

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **3 019 233**

51 Int. Cl.:

H01L 23/00 (2006.01)

H01L 23/58 (2006.01)

H01L 23/488 (2006.01)

H01L 21/02 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **17.10.2019** **PCT/EP2019/078247**

87 Fecha y número de publicación internacional: **30.04.2020** **WO20083745**

96 Fecha de presentación y número de la solicitud europea: **17.10.2019** **E 19786606 (4)**

97 Fecha y número de publicación de la concesión europea: **12.03.2025** **EP 3871252**

54 Título: **Protección de chips de circuito integrado empaquetados con matriz de rejilla de bolas de unión por alambre**

30 Prioridad:

26.10.2018 EP 18202853

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

20.05.2025

73 Titular/es:

NAGRAVISION SÀRL (100.00%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

72 Inventor/es:

AUBRY, PASCAL y
MCLAUCHLAN, ANDREW

74 Agente/Representante:

DEL VALLE VALIENTE, Sonia

ES 3 019 233 T3

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

DESCRIPCIÓN

Protección de chips de circuito integrado empaquetados con matriz de rejilla de bolas de unión por alambre

5 Campo

La presente invención se refiere a un chip de circuito integrado protegido contra alteraciones físicas y/o eléctricas y, más específicamente, se dirige a proteger los circuitos integrados que están empaquetados en forma de matriz de rejilla de bolas de unión por alambre.

10

Antecedentes de la técnica

Los chips de circuitos integrados (IC) suelen ser objeto de ataques físicos, como el análisis de hardware en vivo, con el objetivo de obtener conocimiento del funcionamiento interno del chip y, en consecuencia, influir en el funcionamiento del chip.

15

Durante un ataque de este tipo, el alojamiento de plástico que protege el chip contra daños mecánicos puede abrirse en su cara superior para revelar una capa de pasivación que cubre el sistema de circuitos electrónicos.

20

La capa de pasivación se puede eliminar selectivamente mediante métodos de grabado utilizando un pulidor mecánico o medios químicos para permitir el acceso a las líneas de señal.

Las técnicas de análisis de hardware en vivo se pueden realizar en chips de circuitos integrados durante su funcionamiento, mientras que otras técnicas, como la ingeniería inversa, que tiene como objetivo analizar y reconstruir el funcionamiento del chip, generalmente dan como resultado la destrucción del chip.

25

También se han desarrollado técnicas de ataque mediante la inyección de fallos. En la inyección de fallos, se puede utilizar una fuente de potencia local, por ejemplo, un láser, para alterar el comportamiento del circuito integrado.

30

De manera similar, se conocen técnicas de ataque que permiten realizar un análisis de canal lateral localizado usando una sonda precisa para medir las emanaciones electromagnéticas desde el interior del circuito integrado.

Estas técnicas o una combinación de ellas pueden usarse para extraer secretos almacenados dentro de un chip de circuito integrado.

35

Por lo general, no es deseable un análisis del chip del circuito integrado. Si es posible, se debe evitar el análisis de hardware en vivo, particularmente en el caso de circuitos seguros tales como un microprocesador que incluye una función de monedero electrónico o similares. En la práctica, ya existen varios métodos para dificultar este análisis.

40

Los ataques físicos de todo o parte del chip pueden evitarse mediante los denominados blindajes activos o pasivos.

Un blindaje pasivo comprende planos o pistas metálicas conectadas a un circuito configurado para realizar mediciones de integridad analógicas con el fin de detectar cortes, cortocircuitos o variaciones de carga capacitiva, por ejemplo. En un blindaje activo, puede haber una pluralidad de pistas en donde se inyectan secuencias de bits aleatorias y se comprueba su conformidad desde un extremo de una pista a otro.

45

Los chips de circuito integrado se suministran en una variedad de tipos de paquetes diferentes que permiten la conexión desde el chip de circuito integrado al mundo externo a través de conexiones eléctricas proporcionadas fuera del paquete. Estas conexiones pueden ser, por ejemplo, clavijas, almohadillas o bolas de soldadura.

50

Un tipo conocido de paquete es el de una matriz de rejilla de bolas (BGA). En un BGA, se proporciona una pluralidad de bolas de soldadura en una superficie del paquete para proporcionar conexiones desde el chip de circuito integrado al mundo externo.

55

Por motivos de simplicidad, la superficie del paquete que tiene las bolas de soldadura se denominará en lo sucesivo la superficie inferior del paquete.

Internamente, dentro del paquete BGA, las conexiones se realizan al circuito integrado. Según la forma de conexión, un paquete BGA se considera una BGA de unión por alambre o de chip invertido.

60

La presente solicitud está dirigida a paquetes BGA de unión por alambre. Como puede verse en la sección transversal ilustrativa de la Figura 1, en un paquete BGA 1 de unión por alambre, el circuito integrado 2 está montado sobre un sustrato 8.

65

El circuito integrado se proporciona en una zona de aterrizaje 22 que es un área en una superficie del circuito integrado. La región del sustrato definida por el contorno de la zona de aplicación puede denominarse región de la

zona de aplicación. La región de la zona de aplicación es normalmente, pero no siempre, una región de la zona de aplicación del sustrato. La zona de aplicación puede tener una almohadilla 12 de base metálica, en donde se puede montar el circuito integrado usando un adhesivo. Esta almohadilla de base metálica puede formar parte de un plano de tierra o puede haber una capa separada que proporcione un plano de tierra en la región de la zona de aplicación.

Las conexiones 10 de bola de soldadura se proporcionan en la superficie inferior del paquete para hacer conexiones externas desde el paquete. Las uniones 4 por alambre conectan el circuito integrado a las almohadillas 16 en la superficie superior del sustrato. Las almohadillas 16 están dispuestas en una región periférica del sustrato que rodea la región de la zona de aplicación. Las almohadillas, a su vez, se conectan mediante pistas e interconectan 15 las pistas de la parte inferior que, a su vez, se conectan a las almohadillas con las bolas de soldadura individuales. Como puede verse en la Figura 2, las bolas de soldadura que proporcionan conexiones de señal (como ocurre con las pistas, interconexiones y almohadillas correspondientes) se colocan preferiblemente en la región periférica 28 que rodea la región 22 de la zona de aplicación del sustrato donde se coloca la matriz.

Para facilitar conexiones más complejas y densas, el sustrato puede tener una pluralidad de capas 18 (mostradas como líneas discontinuas) que proporcionan pistas para facilitar las conexiones entre las uniones por alambre en la superficie superior y las bolas de soldadura subyacentes.

Convencionalmente, el circuito integrado está provisto de una carcasa moldeada 6 de plástico para proporcionar protección mecánica. Para ayudar con la transferencia de calor desde el circuito integrado, se pueden proporcionar vías térmicas 14 para transmitir calor a través del sustrato. Estas vías térmicas también pueden proporcionar una conexión eléctrica entre el panel de tierra y la parte inferior del sustrato. Estas vías térmicas se colocan convencionalmente alrededor de la región de la zona de aplicación para garantizar la transferencia de calor desde la almohadilla metálica 12 que se encuentra debajo de la matriz.

En algunas configuraciones, no se proporcionan bolas de soldadura en la región 22 de la zona de aplicación del sustrato subyacente al circuito integrado. En otras configuraciones, se proporcionan bolas de soldadura en la región de la zona de aplicación. Cuando se proporcionan bolas de soldadura en la región de la zona de aplicación, generalmente son conexiones a tierra. Al mismo tiempo, las conexiones de potencia pueden agruparse entre sí extendiéndose desde las esquinas de la región de la zona de aplicación y pueden conectarse comúnmente a un plano de potencia.

La almohadilla de base metálica puede ser un plano de tierra o puede haber un plano de tierra separado debajo de la almohadilla 12 de base metálica. De manera similar, se pueden proporcionar uno o más planos de potencia en otras capas del sustrato. Se apreciará que un plano de tierra o potencia es convencionalmente un área sustancialmente contigua de material conductor en una capa que se extiende para cubrir la región de la zona de aplicación. Los planos de tierra y de potencia son generalmente deseables para mejorar la transferencia de potencia y reducir problemas como el ruido.

El documento US 2003/057550 describe un chip que refleja el preámbulo de la presente reivindicación 1. El documento WO 2016/180977 describe un chip de circuito integrado y un método para proteger el chip de circuito integrado contra alteraciones físicas y/o eléctricas.

La presente solicitud está dirigida a mejorar la seguridad de los chips de circuitos integrados que se empaquetan como BGA de unión por alambre.

Resumen

La presente solicitud está dirigida a la protección contra un ataque que no se ha identificado previamente como posible.

En particular, se ha identificado que los paquetes BGA pueden emplear ataques electromagnéticos localizados de fallos láser dirigidos o de canal lateral, tal como se ha descrito anteriormente, que requieren una estrecha proximidad a la superficie integrada.

En este sentido, para ambas técnicas se prefiere apuntar al sustrato del CI, ya que, combinado con el adelgazamiento, permite el acceso a los transistores del interior sin el efecto de blindaje (ya sea electromagnético o físico) de las capas metálicas del CI utilizadas para enrutar las señales y suministrar potencia.

En el caso de los paquetes con chip invertido, el sustrato está disponible directamente.

En el caso de los paquetes de BGA de unión por alambre, se creía que el sustrato proporcionaba protección. Sin embargo, ahora se comprende que el enfoque convencional de enrutamiento eficiente de las señales dentro del paquete BGA, incluida la agrupación de las conexiones de potencia y tierra, introduce una vulnerabilidad.

En particular, puede dejar grandes áreas del sustrato accesibles incluso cuando se eliminan grandes partes del enrutamiento de los dominios de potencia (tensiones de tierra y de suministro), utilizando una etapa 30 de fresado, como se muestra en la Figura 3. La abertura proporcionada por dicha etapa de fresado a través de la región de la zona de aplicación permite el acceso a grandes secciones del sustrato del circuito integrado.

Por tanto, la presente solicitud proporciona un enfoque contrario a la intuición que niega el conocimiento convencional y busca deliberadamente proporcionar pistas de protección en la región de la zona de aplicación que son necesarias para el funcionamiento adecuado del circuito integrado y cuya interrupción haría que el chip del circuito integrado fuera inoperable. De manera adecuada, estas pistas de protección no son pistas de tierra o potencia, sino que son pistas de señal para proporcionar una señal hacia o desde el circuito integrado.

En consecuencia, la presente solicitud proporciona un chip de circuito integrado empaquetado de matriz de rejilla de bolas de unión por alambre en donde una conexión crítica distinta de la potencia o tierra se encamina a través del sustrato del paquete bajo el circuito integrado.

Más particularmente, según una primera realización, se proporciona un chip según la reivindicación 1, así como un método según la reivindicación 10 para proteger un chip contra un ataque.

Por consiguiente, una primera realización proporciona un chip que comprende un sustrato que tiene una primera superficie y una segunda superficie opuesta a la primera superficie. Un circuito integrado está montado en una zona de aplicación de la primera superficie del sustrato, definiendo la zona de aplicación una región de la zona de aplicación del sustrato. Se proporcionan al menos una pluralidad de contactos en la primera superficie en una región periférica que rodea la región de la zona de aplicación. Una pluralidad de uniones por alambre proporcionan conexiones eléctricas entre el circuito integrado y la pluralidad de contactos. Se proporciona una pluralidad de conexiones de bola de soldadura en la región periférica de la segunda superficie con una pluralidad de pistas de conexión proporcionadas en el sustrato para conectar los contactos eléctricos de la primera superficie con las conexiones de bola de soldadura de la segunda superficie. El chip comprende además al menos una pista de protección que pasa a través de la región de la zona de aplicación del sustrato, en donde el chip está configurado de tal manera que una alteración en la al menos una pista de protección impide el funcionamiento del circuito integrado.

Se puede proporcionar un plano de tierra como una capa de material conductor en la región de la zona de aplicación del sustrato y al menos una pista de protección puede seguir una trayectoria aislada que divide la capa del plano de tierra.

De manera similar, se puede proporcionar un plano de potencia como una capa de material conductor en la región de la zona de aplicación del sustrato y al menos una pista de protección puede seguir una trayectoria aislada que divide la capa del plano de potencia.

Al menos una pista de protección está conectada eléctricamente a al menos una bola de soldadura colocada en la región de la zona de aplicación del sustrato.

Al menos una pista de protección proporciona adecuadamente una conexión eléctrica al circuito integrado que es necesaria para el correcto funcionamiento del circuito integrado.

Al menos una pista de protección es una pista de seguridad. Esta pista de seguridad, a su vez, forma parte de un mecanismo de seguridad que está configurado para detectar una interferencia con la integridad de la pista de seguridad.

Un mecanismo de seguridad de este tipo comprende además, de manera adecuada, un transmisor de señales en el circuito integrado para proporcionar una señal a un primer extremo de la pista de seguridad; y un circuito de detección conectado a un segundo extremo de la pista de seguridad para detectar una alteración en la señal. El circuito de detección puede detectar una interrupción de la pista de seguridad o una modificación de la señal característica en el segundo extremo de la pista, tal como la atenuación o la variación de la impedancia.

De manera adecuada, el mecanismo de seguridad comprende además un circuito de respuesta que responde al circuito de detección para provocar la ejecución de al menos una contramedida. La al menos una contramedida puede comprender restablecer o deshabilitar toda o parte de la funcionalidad del chip. Este restablecimiento puede incluir el borrado del contenido de la memoria del circuito integrado.

En una realización adicional, se proporciona un método para proteger un chip de matriz de rejilla de bolas empaquetado de unión por alambre contra alteraciones. El método comprende adecuadamente las etapas de formar un sustrato que tiene una primera superficie y una segunda superficie opuesta a la primera superficie que tiene una zona de aplicación para un circuito integrado, definiendo la zona de aplicación una región de la zona de aplicación del sustrato, incluyendo la formación del sustrato proporcionar una pluralidad de contactos alrededor de la primera superficie en una región periférica, rodeando la región periférica la región de la zona de aplicación; montar el circuito integrado en la zona de aplicación; conectar una pluralidad de uniones por alambre entre el circuito integrado y la pluralidad de contactos; proporcionar una pluralidad de conexiones de bola de soldadura en una región periférica de la segunda superficie y en donde la etapa de formar el sustrato incluye proporcionar una pluralidad de pistas conductoras en el sustrato para conectar los contactos eléctricos de la primera superficie con las conexiones de bola de soldadura de la segunda superficie.

La formación del sustrato comprende adecuadamente enrutar al menos una pista de protección a través de la región de la zona de aplicación del sustrato, en donde el chip está configurado de tal manera que una alteración en la al menos una pista de protección impide el funcionamiento del circuito integrado.

5 El método puede comprender la etapa de formar una capa de material conductor en la región de la zona de aplicación del sustrato para que actúe como un plano de tierra en donde al menos una pista sigue una trayectoria aislada que divide el plano de tierra.

10 El método puede comprender proporcionar una capa de material conductor en la región de la zona de aplicación del sustrato para que actúe como un plano de potencia y la al menos una pista siga una trayectoria aislada que divide el plano de potencia.

15 El método puede comprender la etapa de formar una trayectoria conductora utilizando al menos una pista conductora entre una de las zonas de aplicación y al menos una bola de soldadura, en donde la al menos una bola de soldadura se coloca en la región de la zona de aplicación del sustrato.

Al menos una pista de protección proporciona una conexión eléctrica al circuito integrado que es necesaria para el correcto funcionamiento posterior del circuito integrado.

20 Al menos una pista de protección es una pista de seguridad que forma parte de un mecanismo de seguridad. El método comprende además proporcionar un circuito de detección en el circuito integrado como parte del mecanismo de seguridad para detectar cualquier interferencia con la pista de seguridad. En ese caso, el circuito de detección está configurado para provocar que un circuito de respuesta habilite las contramedidas. Las contramedidas pueden comprender restablecer o deshabilitar todas o parte de las funcionalidades del chip.

25 **Breve descripción de los dibujos**

Se describirá ahora la presente solicitud con referencia a los dibujos adjuntos, en donde:

30 la Figura 1 es una vista en sección transversal de un paquete BGA de unión por alambre conocido en la técnica;

la Figura 2 es una vista inferior del paquete del tipo mostrado en general en la Figura 1;

35 la Figura 3 es una ilustración de una posible ruta de ataque al sustrato del paquete de la Figura 1;

la Figura 4 es una ilustración que destaca una región en donde se puede proporcionar una medida de protección en un paquete BGA de unión por alambre para reducir la oportunidad de ataque por los medios mostrados en la Figura 3;

40 la Figura 5 es una disposición ilustrativa que ilustra cómo se puede dividir un plano conductor;

la Figura 6 es una disposición ilustrativa adicional que ilustra la división del plano conductor;

45 la Figura 7 es una disposición ilustrativa adicional en donde se proporciona una conexión de bola de soldadura a una señal crítica para reducir la oportunidad de ataque por los medios mostrados en la Figura 3; y

la Figura 8 es un mecanismo de seguridad que puede emplearse con las disposiciones de las Figuras 4 a 7.

Descripción detallada de los dibujos

50 Como se ha descrito anteriormente, se ha identificado una vulnerabilidad al ataque en los paquetes BGA de unión por alambre y la presente solicitud proporciona un método económico para frustrar tales intentos.

55 Como se muestra en la Figura 4, la presente solicitud proporciona una matriz de rejilla de bolas empaquetada de unión por alambre, el chip BGA 40, en donde se emplean medidas de protección en la región 42 del sustrato 8 por debajo de la matriz de circuito integrado. Para evitar la repetición, las características similares a las de la técnica anterior de la Figura 1, emplean los mismos números de referencia.

60 Se apreciará que las medidas de protección se aplican durante la creación del paquete BGA para el paquete y, más particularmente, durante la formación del sustrato, así como en el diseño del chip.

Las medidas de protección se basan en forzar la destrucción física de una o más pistas de protección durante la apertura, fresando o de otra manera el paquete del chip desde el lado de la bola de soldadura para acceder a la matriz.

65 De manera convencional, es posible abrir grandes secciones de la región de la zona de aplicación bajo la matriz, ya que se proporciona una redundancia significativa para las conexiones de potencia y tierra y, por tanto, una gran

parte de la región debajo de la matriz puede eliminarse con un efecto limitado en el funcionamiento del circuito integrado, abriendo por tanto la matriz al ataque.

Más específicamente, los paquetes BGA de unión por alambre normalmente se enrutan para proporcionar las conexiones más eficientes, con bolas de potencia y tierra dispuestas alrededor y dentro de la región de la zona de aplicación del paquete (debajo del chip). Esto también permite la disipación del calor en el gran plano GND. Por lo general, estos planos de potencia y de tierra se vuelven a conectar en varios puntos entre las capas de PCB. Es el área grande y las múltiples conexiones lo que permite abrir grandes áreas por debajo del silicio de la matriz sin ningún efecto sobre la funcionalidad.

La presente solicitud coloca conexiones protectoras (pistas de protección) a través de la región 42 de la zona de aplicación vulnerable. El sustrato comprenderá entonces pistas de conexión para el funcionamiento normal del chip y la conexión de una bola de soldadura a los contactos eléctricos de la primera superficie, así como pistas de protección, que no se utilizan para transmitir una señal desde o hacia el chip desde la bola de soldadura, sino para detectar una intrusión en la zona de aplicación. Para ello, al menos una parte de la pista de protección está situada dentro de la zona de aplicación.

Las pistas de conexión (también conocidas como trazas) resultarían familiares para los expertos en la materia. En general, la longitud de una pista es un orden de magnitud, por ejemplo, al menos diez veces su ancho.

En este contexto, las pistas de protección comienzan adecuadamente en un punto fuera de la región de la zona de aplicación. Se apreciará que las pistas de protección discurren paralelas a las superficies del sustrato. Esto contrasta con las pistas de conexión que discurren sustancialmente perpendiculares a las superficies, como las vías que se emplean convencionalmente para conectar el plano de tierra a las bolas de soldadura que se encuentran debajo. Las pistas de protección pueden proporcionarse en una o más capas del sustrato. En ciertas configuraciones, la pista de protección terminará en un punto fuera de la región de la zona de aplicación, por ejemplo, donde hay una pista de seguridad y se establece una conexión a un detector en el circuito integrado. En otras configuraciones, la pista de protección terminará en un punto dentro de la región de la zona de aplicación y se realizará una conexión eléctrica externa a la segunda mediante una conexión en forma de bola de soldadura (como se describirá más adelante).

La destrucción física o la interferencia con una o más de las pistas de protección pueden deshabilitar la conectividad y, por tanto, la funcionalidad del chip o, donde la pista es una pista de seguridad, permitir la detección y la acción por parte de un mecanismo de seguridad del CI.

El mecanismo de seguridad puede emplear técnicas de protección activa o pasiva (a las que se ha hecho referencia anteriormente y se describen a continuación) que conocerán los expertos en la materia.

Al enrutar una o varias señales críticas directamente por debajo del sustrato de silicio a través de los planos de potencia y/o tierra, se limita el área que se puede abrir sin tener que volver a conectar estas señales y los planos de tierra y potencia.

Se apreciará que cuantas más señales críticas se dirijan a través de la región de la zona de aplicación, más inviable será volver a conectar múltiples señales de corte durante un ataque.

Las señales dirigidas a través de la región de la zona de aplicación se seleccionan para que sean adecuadamente críticas para el funcionamiento del chip.

En un primer enfoque, la naturaleza crítica puede ser directa, es decir, que la señal dirigida a lo largo de una pista conductora en la región de la zona de aplicación sea necesaria para el funcionamiento normal (funcionamiento correcto) del circuito integrado. Como ejemplo, puede ser una conexión de señal de entrada o salida del circuito integrado. Se apreciará que una conexión de señal es distinta de una conexión de potencia, es decir, una tensión de tierra o potencia.

En un segundo enfoque, la naturaleza crítica es indirecta. En este enfoque, la pista conductora es una pista de seguridad (o pista de protección) que forma parte de un mecanismo de seguridad. El mecanismo de seguridad no es necesario para el funcionamiento normal del circuito integrado y, por lo general, no interfiere en el funcionamiento del circuito integrado a menos y hasta que detecte un ataque a la integridad de la pista de seguridad.

Se apreciará que los dos enfoques no son mutuamente excluyentes. Ambos pueden emplearse al mismo tiempo usando diferentes pistas.

Al mismo tiempo, al proporcionar pistas en la misma capa que el plano de tierra o un plano de potencia, los dominios GND y de potencia están adecuadamente menos interconectados, ya que el área contigua de los planos puede segmentarse, creando por tanto más oportunidades para aislar los circuitos críticos/circuitos detectores. Cuando las vías se encuentran en una capa diferente a la de los dominios GND o de potencia, las vías siguen reduciendo el área contigua disponible para el ataque al limitar el espacio disponible para abrirse.

Como se muestra en la Figura 4, una matriz de circuito integrado 2 está posicionada y montada generalmente sobre un sustrato 8. El contorno o perímetro de la matriz define un área, denominada zona de aplicación, que en sintonía define una región de la zona de aplicación del sustrato 8 que se extiende entre las dos superficies y está definida por el área de

la zona de aplicación. Las uniones 4 por alambre conectan la parte superior de la matriz a los contactos 16 en una primera superficie del sustrato. Estos contactos 16 están dispuestos en una región periférica del sustrato que rodea la región 22 de la zona de aplicación. Las conexiones 10 de bola de soldadura se proporcionan en el segundo lado del sustrato.

- 5 Se proporcionan conexiones pasantes, por ejemplo, vía 15, para conectar eléctricamente las conexiones individuales en forma de bola de soldadura a los contactos asociados en la superficie superior.

10 Para impedir el ataque a través de la región de la zona de aplicación de la matriz, al menos una pista conductora se dirige a través de la región de la zona de aplicación 42 del sustrato. Al menos una pista no forma parte de un plano de tierra o potencia. La pista conductora puede ser coplanar con uno u otro plano de tierra o potencia. El chip está configurado de tal manera que una alteración en al menos una pista conductora impide el funcionamiento del circuito.

15 Ahora se describirán varios enfoques potenciales para enrutar rutas críticas a través de la región de la zona de aplicación, que pueden usarse de forma aislada o combinada, con referencia a las Figuras 5 a 7.

20 En la Figura 5, se muestra un plano 52 de tierra que se proporciona en la región de la zona de aplicación del sustrato. Se proporciona una pluralidad de vías térmicas 14 que proporcionan conexiones térmicas y eléctricas al plano de tierra a partir de bolas de soldadura (no mostradas) en la parte inferior del sustrato. Por conveniencia, no se muestran las regiones del avión que se extienden más allá de la región de la zona de aplicación definida por la posición del dado. En la práctica, las conexiones se extenderán de la región de la zona de aplicación a las placas de contacto en donde las uniones por alambre formarán conexiones con la matriz. En general, habrá múltiples conexiones de tierra y potencia diferentes dispuestas en la matriz.

25 Por lo tanto, en un enfoque convencional, se pueden hacer conexiones a tierra a pistas conductoras a lo largo de los lados exteriores de la región de la zona de aplicación con conexiones de potencia en las regiones adyacentes y exteriores a las esquinas de la región de la zona de aplicación.

30 Una pista conductora 56 que está aislada del plano de tierra, pero es coplanar con el mismo, sigue una trayectoria aislada a través del plano de tierra. Esta trayectoria aislada separa el plano de tierra en dos áreas contiguas separadas 54a y 54b. La pista conductora está conectada a través de una almohadilla de contacto y una unión por alambre en un lado. En un primer enfoque, la pista conductora se emplea como parte de un blindaje activo o pasivo y se conecta mediante una segunda almohadilla de contacto y una conexión por cable al circuito integrado y forma parte de un circuito de detección que está configurado para monitorizar cualquier alteración en la pista de protección.

35 En un segundo enfoque, la pista conductora proporciona una conexión a una señal requerida (una conexión crítica) en el circuito integrado y el segundo extremo de la pista conductora se conecta por medio de una vía a una conexión de bola de soldadura en la parte inferior del sustrato. De este modo, una conexión de señal crítica se enruta a través de la región de la zona de aplicación cuya interrupción impide el correcto funcionamiento del circuito integrado.

40 Al mismo tiempo, se apreciará que la separación del plano de base en dos áreas separadas del plano de base 54a y 54b nuevamente limita el alcance de la eliminación del material para acceder al sustrato de la matriz.

45 Se apreciará que el número de pistas conductoras puede aumentarse para aumentar la complejidad y la necesidad de eludir y restablecer las conexiones. Por lo tanto, en la Figura 6, el plano de tierra 62 está dividido en cuatro áreas contiguas separadas 64a, 64b, 64c, 64d por dos pistas conductoras separadas 66, 67, cada una de las cuales puede ser una u otra de una señal crítica para el funcionamiento del circuito o estar conectadas a un circuito de detección. Se apreciará que el enfoque no está restringido a dos pistas conductoras.

50 Aunque se hace referencia a las Figuras 5 y 6 en el contexto de un plano de tierra, se apreciará que también se puede aplicar a un plano de potencia. En el caso de un plano eléctrico, es probable que las vías térmicas estén aisladas del plano, ya que las vías térmicas son conexiones convencionales a tierra.

55 Un enfoque adicional para proteger la región vulnerable se muestra en la Figura 7, en donde se realiza una conexión 74 de unión por alambre a una almohadilla conductora 70 en la superficie superior del sustrato. Como es convencional, la almohadilla conductora 70 está ubicada en la región periférica que rodea la región de la zona de aplicación de la matriz. La almohadilla conductora es para una conexión de señal en lugar de una conexión a tierra o de potencia al circuito integrado.

60 La almohadilla conductora está conectada por medio de una pista conductora 72 a la región de la zona de aplicación de la matriz, donde una vía 78 proporciona una conexión con la parte inferior del sustrato y donde, a su vez, se realiza una conexión eléctrica a una bola 80 de soldadura. La bola 80 de soldadura se proporciona en la región de la zona de aplicación del sustrato directamente debajo de la matriz. Se apreciará que la pista conductora puede estar posicionada en una capa coplanaria con un plano de tierra, un plano de potencia o estar en una capa intermedia. Del mismo modo, la trayectoria conductora entre la almohadilla de contacto y la bola de soldadura puede incluir vías o pistas adicionales en diferentes capas del sustrato.

65

Al colocar una o más conexiones en forma de bola de soldadura centralmente debajo de la matriz para recibir señales críticas distintas de las conexiones de potencia o de tierra, la vulnerabilidad del chip a los ataques a través de la región vulnerable identificada se reduce significativamente. Se apreciará que este enfoque es totalmente contrario a la intuición del diseño de paquetes BGA de unión por alambre, donde el enfoque consiste en tener todas las conexiones de señal dispuestas alrededor de la región periférica.

Se apreciará que la técnica de la Figura 7 puede combinarse fácilmente con la de las Figuras 5 y 6.

La naturaleza del lugar donde la pista conductora es una pista de seguridad se describirá ahora con más detalle. En este enfoque, la naturaleza crítica de la pista conductora es indirecta.

La interferencia con una pista de seguridad en sí misma no interrumpe el funcionamiento normal del circuito integrado.

En cambio, como se muestra en la Figura 7, la pista 86 de seguridad forma parte de un mecanismo 82 de seguridad que reacciona ante una interrupción de la pista de seguridad. El mecanismo de seguridad comprende la pista de seguridad y las conexiones entre la pista de seguridad y el circuito integrado 2 y el sistema 87, 88, 89 de circuitos dentro del circuito integrado que monitoriza un ataque a la integridad de la pista de seguridad. El mecanismo 82 de seguridad generalmente no interfiere en el funcionamiento del circuito integrado 2 a menos y hasta que detecte un ataque a la integridad de la pista 86 de seguridad.

En la Figura 8, el mecanismo 82 de seguridad emplea un transmisor 87 para dirigir una señal a lo largo de la pista 86 de seguridad. Esta señal puede ser una tensión, una corriente o una señal dinámica, tal como un reloj o un flujo digital de bits. Del mismo modo, puede ser una tensión o corriente CC o CA. Un circuito 88 de detección monitoriza cualquier cambio en la señal en el extremo opuesto de la pista de seguridad al transmisor. La detección de un cambio en la señal por el circuito de detección daría como resultado contramedidas por parte de un circuito 89 de respuesta que impidan el funcionamiento normal del chip. Las contramedidas pueden comprender restablecer o deshabilitar todas o parte de las funcionalidades del chip. Estas contramedidas pueden incluir deshabilitar el funcionamiento del circuito integrado o borrar el contenido de la memoria del circuito integrado o ambos.

Una pista de seguridad puede considerarse una pista conductora que está conectada eléctricamente, por ejemplo, utilizando una combinación de pistas, vías y uniones por alambre, a al menos dos terminales del circuito integrado. Esto permite una primera conexión en un extremo de la pista de seguridad a un primer terminal y, a su vez, al transmisor del mecanismo de seguridad. La conexión a un segundo terminal se proporciona en el extremo opuesto de la pista de seguridad. El segundo terminal, a su vez, proporciona una conexión al detector del mecanismo de seguridad.

El mecanismo de seguridad puede ser un blindaje pasivo o un blindaje activo. En ambos casos, un transmisor de señales proporciona una señal a un primer extremo de la pista conductora y el circuito de detección se emplea para monitorizar el extremo opuesto de la pista conductora.

En el caso de un blindaje pasivo, el transmisor y el circuito de detección pueden configurarse para permitir la detección del cambio de la impedancia de la pista conductora. Este cambio puede medirse, por ejemplo, como una capacitancia o como una resistencia. Los blindajes pasivos suelen emplear circuitos analógicos para el transmisor y el detector.

En el blindaje activo, se inyectan secuencias de bits (normalmente aleatorias) al inicio de la pista conductora y, posteriormente, el circuito de detección las prueba en el otro extremo para comprobar si la secuencia de bits llega inalterada tras su recorrido por la pista de seguridad.

Se apreciará que hay una variedad de técnicas diferentes disponibles que pueden seleccionarse ventajosamente para implementar el mecanismo de seguridad como un escudo pasivo o activo.

Las palabras comprende/comprendiendo cuando se usan en esta memoria descriptiva son para especificar la presencia de características, números enteros, etapas o componentes establecidos, pero no excluyen la presencia o adición de una o más características, números enteros, etapas, componentes o grupos de los mismos.

REIVINDICACIONES

1. Un chip (40) que comprende

- 5 un sustrato (8) que tiene una primera superficie y una segunda superficie opuesta a la primera superficie;
un circuito integrado (2) montado en una zona (42) de aplicación en la primera superficie del sustrato (8), definiendo la zona (42) de aplicación una región de la zona de aplicación del sustrato (8) rodeada por una región periférica del sustrato (8);
10 una pluralidad de contactos eléctricos (16) proporcionados alrededor de la primera superficie en la región periférica;
una pluralidad de uniones (74) por alambre que proporcionan conexiones eléctricas entre el circuito integrado (2) y la pluralidad de contactos eléctricos (16);
15 una pluralidad de conexiones (80) de bola de soldadura dispuestas en la región periférica de la segunda superficie;
una pluralidad de conexiones (15) proporcionadas en el sustrato (8) para conectar los contactos eléctricos (16) de la primera superficie con las conexiones (80) de bola de soldadura de la segunda superficie;
20 en donde el sustrato (8) comprende al menos una pista conductora (72) dirigida a través de la región (42) de la zona de aplicación del sustrato (8),
en donde la al menos una pista conductora (72) proporciona una conexión eléctrica al circuito integrado (4) que es necesaria para el funcionamiento normal del circuito integrado (2).
caracterizado por que el chip (4) está configurado de tal manera que una alteración en la al menos una pista conductora impide el funcionamiento del circuito integrado (2),
25 en donde la al menos una pista conductora es una pista (86) de seguridad que forma parte de un mecanismo (82) de seguridad, en donde el mecanismo (82) de seguridad está configurado para detectar una interferencia con la integridad de la pista (86) de seguridad y en respuesta a habilitar al menos una contramedida, el mecanismo (82) de seguridad comprende:
30 un transmisor (87) de señales en el circuito integrado (2) para proporcionar una señal a un primer extremo de la pista (86) de seguridad; y
un circuito (88) de detección conectado a un segundo extremo de la pista (86) de seguridad para detectar una alteración de la señal,
35 en donde el mecanismo (82) de seguridad comprende además un circuito (89) de respuesta que responde al circuito (88) de detección para provocar la ejecución de la al menos una contramedida y en donde la al menos una contramedida comprende restablecer o deshabilitar la totalidad o parte de las funcionalidades del chip.
- 40 2. Un chip según la reivindicación 1, en donde un plano (62) de tierra se proporciona como una capa de material conductor en la región (42) de la zona de aplicación del sustrato (8) y en donde la al menos una pista (72) sigue una trayectoria aislada que divide el plano (62) de tierra.
- 45 3. Un chip según la reivindicación 1, en donde un plano de potencia se proporciona como una capa de material conductor en la región (42) de la zona de aplicación del sustrato (8) y la al menos una pista sigue una trayectoria aislada que divide el plano de potencia.
- 50 4. Un chip según la reivindicación 1, en donde la al menos una pista conductora (72) está conectada eléctricamente a al menos una bola (80) de soldadura, en donde la al menos una bola (80) de soldadura está situada en la región (42) de la zona de aplicación del sustrato (8).
- 55 5. Un método para proteger un chip de matriz de rejilla de bolas empaquetado de unión por alambre contra alteraciones, que comprende las etapas de
formar un sustrato que tiene una primera superficie y una segunda superficie opuesta a la primera superficie que tiene una zona de aplicación para un circuito integrado, definiendo la zona de aplicación una región de la zona de aplicación del sustrato, incluyendo la formación del sustrato proporcionar una pluralidad de contactos eléctricos alrededor de la primera superficie en una región periférica, rodeando la región periférica la región de la zona de aplicación;
60 montar el circuito integrado en la zona de aplicación;
conectar una pluralidad de uniones por alambre entre el circuito integrado y la pluralidad de contactos eléctricos;
proporcionar una pluralidad de conexiones de bola de soldadura en una región periférica de la segunda superficie;
65 en donde la etapa de formar el sustrato incluye proporcionar una pluralidad de conexiones en el sustrato para conectar los contactos eléctricos de la primera superficie con las conexiones de bola de soldadura de la segunda superficie;

- 5 en donde formar el sustrato comprende el enrutamiento de al menos una pista conductora a través de la región de la zona de aplicación del sustrato,
en donde la al menos una pista proporciona una conexión eléctrica al circuito integrado que es necesaria para el correcto funcionamiento posterior del circuito integrado,
caracterizado por que el chip está configurado de tal manera que una alteración en la al menos una pista conductora impide el funcionamiento del circuito integrado,
en donde la al menos una pista conductora es una pista de seguridad, comprendiendo además el método
- 10 proporcionar un mecanismo de seguridad que incluye la pista de seguridad, en donde el mecanismo de seguridad está configurado para detectar una interferencia con la integridad de la pista de seguridad y, en respuesta, a habilitar al menos una contramedida,
proporcionar, mediante el mecanismo de seguridad, una señal a un primer extremo de la pista de seguridad; y
- 15 detectar una alteración de la señal en un segundo extremo de la pista de seguridad y, en respuesta a la detección de una alteración, provocar la ejecución al menos una contramedida y en donde la al menos una contramedida comprende restablecer o deshabilitar la totalidad o parte de las funciones del chip.
- 20 6. Un método según la reivindicación 5, en donde el método comprende la etapa de formar una capa de material conductor en la región de la zona de aplicación del sustrato para que actúe como un plano de tierra en donde la al menos una pista sigue una trayectoria aislada que divide el plano de tierra.
- 25 7. Un método según la reivindicación 6, que comprende además proporcionar una capa de material conductor en la región de la zona de aplicación del sustrato para que actúe como un plano de potencia y la al menos una pista siga una trayectoria aislada que divide el plano de potencia.
- 30 8. Un método según la reivindicación 6, que comprende además la etapa de formar una trayectoria conductora utilizando la al menos una pista conductora entre uno de los contactos de la primera superficie y la al menos una bola de soldadura, en donde la al menos una bola de soldadura se coloca en la región de la zona de aplicación del sustrato.

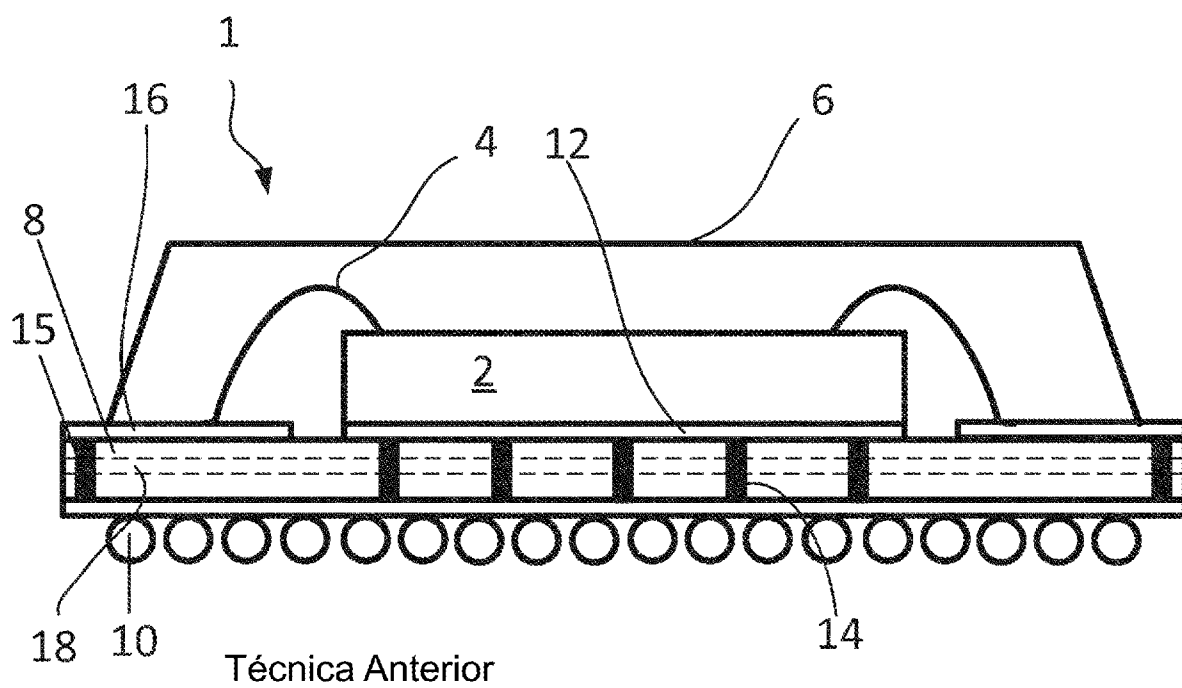
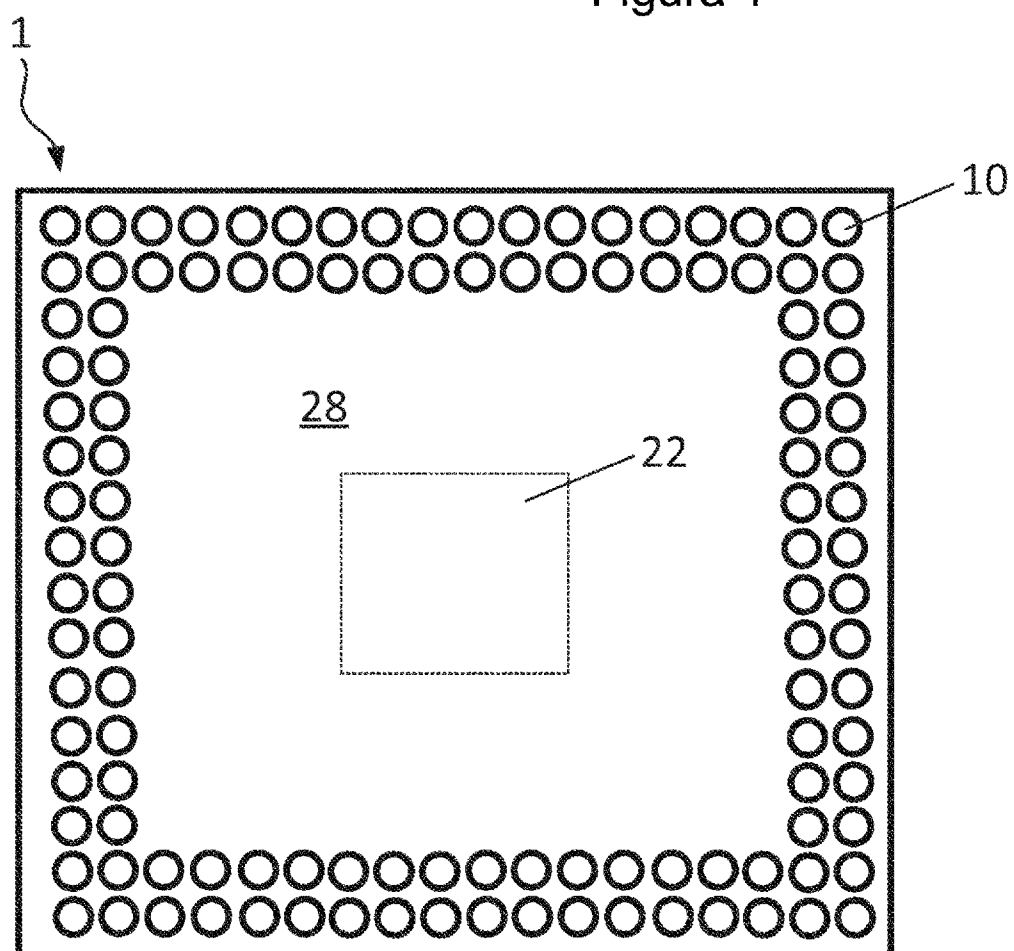


Figura 1



Técnica Anterior

Figura 2

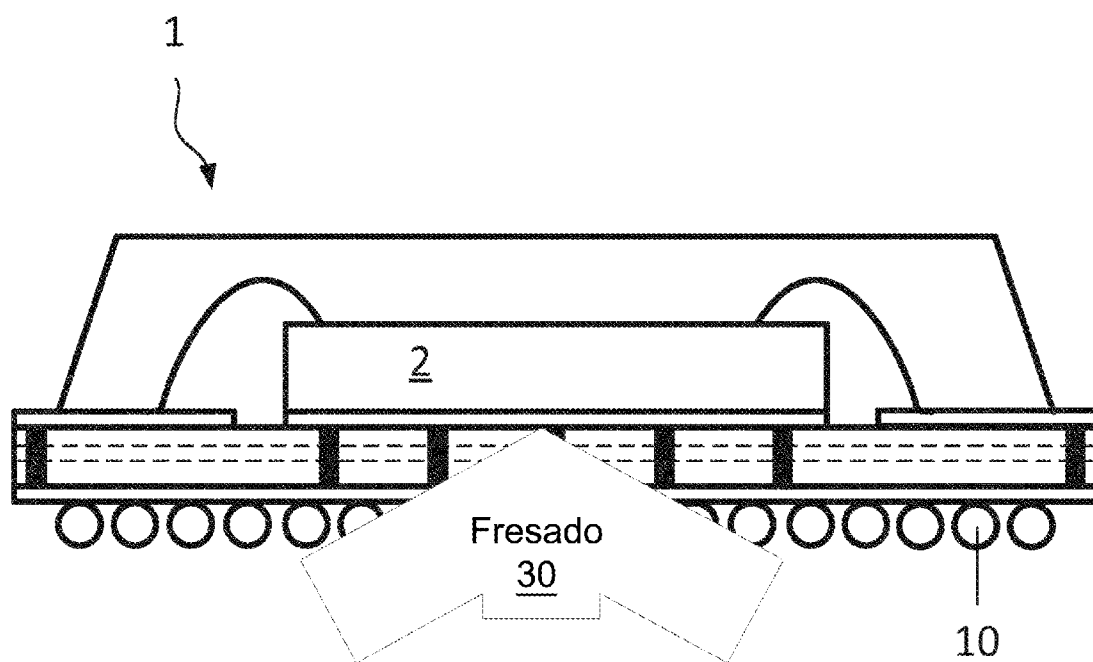


Figura 3

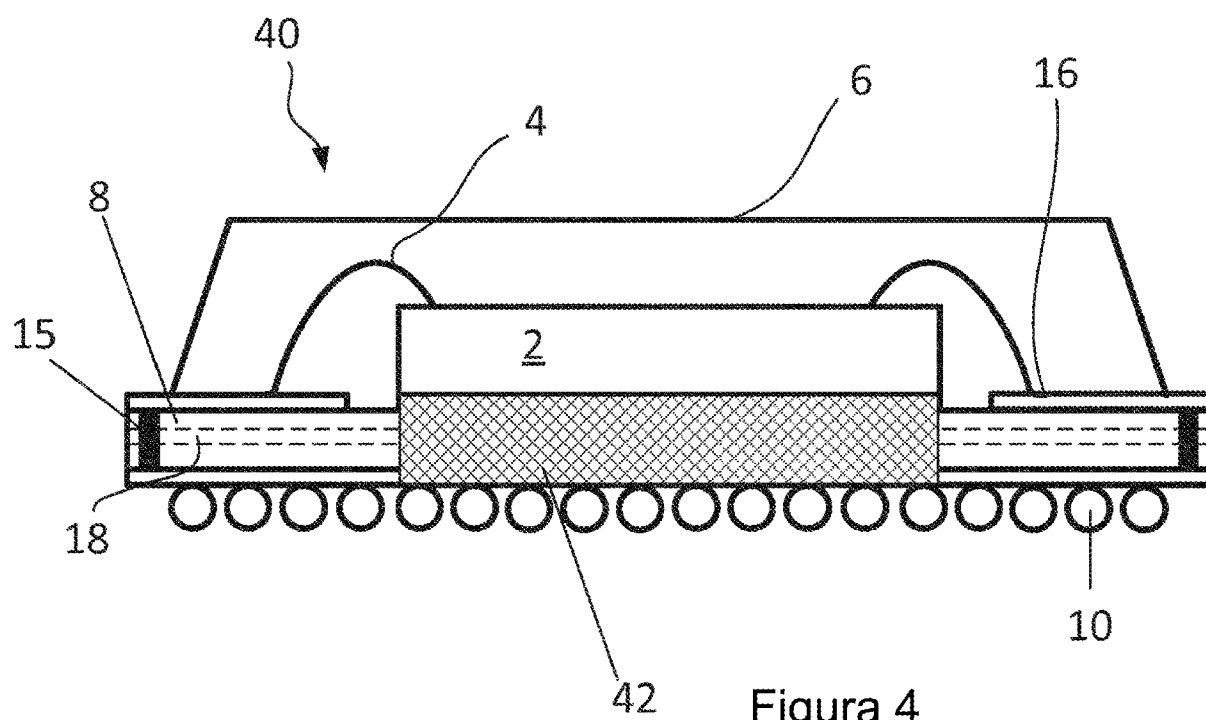


Figura 4

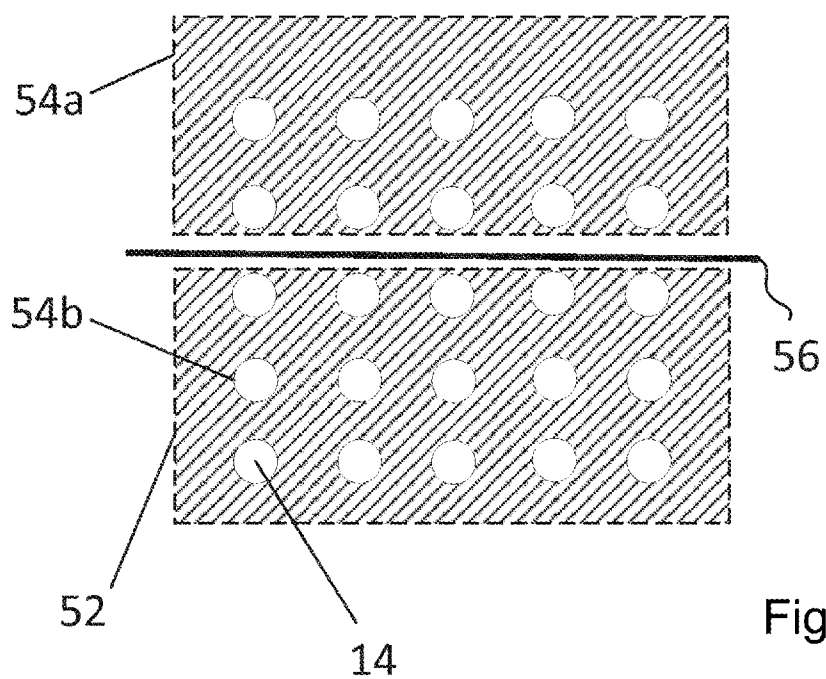


Figura 5

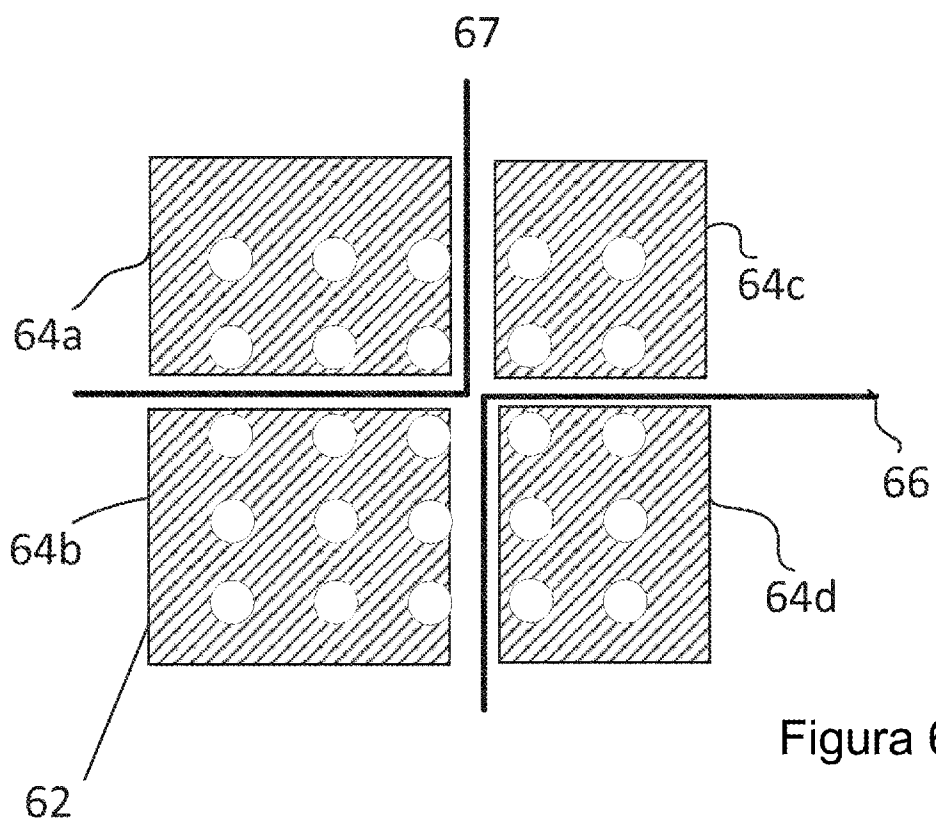


Figura 6

