de posibles implementaciones de sistemas, procedimientos y productos de programa informático de acuerdo con diversas realizaciones del presente objeto divulgado. En este sentido, cada bloque del diagrama de flujo o de los diagramas de bloques puede representar un módulo, segmento o porción de código de programa, que comprende una o más instrucciones ejecutables para implementar la función(es) lógica especificada. También debe tenerse en cuenta que, en algunas implementaciones alternativas, las operaciones ilustradas o descritas pueden ocurrir en un orden diferente o en combinación o como operaciones concurrentes en lugar de operaciones secuenciales para lograr el mismo efecto o equivalente.

Las correspondientes estructuras, materiales, actos y equivalentes de todos los medios o elementos de función más etapa en las reivindicaciones a continuación pretenden incluir cualquier estructura, material, o acto para realizar la función en combinación con otros elementos reivindicados como se reivindica específicamente. Tal como se usan en el presente documento, las formas singulares "un", "una" y "el/la" se pretende que incluyan asimismo las formas plurales, a menos que el contexto indique claramente lo contrario. Se entenderá además que los términos "comprende" y/o "que comprende" y/o "que tiene" cuando se usan en esta especificación, especifican la presencia de características, integrantes, etapas, operaciones, elementos y/o componentes declarados, pero no excluye la presencia o adición de una o más características adicionales, integrantes, etapas, operaciones, elementos, componentes y/o grupos de los mismos.

La terminología utilizada en el presente documento no debe entenderse como limitante, a menos que se especifique otra cosa, y es para el fin de describir realizaciones particulares únicamente y no se pretende que sea limitante del objeto divulgado. Si bien se han ilustrado y descrito ciertas realizaciones del objeto divulgado, quedará claro que la divulgación no se limita a las realizaciones descritas en el presente documento. Numerosas modificaciones, cambios, variaciones, sustituciones y equivalentes no están excluidos.

REIVINDICACIONES

1. Un mecanismo informatizado para evaluación de vulnerabilidad en una disposición (100) que tiene células (102) y unidades de circuitos como interceptores (104), que comprende al menos un aparato informatizado configurado para realizar operaciones (200) que incluye:

recibir la disposición (100) con interceptores (104) incorporados en posiciones preestablecidas;
virtualmente induciendo fallos en la disposición al modelar un fenómeno físico que afecta los tiempos en la disposición (100);
detectar violaciones de tiempo en las células (102) e interceptores (104) que responden a los fallos inducidos en función de las discrepancias entre los tiempos y las especificaciones proporcionadas de los mismos; y
determinar la vulnerabilidad de la disposición (100) a fallos de acuerdo con las violaciones de tiempo detectadas fuera de los interceptores (104).

2. El mecanismo de acuerdo con la reivindicación 1, en el que la disposición (100) se divide en particiones (118) que incluyen las células (102), redes o una combinación de las mismas según un diámetro (114) del fenómeno físico.

3. El mecanismo de acuerdo con la reivindicación 2, en el que el fenómeno físico es un haz (112) láser virtual que tiene una intensidad representada por un factor de tiempo y el diámetro (114), el haz (112) altera los tiempos especificados de las células (102) y las redes de las particiones (118) de acuerdo con el factor tiempo.

4. El mecanismo de acuerdo con la reivindicación 2, en el que la operación de detectar violaciones de temporización en las células (102) e interceptores (104) comprende detectar en cada partición (118) discrepancias entre los temporizadores de las células (102) y las redes y las especificaciones proporcionadas de las mismas.

5. El mecanismo de acuerdo con la reivindicación 1, en el que el aparato informatizado realiza la operación de inducir fallos virtualmente en la disposición (100) modelando un fenómeno físico que afecta los tiempos en la disposición (100), la operación de detectar violaciones de temporización en las células (102) e interceptores (104) que responden a los fallos inducidas, y la operación de determinar la vulnerabilidad del disposición (100) a los fallos de acuerdo con los fallos detectadas secuencial y repetidamente con diferentes intensidades que afectan de manera diferente tiempos en la disposición (100).

6. El mecanismo de acuerdo con la reivindicación 1, en el que el aparato informatizado realiza la operación de inducir fallos virtualmente en la disposición (100) al modelar un fenómeno físico que afecta los tiempos en las células (102) e interceptores (104), la operación de detectar violaciones de temporización en la disposición (100) en respuesta a los fallos inducidas, y la operación de determinar la vulnerabilidad de la disposición (100) a fallos de acuerdo con las violaciones de temporización detectadas fuera de los interceptores (104) secuencial y repetidamente con diferentes extensiones del fenómeno físico modelado que afecta de manera diferente a los tiempos en la disposición (100).

7. El mecanismo de acuerdo con la reivindicación 1, en el que las posiciones de los interceptores (104) en la disposición (100) se modifican en respuesta a la operación de determinar la vulnerabilidad de la disposición (100) a fallos y el aparato informatizado realiza además las operaciones repetidamente para verificar más a fondo la vulnerabilidad de la disposición (100) a fallos.

8. El mecanismo de acuerdo con la reivindicación 1, en el que la cantidad de los interceptores en la disposición (100) se modifica en respuesta a la operación de determinar la vulnerabilidad de la disposición (100) a fallos y el aparato informatizado realiza además las operaciones repetidamente para verificar más a fondo la vulnerabilidad de la disposición (100) a los fallos.

9. El mecanismo de acuerdo con la reivindicación 1, en el que las posiciones y la cantidad de los interceptores (104) en la disposición (100) se modifican en respuesta a la operación de determinar la vulnerabilidad de la disposición (100) a fallos y el aparato informatizado realiza además las operaciones repetidamente para una mayor verificación de la vulnerabilidad de la disposición (100) a fallos.

10. El mecanismo de acuerdo con la reivindicación 1, en el que el fenómeno físico modelado es una irradiación electromagnética modelada.

11. El mecanismo de acuerdo con la reivindicación 1, en el que el fenómeno físico modelado es un calentamiento modelado.

Fig. 1A

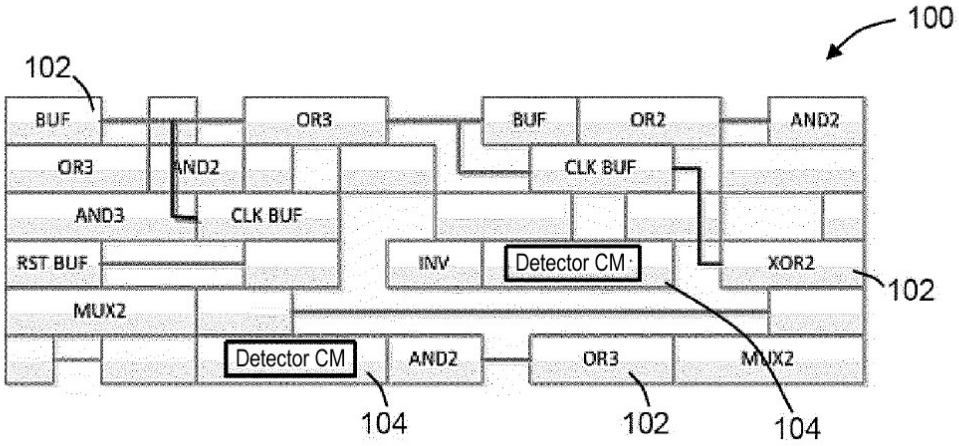

Fig. 1B

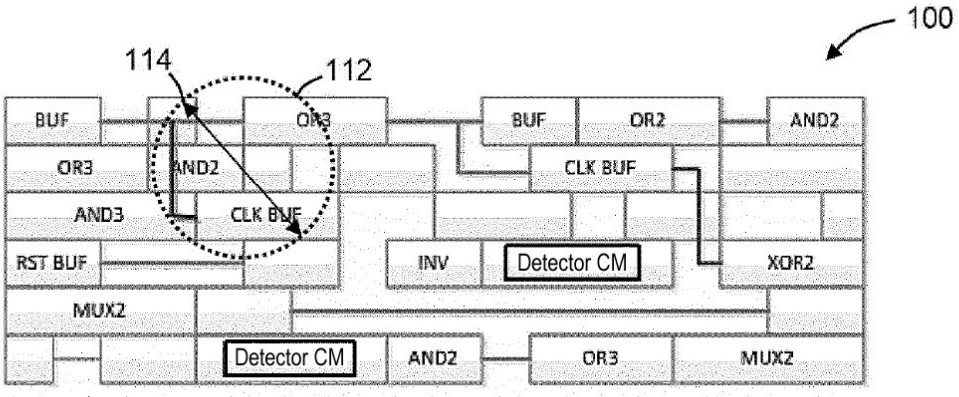

Fig. 1C

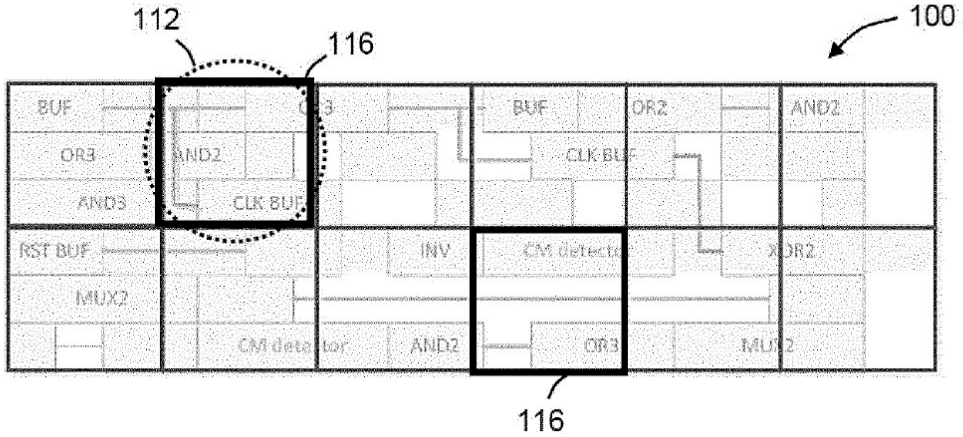

Fig. 2A

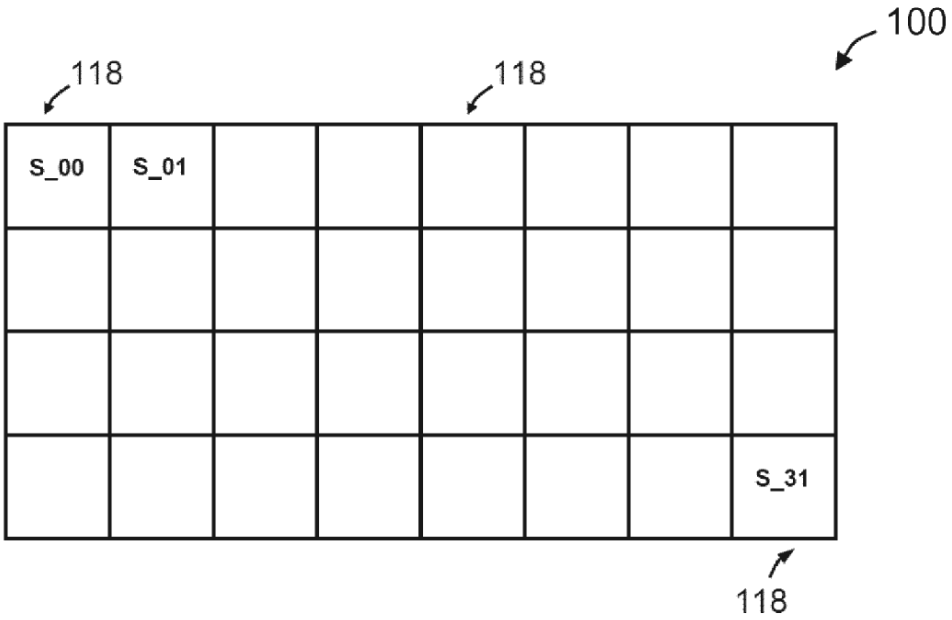

Fig. 2B

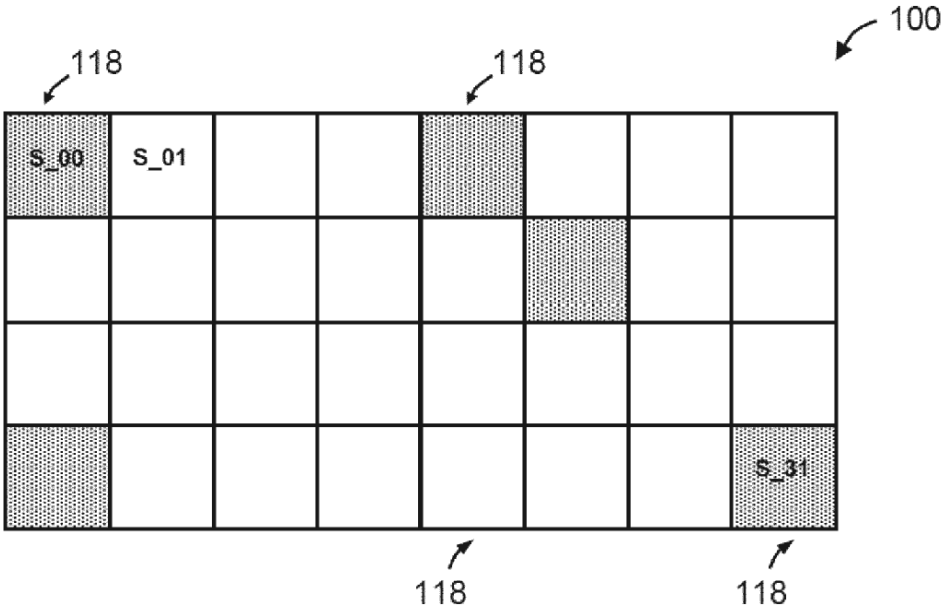

Fig. 2C

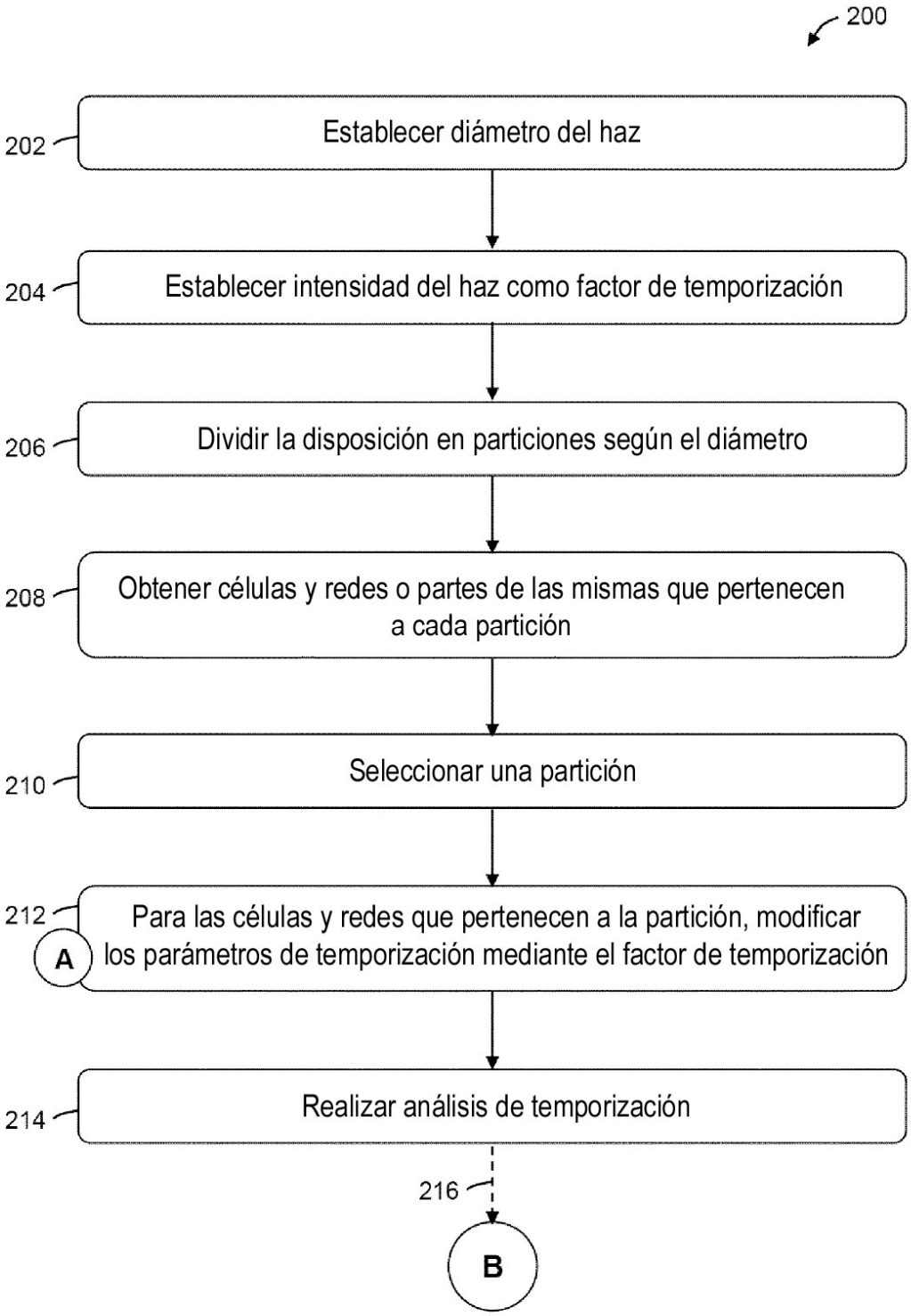
200
202
Establecer diámetro del haz
204
Establecer intensidad del haz como factor de temporización
206
Dividir la disposición en particiones según el diámetro
208
Obtener células y redes o partes de las mismas que pertenecen a cada partición
210
Seleccionar una partición
212
A
Para las células y redes que pertenecen a la partición, modificar los parámetros de temporización mediante el factor de temporización
214
Realizar análisis de temporización
216
B

Fig. 2C (continuación)