(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 270 623**

(51) Int. Cl.:
G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **99957280 .3**
(86) Fecha de presentación : **04.11.1999**
(87) Número de publicación de la solicitud: **1053518**
(87) Fecha de publicación de la solicitud: **22.11.2000**

(54) Título: **Circuito de protección para un circuito integrado.**

(30) Prioridad: **05.11.1998 EP 98120986**
15.04.1999 DE 199 17 080

(45) Fecha de publicación de la mención BOPI:
01.04.2007

(45) Fecha de la publicación del folleto de la patente:
01.04.2007

(73) Titular/es: **Infineon Technologies AG.**
St.-Martin-Strasse 53
81669 München, DE
SIEMENS AKTIENGESELLSCHAFT

(72) Inventor/es: **Otterstedt, Jan;**
Richter, Michael;
Smola, Michael y
Eisele, Martin

(74) Agente: **Carvajal y Urquijo, Isabel**

DESCRIPCIÓN

Circuito de protección para un circuito integrado.

Determinadas formas de circuitos electrónicos, especialmente circuitos electrónicos para el empleo en tarjetas de chips, requieren una alta cota de secreto de las informaciones del circuito o de datos internos del chip. Estas informaciones relevantes para la seguridad deben protegerse tanto frente al análisis extraño como también frente a la manipulación.

Para conseguir esta protección, se han seguido diferentes caminos. Por ejemplo, los circuitos integrados han sido provistos con una envoltura metálica, por ejemplo de plata o de titanio, con lo que se puede impedir una lectura del circuito integrado por medio de rayos X. Además, ha dado buen resultado disponer en el plano más superior de circuito de un circuito integrado una banda de conductores como línea de placa de protección y supervisar sus propiedades físicas, como su resistencia, su capacidad, etc. En el caso de determinación de una modificación, por ejemplo a través de un cortocircuito, puesta a tierra o separación en una observación o manipulación no deseadas, se activa entonces una señal de alarma. Un circuito de protección de este tipo se puede deducir a partir de la patente de los Estados Unidos US 5.389.738. No obstante, se ha revelado que estos tipos de circuito de protección son insuficientes, puesto que las propiedades físicas esperadas pueden ser simuladas a través de medidas externas adecuadas y de esta manera no se puede establecer a través del circuito de protección un acceso exterior a través de observación o manipulación y, por lo tanto, no se pueden tomar contramedidas adecuadas.

En el documento WO 96/00953 se describe un procesador criptográfico, en el que las conexiones de salida de un primer enganche están conectadas, a través de líneas dispuestas de acuerdo con un patrón determinado, con conexiones de entrada de otro enganche. Las conexiones de salida del primer enganche son activadas desde un generador de números aleatorios. Cuando los niveles lógicos recibidos son diferentes de los niveles lógicos originales, se supone que se ha llevado a cabo un ataque a la unidad de procesador. Las bandas de conductores se cruzan en regiones previstas para ello.

En el lugar de la literatura Mori y col.: "Superdistribution: The Concept and the Architecture", Transactions of the Institute of Electronics, Information and Communication Engineers of Japan, Vol. E73, Nº 7, Julio de 1990 (1990-07), páginas 1133 - 1146 se describe un sistema para la distribución de software. Un módulo protegido en este sistema puede contener circuitos de protección en varios planos del circuito por debajo y/o por encima de un circuito integrado. La distancia entre las bandas de conductores está configurada tan suficientemente reducida que no es posible una penetración en el caso de un ataque.

En el documento US-A-4 593 384 se describe un circuito de protección, en el que las bandas de conductores se extiende sobre varios planos del circuito, con el fin de impedir un ataque no autorizado.

La invención tiene el cometido de indicar un circuito de protección para circuitos integrados, que proporciona una protección mayor frente a observación o manipulación no deseadas.

Este cometido se soluciona a través de un circuito de protección para circuitos integrados con las características indicadas en la reivindicación 1. Los desarrollos ventajosos de la invención son objeto de las reivindicaciones dependientes.

El circuito de protección de acuerdo con la invención está dispuesto en al menos un plano del circuito por encima o también por debajo del circuito integrado. En este caso, este circuito de protección muestra una o varias bandas de conductores, que son impulsadas con señales que se modifican con el tiempo o también con señales diferentes. Estas señales son transmitidas a través de las bandas de conductores y a continuación son investigadas por el o los detectores, comparando en cada caso la señal resida a investigar con una señal de referencia, es decir, la señal esperada. Si uno o varios de los detectores establecen una desviación significativa, entonces éstos emiten una señal de alarma, que transfiere al circuito integrado a un modo de seguridad. En este modo, se puede borrar entonces el contenido de las células de la memoria, de manera que los programas de control y los datos memorizados no se pueden leer e interpretar.

Por medio de la utilización de varias señales diferentes, que son conducidas sobre varias bandas de conductores y a continuación son analizadas a través de los diferentes detectores, es casi imposible alimentar las señales que disparan la alarma de la manera correcta desde el exterior durante un intento de lectura o manipulación y simular ante los detectores la presencia de estas señales. Por ejemplo, si se erosiona el circuito integrado en la superficie de forma mecánica desde arriba, de manera que debe posibilitarse una visión de los planos de circuito subyacentes del circuito integrado, entonces se ven afectadas en primer lugar las bandas de conductores superpuestas del circuito de protección, lo que conduce a una modificación o bien a una interrupción de la transmisión de las señales, que es determinada a través de uno o también de varios detectores. Lo mismo se aplica también de una manera correspondiente cuando se toman bandas de conductores individuales con agujas de miniatura, con lo que se producen modificaciones, por ejemplo, en la forma de la señal, en la atenuación de la señal o similares. Todas estas modificaciones provocan ahora regularmente una detección de error de diferentes detectores.

Por lo tanto, no sólo debe simularse una única señal, sino una pluralidad de señales diferentes. Precisamente en lo que se refiere a las particularidades espaciales muy limitadas de un circuito integrado es casi imposible alimentar esta pluralidad de señales simuladas de una manera específica a los diferentes detectores. Por lo tanto, se proporciona una protección casi completa del circuito integrado a través del circuito de protección que se coloca encima.

De una manera preferida, el circuito integrado está rodeado en forma de sándwich por medio de un circuito de protección por debajo del circuito integrado, de manera que se excluye una observación o manipulación a través del circuito de protección tanto desde arriba como también desde abajo.

Ha dado buen resultado configurar los detectores de tal forma que se investiga su integridad durante la evaluación de las señales transmitidas, lo que se puede llevar a cabo especialmente a través de una comparación cruzada de las sumas, a través de una comprobación de la paridad o a través de otras comparaciones de la signatura. A través de esta comparación de la integridad entre la señal transmitida y el valor

de la integridad de la señal esperada, llamada también señal de referencia, es posible impedir una manipulación del circuito de protección, en la que, por decirlo así, el detector es cortocircuitado, en el que se da una y la misma señal tanto como señal de referencia como también como señal transmitida al detector con una simple comparación de la identidad para la determinación de un comportamiento erróneo.

Las diferentes señales, que son alimentadas a las diferentes bandas de conductores, se pueden realizar a través de un generador de señales común, o también a través de una pluralidad de generadores de señales individuales. De una manera preferida, el o los generadores están en conexión con los detectores, en el sentido de que el detector respectivo recibe desde el generador asociado al mismo una información sobre el modo y manera de la señal previsible, la señal de referencia. De esta manera es posible que los generadores modifiquen sus señales emitidas de una manera dinámica y comuniquen estas modificaciones a los detectores, lo que dificulta adicionalmente la simulación de las señales en el caso de un ataque, puesto que ahora se tiene en cuenta el desarrollo temporal de las señales.

Se ha revelado que es especialmente ventajoso que las bandas de conductores se extiendan sobre varios planos de circuito, con lo que es posible una cobertura esencialmente mejorada de l circuito integrado a proteger, como también la visión en la estructura del circuito de protección sobre varios planos del circuito y, por lo tanto, se dificulta en una medida esencial una visión en el modo y manera de la generación, de la conducción de la señal y de la detección de las diferentes señales y de esta manera no está disponible para una simulación desde el exterior. Por lo tanto, cada modificación del circuito de protección a través de una intervención desde el exterior conduce a una detección del comportamiento erróneo, puesto que es extraordinariamente difícil o bien casi se excluye una simulación a través de la estructura tridimensional extraordinariamente difícil de la configuración de la banda de conductores o bien su conducción. Por lo tanto, se muestra claramente que un plano de circuito del circuito de protección protege al otro plano de circuito del circuito de protección frente a un análisis. Por lo tanto, se consigue una protección extraordinariamente amplia y segura para el circuito integrado.

De acuerdo con una forma de realización preferida del circuito de protección, las bandas de conductores del circuito de protección están configuradas de tal forma que cubre en gran medida, de una manera idean en toda la superficie, el circuito integrado a proteger, de tal manera que en una visión a fondo a través del circuito de protección sobre el circuito integrado no existe ya ninguna posibilidad de acceder directamente al circuito de protección por ejemplo a través de taladros o similares, es decir, sin lesionar la banda de conductores. Esta cobertura amplia o completa se posibilita precisamente a través de una configuración de la banda de conductores sobre varios planos del circuito o en varios planos del circuito de una manera especial por una vía sencilla y segura, puesto que las bandas de conductores se pueden disponer en un plano a distancia suficiente entre sí y de esta manera se impide una diafonía y la zona entre las bandas de conductores se puede cubrir precisamente a través de bandas de conductores en el otro plano de circuito del circuito de protección, de manera que se posibilita una cobertura completa del circuito integrado o bien de las partes esenciales de este circuito integrado.

Si se intenta ahora acceder, por ejemplo por medio de un taladro, al circuito integrado, entonces esto conduce a una lesión de una de las bandas de conductores, lo que conduce a una señal modificada. Si se configura la banda de conductores con una anchura muy reducida de la banda de conductores, que corresponde a un taladro de este tipo o menor, entonces cada taladro de este tipo conduce a una interrupción de la banda de conductores y, por lo tanto, a una señal errónea muy segura de detectar. También es posible que un taladro de este tipo conduzca a un cortocircuito entre diferentes bandas de conductores, que se reconoce como irrupción total de la señal con mucha seguridad como señal errónea a través de los detectores correspondientes. En este caso, la anchura de la banda de conductores se selecciona de una manera preferida de tal forma que corresponde a la anchura mínima de la banda de conductores en la tecnología de chips utilizada determinada. A través de estas configuraciones especiales de las bandas de conductores, por una parte, como bandas de conductores muy estrechas y, por otra parte, en el sentido de que se extienden así como cubren una superficie lo más grande posible de los diferentes planos del circuito, se proporciona una medida excelente de acción de protección contra un ataque mecánico en el circuito de protección. Un ataque de este tipo se puede proporcionar a través de taladros o a través de cepillado.

De acuerdo con una forma de realización preferida de la invención, el o los detectores del circuito de protección están dispuestos en un plano del circuito por debajo del plano más alto del circuito con bandas de conductores del circuito de protección y están protegidos a través de estas bandas de conductores contra un ataque no deseado. A través de esta estructura sistemática se proporciona una protección en cascada a través de las bandas de conductores de los circuitos de protección para los detectores del circuito de protección y a través de la banda de conductores con detectores para el circuito integrado.

A través de esta disposición se impide una observación o manipulación del o de los detectores en virtud de la protección a través de las líneas superpuestas, lo que excluye otra posibilidad de ataque, en la que se pueden alimentar señales a los detectores directamente sin pasar a través de las bandas de conductores.

De una manera correspondiente, se ha revelado que es ventajoso disponer el o los generadores en un plano del circuito, que están protegidos a través de líneas superpuestas del circuito de protección. Por lo tanto, una disposición de este tipo de los detectores o bien de los generadores del circuito de protección se ha revelado como un medio esencial para elevar el efecto de protección del circuito de protección contra acceso no autorizado.

Si se generan las diferentes señales de una manera totalmente independiente entre sí, por ejemplo por generadores independientes, entonces se asegura que estas señales sean esencialmente diferentes en su curva de la señal, puesto que no dependen sistemáticamente unas de otras y de esta manera solamente se pueden simular con un gasto extremo y con dificultades extremas. Esto tanto más en la medida en que la pluralidad de señales diferentes deben ser introducidas dirigidas

al objetivo en las bandas de conductores correctas o bien en los detectores correctos, lo que es casi imposible en las dimensiones espaciales extraordinariamente reducidas del circuito integrado con el circuito de protección. Por lo tanto, un circuito de protección de este tipo se ha revelado como especialmente exitoso en la protección de un circuito integrado.

Se pueden asociar a una banda de conductores varios detectores, que toman la señal sobre una de las bandas de conductores en una posición específica para el detector respectivo y la supervisan. Por lo tanto, en este tipo de configuración, se divide la banda de conductores en varias secciones de la banda de conductores, que son supervisadas en cada caso a través de detectores asociados a las mismas. De este modo, estas secciones de bandas de conductores asumen la función de una banda de conductores supervisada. Pero, además, a través de la supervisión múltiple de toda la banda de conductores con las diferentes secciones de bandas de conductores se asegura que si no se puede percibir una intervención en esta banda de conductores a través de las medidas adecuadas de prevención de la intervención a través de uno de los detectores, entonces los otros o una parte de los otros detectores pueden establecer, sin embargo, en toda la banda de conductores una modificación de la señal supervisada y pueden disparar una alarma. De esta manera, a través de la disposición redundante de los detectores en una banda de conductores se proporciona un efecto de protección incrementado del circuito de protección.

En general, se pretende prever el mayor número posible de líneas de señales y el mayor número posible de generadores de señales o bien de detectores de señales, que dificultan un ataque en forma de reconfiguración simplemente a través de su número- En función del tamaño del circuito integrado, se fijan, sin embargo, límites, puesto que muchas señales individuales representan un gasto de hardware alto, lo que conduce a un encarecimiento significativo del circuito a través de las medidas de seguridad.

En la invención, el método descrito más arriba de la generación de señales de protección está combinado, por lo tanto, con un multiplexor y con un demultiplexor. De esta manera, a través de un procedimiento de acceso múltiple temporal se conectan diversas bandas de conductores del circuito de protección en instantes diferentes con las mismas salidas de los generadores o entradas de los detectores. De este modo, el número de los generadores y detectores es menor que el número de los segmentos de cuadro.

Otra ventaja de esta disposición se puede ver en que se reduce también el número de las líneas de referencia, que alimentan a los detectores con una señal de referencia desde el generador respectivo, lo que conduce a un ahorro considerable de superficie de chip.

El multiplexor y el demultiplexor o bien se pueden controlar de una manera centralizada sincronizada, o su estado depende solamente del número de los ciclos de pulso de reloj precedentes del sistema de pulso de reloj común. Es especialmente ventajosa una activación casual o pseudocasual de los canales del multiplexor. Una activación casual auténtica requiere una sincronización continua del multiplexor y del demultiplexor a través de señales de control especiales. Una activación pseudocasual permite una generación local de señales de control idénticas en cada caso en la proximidad espacial del multiplexor y el demultiplexor.

De acuerdo con una forma de realización especialmente preferida del circuito de protección, en el caso de varios detectores, éstos están conectados en red entre sí. De esta manera se consigue que tan pronto como un detector establece un comportamiento erróneo y, por lo tanto, un ataque no permitido sobre el circuito integrado, el circuito integrado es activado de tal forma que se transfiere a un modo de seguridad amplia. A través de la conexión en red es posible también que los detectores individuales verifiquen la capacidad funcional de los otros detectores o también sólo la presencia de los otros detectores en el marco de una función de reconocimiento o en el marco de una función de vigilancia y de esta manera reconozcan un ataque no autorizado en el circuito de protección o bien en el chip integrado y activen el modo de seguridad correspondiente del circuito integrado.

Se ha revelado que es ventajoso conectar en red, además de los detectores, también los generadores, con lo que se puede reconocer un fallo o una intervención en un generador. Además, ahora a través de la conexión en red de los generadores con los detectores es posible que los generadores transmitan a los detectores asociados a ellos información sobre las señales emitidas por ellos, por ejemplo sobre un desarrollo del tiempo, sobre su nivel, sobre su forma o similar. De esta manera, se puede elevar esencialmente la variabilidad de las diferentes señales y, por lo tanto, los grados de libertad del circuito de protección, lo que dificulta la intervención y, por lo tanto, eleva de una manera esencial la acción de protección del circuito de protección frente a un ataque no anunciado sobre el circuito integrado.

El circuito de protección de acuerdo con la invención muestra, por lo tanto, la idea básica de no disponer ya de forma localmente concentrada los componentes del circuito de protección, sino descentralizarlos, distribuirlos sobre una zona espacial mayor, multiplicarlos y configurarlos de una manera diferenciada. Esto conduce a que la generación y transporte se distribuya sobre las bandas de conductores y la supervisión de las señales se distribuya sobre varias unidades redundantes, lo que conduce a una mayor seguridad contra una observación o manipulación no anunciada del circuito de protección o bien del circuito integrado a proteger.

Los circuitos de protección de acuerdo con la invención para circuitos integrados y sus ventajas se explican en detalle a continuación con la ayuda de ejemplos de realización por medio de los dibujos. En este caso:

La figura 1 muestra una estructura de circuito de un circuito de protección con un generador de señales y un detector de señales por cada banda de conductores.

La figura 2 muestra una estructura de circuito de otro circuito de protección a modo de ejemplo.

La figura 3 muestra una representación en sección a través de un circuito integrado con circuito de protección y

La figura 4 muestra una estructura de circuito de un circuito de protección de acuerdo con la invención con disposiciones de demultiplexor y multiplexor.

En la figura 1 se representa de forma esquemática la estructura de un circuito de protección para un circuito integrado. Muestra tres bandas de conductores 10, 11, 12 separadas unas de las otras y que se extienden en paralelo. Estas bandas de conductores 10, 11,

12 se extienden en forma de meandro y cubren una zona determinada en un plano de circuito del circuito integrado.

Las bandas de conductores 10, 11, 12 están conectadas en cada caso con un generador de señales 20, 21, 22 propio. A través de los generadores de señales 20, 21, 22 se alimentan a las bandas de conductores 10, 11, 12 señales independientes entre sí y, por lo tanto, en principio también diferentes. Las señales alimentadas se extienden a través de las bandas de conductores 10, 11, 12 y son analizadas en el extremo de las bandas de conductores 10, 11, 12 por medio de un detector 30, 31, 32 que está asociado a cada banda de conductores.

En el marco de este análisis, se comparan las diferentes señales recibidas a través de las bandas de conductores 10, 11, 12 con las señales de referencia alimentadas a través de las líneas de comunicación 13, 14, 15 entre los generadores 20, 21, 22 y los detectores 30, 31, 32 asociados a los mismos. Las señales de referencia o bien representan directamente las señales, tal como aparecen a través del paso por las bandas de conductores 10, 11, 12, o proporcionan las informaciones necesarias para determinar a partir de ellas las informaciones necesarias para las señales de referencia.

La evaluación en los detectores 30, 31, 32 se lleva a cabo comparando las señales de referencia con las señales entrantes, obtenidas a través de las bandas de conductores 10, 11, 12. Cuando se establece una diferencia, se genera una señal de alarma como señal de control para el circuito integrado y se conduce a través de la línea de alarma 4, que está asociada a cada detector 30, 31, 32, hasta el circuito integrado.

Con la ayuda de esta señal de alarma se transfiere entonces el circuito integrado a un estado, que se designa como modo de seguridad. En este modo de seguridad no se pueden leer ya, por ejemplo, los contenidos de las células de la memoria, puesto que están totalmente borrados, por ejemplo, inmediatamente después de la transición al modo de seguridad y de este modo se pierden las informaciones contenidas en ellas de una manera definitiva. De este modo, no es posible ya leer o manipular las informaciones importantes del circuito integrado que están contenidas en la memoria del programa y en la memoria de datos, por ejemplo la clave codificada o los números Pin o datos personales del usuario.

A través de la configuración descentralizada múltiple de las bandas de conductores 10, 11, 12, de los generadores de señales 20, 21, 22 y de los detectores 30, 31, 32 solamente se puede simular todavía este circuito de protección de una manera muy difícil a través de la alimentación de señales exteriores, para obtener informaciones más detalladas sobre el circuito integrado a proteger, por ejemplo sobre la base de un proceso de cepillado o de un proceso de perforación o similar.

Debido a la necesidad de no sólo simular la señal sino de simular al mismo tiempo una pluralidad de señales diferentes en lugares diferentes para diferentes detectores, que están dispuestos en una zona espacialmente muy limitada, es casi imposible llevar a cabo un ataque sobre el circuito integrado sin la determinación de una modificación de la señal y, por lo tanto, de un comportamiento erróneo y, por consiguiente, de un ataque sobre el circuito de protección con el circuito integrado a proteger. Si un detector 30 comprobase un comportamiento erróneo de la señal alimentada al mismo de la banda de conductores 10, entonces depositará una señal de alarma, de una manera independiente de los otros detectores 31, 32, a través de la línea de alarma 4 en el circuito integrado y de esta manera disparará el modo de seguridad.

A través de la configuración paralela en forma de meandro de las bandas de conductores 10, 11, 12 se proporciona una estructura cerrada, cubriendo las superficies, de las bandas de conductores, que protege al circuito integrado subyacente o al menos a una zona del mismo frente a un acceso a través de estas bandas de conductores 10, 11, 12. Si alguien tratase de llegar con medios mecánicos al circuito integrado que se encuentra debajo de las bandas de conductores 10, 11, 12, entonces se vería forzado en gran medida a lesionar una de las bandas de conductores 10, 11, 12 o incluso a interrumpirlas totalmente, lo que conduce a una modificación significativa de la señal transmitida a través de esta banda de conductores. Esta modificación significativa es identificada como comportamiento erróneo a través del detector 30, 31, 32 que está asociado a esta banda de conductores y se emite una señal de alarma correspondiente.

Las bandas de conductores 10, 11, 12 están configuradas con una anchura de banda de conductores tan estrecha que cualquier taladro para la superación de los planos de circuito 2, 3 del circuito de protección conduce a una interrupción de una banda de conductores. A tal fin, es necesario seleccionar muy reducida la distancia de las bandas de conductores 10, 11, 12 individuales y disponer la banda de conductores estrechamente en forma de meandro en el o en los planos del circuito. Por lo tanto, se da una interrupción absolutamente segura a través de una observación o manipulación que debe evitarse, siendo interrumpida totalmente la señal sobre esta banda de conductores 10, 11, 12 interrumpida y siendo interpretada como un ataque.

Las señales generadas a través de los generadores 20, 21, 22 son señales especiales, la mayoría de las veces digitales, pero también analógicas, que permiten poner de manifiesto una modificación sobre la vía de transmisión a través de la banda de conductores 10, 11, 12 claramente en una modificación de la señal.

En la figura 2 se representa de forma esquemática una configuración de otro circuito de protección. Aquí se da una única estructura coherente de las bandas de conductores, que muestra un punto de alimentación 9 para una señal, formada a través de un generador de señales 20, en la estructura de la banda de conductores.

En la estructura de bandas de conductores están previstas cuatro posiciones para el acoplamiento de una señal transmitida a través de la estructura de bandas de conductores. Cada una de estas posiciones de acoplamiento está provista con un amplificador 43, 44, 45, 46 para la amplificación de la señal desacoplada. Estas señales amplificadas son alimentadas a continuación a los detectores 33, 34, 35, 36. La estructura de bandas de conductores forma, en función del punto de toma respectivo, la banda de conductores 10a, es decir, la estructura de la banda de conductores entre el punto de alimentación 9 y el punto de toma del amplificador 43 para el detector 33, la banda de conductores 10b entre el punto de alimentación 9 y el punto de toma que se define a través del amplificador 44 para el detector 34, la banda de conductores 10c

entre el punto de alimentación 9 y el punto de toma para el amplificador 45 para el detector 35 y la banda de conductores 10d entre el punto de alimentación 9 y el punto de toma para el amplificador 46 para el detector 36.

Cada uno de los detectores trabaja de una manera independiente de los otros detectores y puede activar a través de su línea de alarma 4 el circuito integrado de tal manera que éste es transferido al modo de seguridad.

El generador 20 está conectado a través de las líneas de conexión 16, 17, 18, 19 con los detectores 33, 34, 35, 36 y transmite a estos detectores las informaciones específicas para las señales de referencia para la supervisión de la banda de conductores 10a, 10b, 10c, 10d. El generador 20 selecciona de una manera controlada por software de forma casual el tipo de la señal alimentada y señaliza a través de las líneas de comunicación 16, 17, 18, 19 correspondientes a los detectores la forma de la señal alimentada. Los detectores 33, 34, 35 evalúan la señal alimentada a ellos por el generador 20 a través de la línea de comunicación 16, 17, 18, 19, comparándola con la señal de la banda de conductores 10a, 10b, 10c, 10d alimentada por los puntos de toma. Si existe una diferencia significativa, es decir, si se constante un comportamiento erróneo, entonces cada detector 33, 34, 35, 36 emitirá una alarma de una manera independiente de los otros a través de su línea de alarma 4 y de esta manera transferirá al circuito integrado al modo de seguridad.

A través de la configuración coherente de solape de la banda de conductores 10a, 10b, 10c, 10d se consigue que una intervención en la banda de conductores del sistema de bandas de conductores conduzca a una modificación no sólo de una banda de conductores 10aa, 10b, 10c, 10d, sino al mismo tiempo a una modificación de la señal sobre varias bandas de conductores 10aa, 10b, 10c, 10d. De esta manera, en el caso de una observación o manipulación no deseada, no solo la señal de un detector, sino de varios, especialmente de todos los detectores 33, 34, 35, 36 de este sistema de bandas de conductores son impulsadas con una señal simulada y correcta. Esta señal debe corresponder en su forma y su tipo y en su desarrollo temporal a la señal de referencia, que es alimentada de una manera directa o indirecta a través de la línea de comunicación 16, 17, 18, 19 desde el generador 20 a los detectores 33, 34, 35, 36. En este caso, está claro que el generador 20 representado está en condiciones de modificar de una manera dinámica, bajo control de software, su señal alimentada en el punto de alimentación 9 y de esta manera excluir en gran medida la observación o manipulación del circuito de protección y, por lo tanto, del circuito integrado protegido a través del circuito de protección.

En la figura 3 se representa la estructura de capas del circuito integrado 1 con el circuito de protección dispuesto encima. En la figura 3 se ha prescindido de la representación de un circuito de protección correspondiente sobre el lado inferior del circuito integrado. Un segundo circuito de protección sobre el otro lado del circuito integrado 1 muestra una estructura correspondiente al circuito de protección representado aquí.

El circuito de protección está dispuesto por encima del circuito integrado 1. Muestra dos planos de circuito 2, 3 superpuestos, que están separados uno del otro por medio de una capa de aislamiento 5 y del circuito integrado 1 a proteger. A través de esta capa de aislamiento se excluye un cortocircuito eléctrico entre las bandas de conductores 10, 11 y el circuito integrado 1.

En el primer plano del circuito 2, las bandas de conductores 10 están configuradas en forma de tiras y están separadas entre sí por medio de zonas de aislamiento 6 en forma de tiras. Las bandas de conductores 10 están dispuestas paralelas entre sí en el primer plano del circuito 2. Por encima del plano del circuito 2 está dispuesto un segundo plano del circuito 3, que muestra las bandas de conductores 11 correspondientes en forma de tiras, dispuestas paralelas entre sí. También estas bandas de conductores 11 están separadas unas de otras a través de zonas de aislamiento 6 y, por lo tanto, están aisladas entre sí. Las bandas de conductores 10 están dispuestas de tal forma que cubren totalmente, en colaboración con las bandas de conductores 11, el circuito integrado a proteger. Esta cobertura total se consigue cuando en la vista al trasluz a través del primero y el segundo plano del circuito 2, está protegido cada punto del circuito integrado a proteger o bien cada punto a proteger del circuito integrado 1 está cubierto o bien por las bandas de conductores 10 o por las bandas de conductores 11 o tanto por las bandas de conductores 10 como también por las bandas de conductores 11.

Si alguien quiere acceder al circuito integrado a proteger 1, entonces debe atravesar en primer lugar el circuito de protección y en este caso debe romper los planos del circuito 2, 3 y lesionar aquí, en virtud de la cobertura total, al menos una de las bandas de conductores 10, 11. Una lesión de este tipo, que puede representar, por ejemplo, una interrupción completa de las bandas de conductores o un cortocircuito entre las bandas de conductores en un plano del circuito 2, 3 o entre los planos del circuito 2, 3 o también puede consistir solamente en una destrucción parcial de las bandas de conductores 10, 11, conduce a una modificación clara de la señal transmitida, que es interpretada, en comparación con la señal de referencia a través del detector correspondiente como señal errónea y, por lo tanto, como ataque sobre el circuito de protección o bien sobre el circuito integrado 1 a proteger, lo que conduce a la deposición de una señal de alarma en el circuito integrado. A través de esta señal de alarma se transfiere entonces el circuito integrado 1 al modo de seguridad.

En el primer plano del circuito 2 se protegen a través del plano del circuito 3 superpuesto con las bandas de conductores 11 dispuestas de forma correspondiente los generadores 20, 21, 22 no representados aquí o bien los detectores 30 a 36 correspondientes no representados aquí. En particular, esta disposición se lleva a cabo de una manera distribuida sobre todo el primer plano del circuito 2, lo que limita claramente las posibilidades de salvar el circuito de protección.

En la figura 4 se muestra un ejemplo de realización de la invención con ocho bandas de conductores 40... 47. Estas ocho bandas de conductores 40... 47 están divididas en dos grupos de cuatro bandas de conductores 40... 43 o bien 44 ... 47 cada uno. A cada uno de los dos grupos está asociado un generador de señales 60 o bien 62 y un detector de señales 61 o bien 63. Las señales de los generadores de señales 60, 62 son alimentadas a los grupos de bandas de conductores 40... 43 o bien 44... 47 a través de desmultiplicadores 50 o bien 52 y las señales transmitidas a través de las bandas de conductores son alimentadas a través de

multiplexores 51 o bien 53 a los detectores de señales 61 o bien 63.

Para poder alimentar a los detectores de señales 61, 62 las señales de referencia necesarias, solamente es necesario en esta configuración de la invención una línea de comunicación 48 o bien 49 por cada grupo de bandas de conductores. Los detectores de señales 61, indican también aquí cuándo la señal recibida a través de los multiplexores 51, 53 no coincide con el esperado.

En el ejemplo de realización representado con dos grupos de bandas de conductores 40... 43 o bien 44 ... 47 se muestran dos posibilidades diferentes de la activación de los demultiplexores 50, 52 y los multiplexores 51, 53. En el grupo de bandas de conductores 40... 43 representad en la parte superior de la figura 4 se activan el demultiplexor 50 y el multiplexor en común desde un generador auténtico de números aleatorios 70 para la selección de una de las bandas de conductores 40... 43. En el grupo de bandas de conductores 44... 47 representado debajo se activan el demultiplexor 52 respectivo y el multiplexor 53 correspondiente desde dos generadores de números pseudo-aleatorios diferentes, pero configurados del mismo tipo, que suministran los mismos números aleatorios en virtud de su estructura del mismo tipo con un pulso de reloj común en los mismos instantes. No obstante, en principio es posible también activar los demultiplexores 50, 652 y los multiplexores 51, 53 a través de una señal de pulso de reloj propiamente dicha, lo que es, en efecto, sencillo desde el punto de vista de la técnica de circuitos, pero es crítico para la seguridad.

En una superficie de chip dada, en virtud de este desarrollo de acuerdo con la invención de un circuito de protección, se puede realizar un buen compromiso entre una cobertura lo más completa posible de la superficie del chip con bandas de conductores lo más estrechas posible y los más adyacentes posible entre sí, y el deseo de un gasto técnico de circuito lo más reducido posible.

REIVINDICACIONES

1. Circuito de protección para un circuito integrado (1), en el que el circuito de protección está dispuesto en al menos un plano del circuito (2, 3) por debajo y/o por encima del circuito integrado (1), con varias bandas de conductores (40 - 47), que son impulsadas con al menos una señal desde al menos un generador de señales (60, 62), con al menos un detector (61, 63), que evalúa las diferentes señales transmitidas a través de las bandas de conductores (40 - 47) individuales para determinar un comportamiento de error y en el caso de que se determine la existencia de un comportamiento de error de este tipo, se puede emitir una señal de control para transferir el circuito integrado (1) a un modo de seguridad, con un demultiplexor (50, 52), en el que está conectado un extremo de las bandas de conductores (40 - 47), con un multiplexor (51, 53), en el que está conectado un extremo de las bandas de conductores (40 - 47) y, por una parte, con un generador de señales de selección (70) controlado de forma aleatoria para la activación del demultiplexor (50) y del multiplexor (51) para la selección de una de varias bandas de conductores o, por otra parte, tanto con un generador de señales de selección (71) controlado de forma aleatoria para la activación del demultiplexor (52) como también con un generador de señales de selección (72) controlado de forma aleatoria y configurado del mismo tipo para la activación del multiplexor (53), en cada caso para la selección de una de las varias bandas de conductores, en el que al menos un generador de señales (60, 62) está acoplado con el demultiplexor (60, 52) y al menos un detector (61, 63) está acoplado con el multiplexor (51, 53).

2. Circuito de protección de acuerdo con la reivindicación 1, **caracterizado** porque el generador de señales de selección (70) es un generador de número aleatorio (70).

3. Circuito de protección de acuerdo con la reivindicación 1, **caracterizado** porque el generador de señales de selección es un generador de números pseudo-aleatorios (71, 72).

4. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado** porque están previstos varios detectores (30,..., 36), que están conectados en red entre sí.

5. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 4, **caracterizado** porque están previstos varios generadores de señales (20, 21, 22), que están conectados en red entre sí.

6. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado** porque las bandas de conductores se extienden sobre varios planos de circuito (2, 3) del circuito de protección.

7. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 6, **caracterizado** porque las bandas de conductores están configuradas de tal forma que el circuito integrado (1) a proteger está cubierto en gran medida o totalmente.

8. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 7, **caracterizado** porque las bandas de conductores están configuradas con una anchura estrecha.

9. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado** porque los detectores están dispuestos en un plano de circuito (2) debajo del plano del circuito (3) con las bandas de conductores (11) y están dispuestos protegidos a través de estas bandas de conductores (11).

10. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 9, **caracterizado** porque el generador de señales de selección (70, 71) está dispuesto en un plano del circuito (2) debajo del plano del circuito (3) con las bandas de conductores y está protegido contra el acceso a través de estas bandas de conductores (11).

11. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado** porque las diferentes señales son generadas de una manera independiente entre sí.

12. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 11, **caracterizado** porque el generador de señales de selección (70, 71) está diseñado para diferentes señales, de tal forma que las señales se modifican de una manera dinámica en el transcurso del tiempo.

13. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 12, **caracterizado** porque el circuito integrado (1) está rodeado en forma de sándwich por medio de varios planos de circuito (2, 3) del circuito integrado.

14. Circuito de protección de acuerdo con una de las reivindicaciones 1 a 13, **caracterizado** porque está prevista una unidad para la determinación del valor de integridad de una señal alimentada al detector y este valor de integridad es evaluado para la determinación de un comportamiento erróneo.

FIG 1

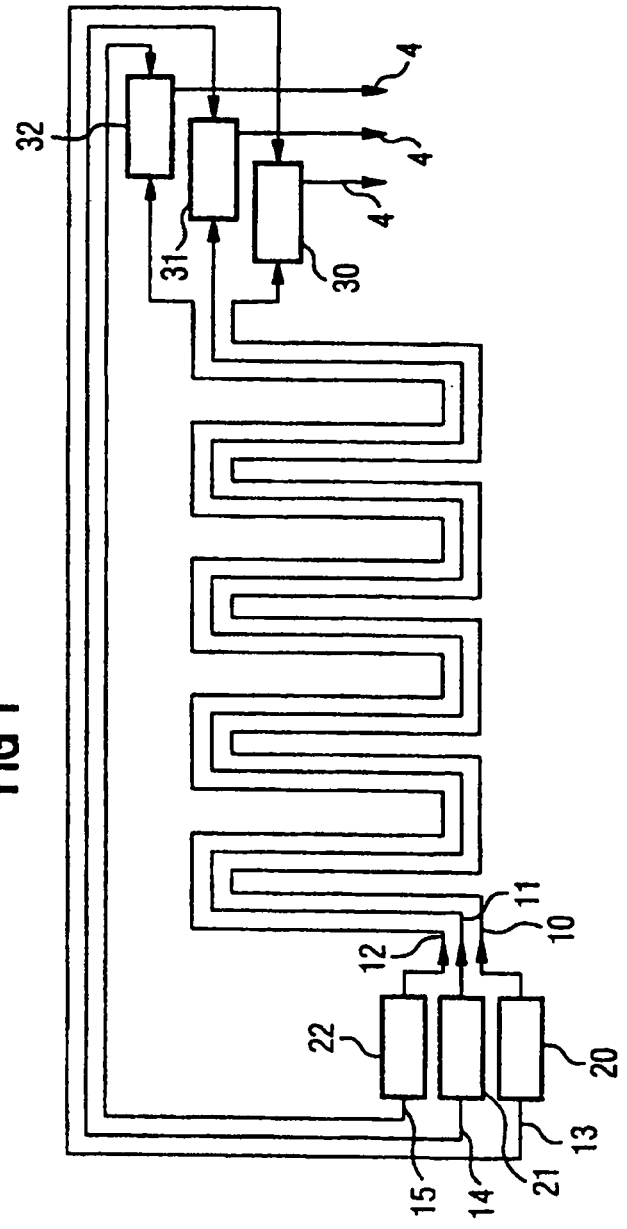

FIG 2

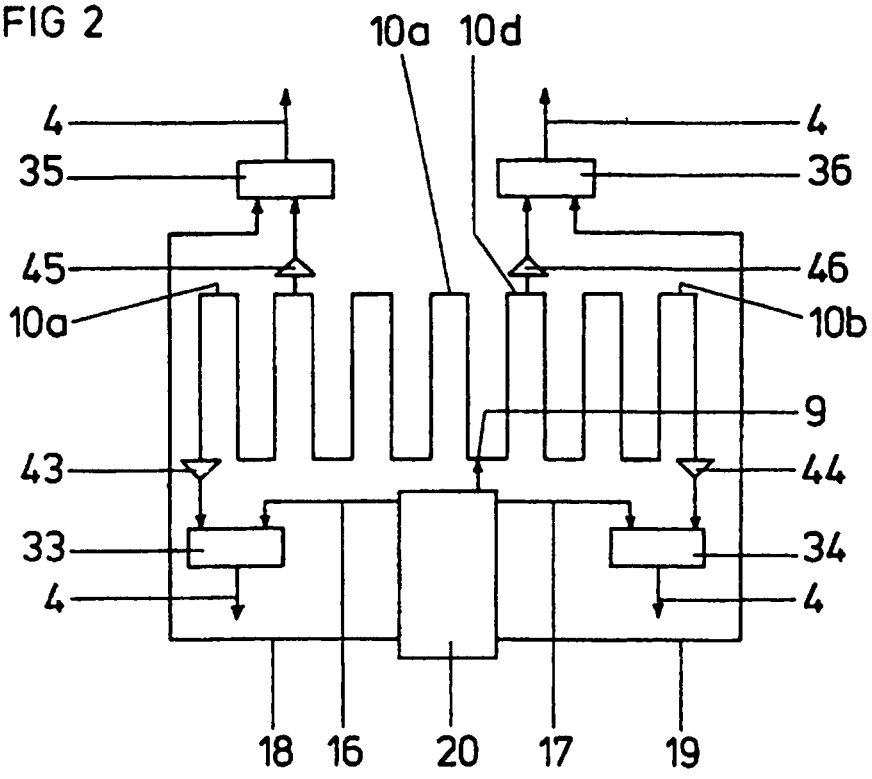
10a
10d
4
4
35
36
45
46
10a
10b
9
43
44
33
34
4
4
18
16
20
17
19

FIG 3

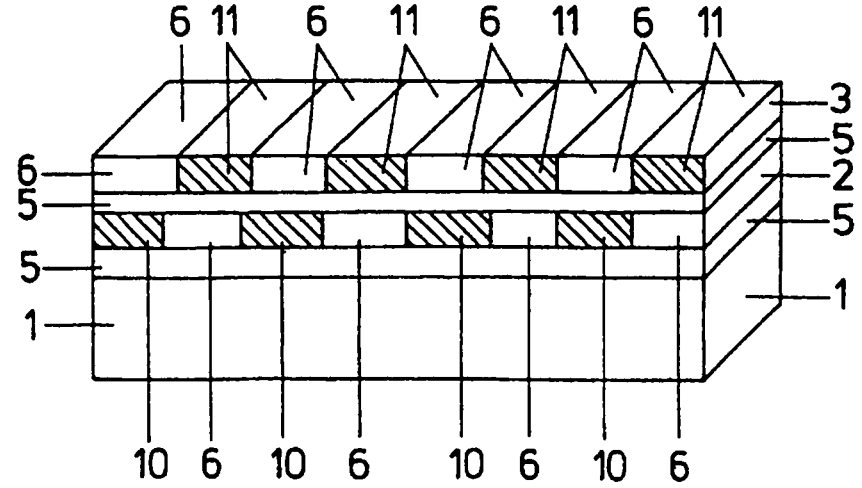
6
11
6
11
6
11
6
11
3
5
2
5
6
5
5
1
1
10
6
10
6
10
6
10
6

Fig. 4