

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 875 465**

51 Int. Cl.:

**G09C 1/00** (2006.01)

**G06F 21/87** (2013.01)

**H01L 23/00** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **22.09.2016 PCT/EP2016/072564**

87 Fecha y número de publicación internacional: **30.03.2017 WO17050910**

96 Fecha de presentación y número de la solicitud europea: **22.09.2016 E 16775585 (9)**

97 Fecha y número de publicación de la concesión europea: **17.03.2021 EP 3353767**

54 Título: **Sistema de detección de intrusiones por reconfiguración**

30 Prioridad:

**22.09.2015 FR 1501959**

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

**10.11.2021**

73 Titular/es:

**THALES (100.0%)  
Tour Carpe Diem, Place des Corolles, Esplanade  
Nord  
92400 Courbevoie, FR**

72 Inventor/es:

**SALIBA, ERIC;  
GRISAL, OLIVIER;  
DUPREZ, ADRIEN y  
MIQUEL, STÉPHANE**

74 Agente/Representante:

**PONTI & PARTNERS, S.L.P.**

ES 2 875 465 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

Sistema de detección de intrusiones por reconfiguración

- 5 **[0001]** La presente invención se refiere a un sistema de detección de intrusiones según el preámbulo de la reivindicación 1.
- [0002]** La presente invención se refiere también a un procedimiento asociado de detección de intrusiones.
- 10 **[0003]** En el ámbito de la seguridad informática, uno de los retos consiste en proteger los equipos por los que pasa la información sensible. Tales equipos comprenden en particular circuitos impresos o circuitos integrados. Un circuito impreso, también llamado tarjeta electrónica, es un soporte que permite mantener y conectar eléctricamente entre sí un conjunto de componentes electrónicos. Un circuito integrado, también llamado chip electrónico, es un conjunto de componentes electrónicos que reproducen una o más funciones electrónicas y que generalmente integran
- 15 varios tipos de componentes electrónicos básicos en un volumen reducido.
- [0004]** Las pistas de un circuito impreso y las conexiones de los componentes electrónicos conectados a tal circuito impreso son susceptibles de sufrir ataques físicos. Tales ataques físicos consisten, en particular, en la aproximación de sondas o en la conexión de electrodos en las pistas del circuito impreso o en las conexiones de los
- 20 componentes conectados al circuito impreso para capturar las señales que pasan por las pistas o las conexiones o para inyectar señales. Los atacantes utilizan las señales capturadas para recopilar datos confidenciales. Las señales inyectadas se utilizan para interrumpir las señales intercambiadas o provocar un mal funcionamiento del equipo.
- [0005]** Es probable que estos ataques similares se lleven a cabo en circuitos integrados.
- 25 **[0006]** Por lo tanto, los sistemas de protección física se utilizan para proteger los circuitos impresos y los circuitos integrados de tales equipos contra las intrusiones. Los sistemas de protección comprenden, por ejemplo, mallas de protección bidimensionales o tridimensionales. Las mallas están formadas en particular por distintos circuitos eléctricos que forman patrones y cuya continuidad, o alteración, se verifica haciendo circular una corriente de control
- 30 y detectando pérdidas de corriente, debidas a una interrupción del circuito, o la modificación de una de las características eléctricas de la corriente, debido a una alteración del circuito. Las mallas están dispuestas, por ejemplo, encima y/o debajo de los componentes del equipo que se va a proteger, tales como las pistas y conexiones de un circuito impreso o las capas de silicio de un circuito integrado. Las mallas incluyen en particular una estructura y patrones elegidos para permitir la detección de intentos de intrusión. Cuando se detecta un intento de intrusión, el
- 35 sistema de protección inicia acciones de reacción que consisten, por ejemplo, en borrar datos sensibles del equipo.
- [0007]** Sin embargo, al ser cada vez más sofisticados los ataques, la estructura y los patrones diseñados para las mallas son cada vez más complejos, lo que aumenta el tiempo y el coste de desarrollo de las mallas.
- 40 **[0008]** Además, es probable que los atacantes eludan la protección proporcionada por tales mallas después de una fase de ingeniería inversa. La ingeniería inversa, conocida igualmente como diseño inverso, es la actividad que consiste en estudiar un objeto para determinar el funcionamiento interno o procedimiento de fabricación.
- [0009]** Después de la ingeniería inversa, el atacante tiene conocimiento de las posiciones y propiedades de los
- 45 diferentes circuitos eléctricos de la malla. Es probable que el atacante puentee algunos de estos circuitos eléctricos y, por lo tanto, los corte para liberar espacio de acceso al equipo protegido, sin que el sistema de protección detecte la intrusión. Se entiende por el término «puentear», la acción de cortocircuitar un circuito eléctrico.
- [0010]** Los documentos US 2013/0055416 A, US 2013/104252 A y US 7 710 286 B ilustran ejemplos de
- 50 dispositivos de detección de intrusiones.
- [0011]** Existe por tanto la necesidad de un sistema que permita, por un lado, responder a ataques sofisticados sin aumentar la complejidad de las mallas de protección y, por tanto, su tiempo y coste de desarrollo, así como su coste de producción; por otro lado, hacer inoperante para un atacante el cortocircuito de uno o varios circuitos
- 55 eléctricos de una malla después de la ingeniería inversa.
- [0012]** A tal efecto, la invención tiene como objetivo un sistema de detección de intrusiones del tipo mencionado anteriormente, en el que el sistema comprende además las características de la parte caracterizadora de la reivindicación 1.
- 60 **[0013]** Según las realizaciones particulares, el sistema de detección de intrusiones comprende una o varias de las características de las reivindicaciones 2 a 11, tomadas de forma aislada o según todas las combinaciones técnicamente posibles.
- 65 **[0014]** La invención se refiere igualmente a un procedimiento de detección de intrusiones según la

reivindicación 12.

**[0015]** Otras características y ventajas de la invención aparecerán con la lectura de la siguiente descripción de las realizaciones de la invención, dada a título de ejemplo únicamente y en referencia a los dibujos que son:

5

- figura 1, una vista esquemática en sección de un ejemplo de un sistema de detección de intrusiones que monta en sección una película de detección formada por una superficie de interconexión, superficies de malla así como un módulo de configuración, un módulo de detección y un módulo de reacción,

- figura 2, una vista superior esquemática de una primera superficie de malla del sistema de la figura 1,

10 - figura 3, una vista superior esquemática de la superficie de interconexión del sistema de la figura 1,

- figura 4, una vista superior esquemática de una segunda superficie de malla del sistema de la figura 1,

- figura 5, una vista superior esquemática de un ejemplo de un patrón de una celda de una superficie de malla de la figura 1,

15 - figura 6, un diagrama de flujo de un ejemplo de un procedimiento de detección de intrusiones que utiliza una configuración dinámica de las interconexiones, y

- figura 7, un diagrama de flujo de otro ejemplo de un procedimiento de detección de intrusos que utiliza una configuración dinámica y una configuración estática de las interconexiones.

20 **[0016]** Un sistema de detección de intrusiones 1 se ilustra en la figura 1.

**[0017]** El sistema 1 está destinado a proteger un equipo a través del cual pasa información sensible. El equipo comprende, por ejemplo, un circuito impreso o un circuito integrado. El equipo es, por ejemplo, un dispositivo de encriptación o un equipo de transmisión a través del cual pasan datos encriptados tales como datos bancarios.

25 **[0018]** El sistema 1 es adecuado para detectar intentos de intrusión que provienen del exterior del sistema 1. Los intentos de intrusión son en particular ataques físicos que consisten en acercarse a sondas o conectar electrodos a un circuito impreso del equipo protegido por el sistema 1.

30 **[0019]** El sistema 1 comprende una película de detección 1A apta para envolver completamente el equipo que se va a proteger o al menos para cubrir la totalidad o parte de los circuitos impresos y circuitos integrados del equipo. La película 1A está limitada a una superficie plana del equipo y, por lo tanto, se extiende solo en dos dimensiones o se extiende sobre al menos dos superficies desplazadas angularmente y, por tanto, forma una superficie tridimensional.

35 **[0020]** La película 1A comprende al menos una superficie de malla 2, comprendiendo cada superficie de malla 2 al menos dos celdas 3. La película 1A comprende además al menos una superficie 4 para interconectar las celdas 3 de cada superficie de malla 2.

40 **[0021]** El sistema 1 comprende también un módulo 6 para configurar las interconexiones de los conectores 24 de la superficie de interconexión 4 a lo largo del tiempo. El sistema 1 comprende también un módulo de detección de intrusiones 8 y un módulo 10 para reaccionar a los intentos de intrusión detectados por el módulo de detección 8.

**[0022]** Opcionalmente, el sistema 1 comprende también un órgano tal como un temporizador configurado para activar el módulo de configuración 6 y/o el módulo de detección 8.

45

**[0023]** En el ejemplo de la figura 1, la película 1A comprende dos superficies de malla 2 y una superficie de interconexión 4.

50 **[0024]** Como se ilustra en las figuras 2 y 4, cada superficie de malla 2 comprende treinta y cinco celdas 3. Las celdas 3 tienen, por ejemplo, una superficie idéntica igual a 54 milímetros cuadrados (mm<sup>2</sup>). Alternativamente, las celdas 3 tienen diferentes tamaños.

55 **[0025]** Las celdas 3 son segmentos continuos de pistas conductoras, cada una de las cuales comprende un patrón geométrico 20 que cubre toda la superficie de la celda 3, como se ilustra en la figura 5. La colocación de extremo a extremo de los patrones 20 a través de las interconexiones de los conectores 24 forman una malla.

60 **[0026]** Cada patrón 20 es una parte de un circuito eléctrico continuo curvilíneo sin cruce y cuya rotura o alteración de una característica eléctrica permite detectar un intento de intrusión en el sistema 1. Los patrones 20 tienen, por ejemplo, formas de bustrofedón tal como se representan en la figura 5 o formas más complejas, por ejemplo, en espiral o laberíntica.

**[0027]** La superficie de interconexión 4 está configurada para interconectar celdas 3 de la misma superficie de malla 2 o celdas 3 de diferentes superficies de malla 2 para formar una malla más o menos compleja.

65 **[0028]** En el ejemplo ilustrado en la figura 3, la superficie de interconexión 4 comprende un componente

programable 23 y una pluralidad de conectores 24.

**[0029]** El componente programable 23 es, por ejemplo, un FPGA (acrónimo de Field-Programmable Gate Array, traducido al español por Red de puertas programables).

5

**[0030]** El componente programable 23 es capaz de activar el módulo de configuración 6, el módulo de detección 8, el módulo de reacción 10 y, opcionalmente, el temporizador.

**[0031]** El componente programable 23 está configurado igualmente para determinar las interconexiones de los conectores 24 en la superficie de interconexión 4 y para interconectar los conectores 24 según las interconexiones determinadas. El componente programable realiza, por ejemplo, una función de evolución de las interconexiones adecuadas para hacer evolucionar con el tiempo las interconexiones de los conectores 24 para cada grupo de celdas 3 conectadas.

**[0032]** Los conectores 24 están, por un lado, conectados a los extremos de los patrones 20 de las celdas 3. Los conectores 24 están, por otro lado, interconectados por el componente programable 23 para conectar en serie celdas 3 de las superficies de malla 2 según una primera configuración, para formar grupos de celdas conectadas. Estos grupos de celdas conectadas en serie se denominan también «equipotenciales». Puede haber varios equipotenciales en paralelo, cada uno correspondiente a un grupo de celdas.

20

**[0033]** Como variante, la superficie de interconexión 4 comprende varios componentes programables 23.

**[0034]** Como variante, la superficie de interconexión 4 comprende un microsistema electromecánico controlado por actuadores. Un microsistema electromecánico, también llamado MEMS (acrónimo en inglés de Microelectromechanical Systems), es un microsistema que comprende uno o varios elementos mecánicos y utiliza electricidad como fuente de energía, con el fin de realizar una función de sensor y/o actuador, con al menos una estructura que presenta unas dimensiones micrométricas.

25

**[0035]** Los patrones 20 de celdas 3 de cada grupo de celdas conectadas forman un circuito eléctrico continuo de patrones. Por ejemplo, las figuras 2 y 4 ilustran diferentes circuitos eléctricos continuos de patrones, estando representadas las celdas 3 de un mismo circuito eléctrico por un mismo tipo de sombreado o líneas de puntos.

30

**[0036]** El módulo de configuración 6 es capaz de configurar las interconexiones de los conectores 24 según la primera configuración de la superficie de interconexión 4.

35

**[0037]** El módulo de configuración 6 es capaz de reconfigurar con el tiempo las interconexiones de los conectores 24 según una nueva configuración de la superficie de interconexión 4. Por tanto, el módulo de configuración 6 puede modificar con el tiempo la configuración actual de la superficie de interconexión 4 para obtener una nueva configuración de la superficie de interconexión 4 y reconfigurar el conjunto de las interconexiones de los conectores 24 según la segunda configuración.

40

**[0038]** El módulo de configuración 6 puede determinar de manera aleatoria cada configuración entre una pluralidad de configuraciones de la superficie de interconexión 4.

**[0039]** Preferiblemente, cada configuración se elige entre una pluralidad de configuraciones probadas y validadas en la fábrica para evitar errores de configuración o configuraciones no óptimas. En este caso, la determinación de cada configuración es pseudoaleatoria, es decir que aunque se conocen las posibles configuraciones, la multiplicidad de configuraciones no permite prever la configuración que elegirá el módulo de configuración 6.

50

**[0040]** El módulo de configuración 6 puede modificar además la configuración de la superficie de interconexión 4 cuando el módulo de detección 8 detecta un intento de intrusión.

**[0041]** En este caso, el módulo de configuración 6 es, por ejemplo, adecuado para modificar la configuración de la superficie de interconexión 4 para aumentar el número de grupos de celdas conectadas en la zona de la superficie de malla 2 donde se ha detectado un intento de intrusión. Tal aumento del número de grupos de celdas y por lo tanto de circuitos eléctricos continuos en una zona se denomina «ajuste de malla» en la zona. El ajuste de la malla en una zona permite hacer aún más complejo el recurso a unas derivaciones para liberar un espacio de acceso en la zona que se va a proteger.

60

**[0042]** Como variante, el módulo de configuración 6 es capaz de aumentar o disminuir el número de celdas de un grupo en una parte de la superficie de interconexión 4 en función de una regla predefinida, de un estado o de un evento.

**[0043]** Como variante y/o adicionalmente, el módulo de configuración 6 se activa en momentos elegidos

65

aleatoriamente, pseudoaleatoriamente o incluso periódicamente por el temporizador del sistema 1, lo que dificulta que un atacante se anticipe a la configuración de la superficie de interconexión 4.

5 **[0044]** Como variante y/o adicionalmente, el módulo de configuración 6 es capaz de modificar la configuración de la superficie de interconexión 4 para desplazar a lo largo del tiempo, en una o en cada superficie de malla 2, la zona de la superficie de malla 2 que presenta el número de grupos de celdas conectadas más elevado. Una zona densa en grupos de celdas y por tanto en circuitos eléctricos permite detectar en efecto una intrusión con mayor facilidad. Por otro lado, tal zona utiliza más recursos para funcionar. El desplazamiento de tal zona permite por tanto efectuar un compromiso entre la precisión de detección de una intrusión y el consumo del sistema 1.

10 **[0045]** Cuando la superficie de interconexión 4 comprende el componente programable 23, el módulo de configuración 6 es, por ejemplo, una aplicación de software integrada en el componente programable 23.

15 **[0046]** Cuando la superficie de interconexión 4 comprende un microsistema electromecánico controlado por actuadores, el módulo de configuración 6 es capaz de activar los actuadores.

20 **[0047]** El módulo de detección 8 es capaz de detectar una modificación de una impedancia característica de cada grupo de celdas conectadas eléctricamente y, en particular, una interrupción de la continuidad o una alteración de los circuitos continuos formados por los grupos de celdas conectados a lo largo de la superficie de interconexión 4. Dado que una intrusión se caracteriza por una rotura o una alteración, el módulo de detección 8 es adecuado para detectar intrusiones. Por ejemplo, el módulo de detección 8 es adecuado para detectar un corte eléctrico por lazo seco, emisión-recepción de una señal, medición de latencia o cualquier otro procedimiento que permita detectar la alteración de un circuito constituido por un grupo de celdas interconectadas.

25 **[0048]** El módulo de detección 8 está configurado para aplicar una política de seguridad tras la detección de una interrupción en la continuidad de un grupo de celdas conectadas. La política de seguridad incluye, por ejemplo, el borrado de datos sensibles del equipo protegido por el sistema 1, la activación de pruebas complementarias tales como pruebas de integridad de las superficies de malla 2 o incluso la reconfiguración de las interconexiones de los conectores 24 según una nueva configuración de la superficie de interconexión 4 para realizar un complemento de  
30 detección.

**[0049]** Normalmente, el módulo de detección 8 está configurado para emitir periódicamente señales eléctricas en cada circuito eléctrico, para verificar después que se hayan recibido correctamente. En el caso de una mala recepción de una señal eléctrica, el módulo de detección 8 es capaz de detectar una alteración física de uno o varios  
35 circuitos eléctricos. En este ejemplo, el módulo de configuración 6 somete al módulo de detección 8 para que el módulo de detección 8 conozca las señales que se supone que debe recibir en la recepción.

40 **[0050]** Como variante y/o adicionalmente, el módulo de detección 8 incluye varios procedimientos de detección de rotura o alteración de un circuito y los utiliza de forma combinada según un entrelazado temporal definido, pseudoaleatorio o aleatorio.

**[0051]** El módulo de detección 8 está configurado para ser activado a una frecuencia regular, al menos igual a la frecuencia de reconfiguración, por parte del módulo de configuración 6, de las interconexiones de los conectores 24 de la superficie de interconexión 4.

45 **[0052]** Como variante, el módulo de detección 8 se activa en momentos elegidos aleatoriamente o pseudoaleatoriamente por el temporizador del sistema 1.

**[0053]** Cuando la superficie de interconexión 4 comprende el componente programable 23, el módulo de  
50 detección 8 es, por ejemplo, una aplicación de software integrada en el componente programable.

**[0054]** El módulo de reacción 10 está conectado al módulo de detección 8.

55 **[0055]** El módulo de reacción 10 permite iniciar una acción de reacción en respuesta a un intento de intrusión en el sistema 1 detectado por el módulo de detección 8. Por ejemplo, el módulo de reacción 10 está configurado para borrar los datos sensibles presentes en el equipo protegido por el sistema 1, para activar pruebas adicionales y/o para desencadenar una reconfiguración de las interconexiones de los conectores 24.

**[0056]** Cuando la superficie de interconexión 4 comprende el componente programable 23, el módulo de  
60 reacción 10 es, por ejemplo, una aplicación de software integrada en el componente programable.

**[0057]** Ventajosamente, el temporizador es un temporizador de bajo consumo. Para que el consumo total se mantenga bajo, la relación entre los periodos de vigilia y sueño del módulo de configuración 6 y/o del módulo de  
65 detección 8 activado por el temporizador es, por ejemplo, del orden de 1 por 1000, es decir, de 1000 microsegundos de vigilia por un segundo de sueño, sin embargo, con diferencias muy pequeñas entre la vigilia con respecto al tiempo

de implementación de un ataque.

**[0058]** Ahora se describirá un procedimiento de detección de intrusiones a partir del sistema de detección de intrusiones 1 de la figura 1.

5

**[0059]** Inicialmente, el procedimiento de detección de intrusiones comprende una etapa 100 de suministro del sistema de detección de intrusiones 1 tal como se describió anteriormente.

**[0060]** Entonces, el procedimiento de detección de intrusiones comprende una etapa 110 de determinación por el módulo de configuración 6 de una primera configuración de la superficie de interconexión 4.

**[0061]** Después, durante una siguiente etapa 120, el módulo de configuración 6 realiza la configuración de las interconexiones de los conectores 24 de la superficie de interconexión 4 según la primera configuración de la superficie de interconexión 4 previamente determinada durante la etapa 110.

15

**[0062]** A continuación, durante la siguiente etapa 130, se activa el módulo de detección 8 para detectar una posible interrupción de la continuidad eléctrica en cada grupo de celdas 3 interconectadas eléctricamente por los conectores 24 según la primera configuración de la superficie de interconexión 4. El módulo de detección 8 se activa, por ejemplo, en un momento elegido aleatoriamente por el temporizador.

20

**[0063]** Cuando el módulo de detección 8 detecta una interrupción en la continuidad de un circuito continuo, el módulo de detección 8 se comunica, durante una etapa 140, con el módulo de reacción 10. A continuación, el módulo de reacción 10 efectúa acciones de protección en el equipo protegido por el sistema 1.

**[0064]** A continuación, las etapas 110 a 140 se repiten a lo largo del tiempo. El módulo de configuración 6 se activa, por ejemplo, en momentos elegidos aleatoriamente por el temporizador. La configuración de la interconexión de los conectores 24 realizada por el módulo de configuración 6 durante la etapa 110 es alternativamente, por ejemplo, en función del estado del sistema o de un evento detectado.

**[0065]** Así, las interconexiones entre los conectores 24 se reconfiguran a lo largo del tiempo, lo que permite obtener nuevas configuraciones de la superficie de interconexión 4 y detectar posibles shunts de varias celdas con diferentes equipotenciales.

**[0066]** Como variante, el módulo de detección 8 se activa varias veces entre dos configuraciones, mediante el módulo de configuración 6, de las interconexiones de los conectores 24 de la superficie de interconexión 4. La activación del módulo de configuración 6 es, de hecho, independiente de la activación del módulo de detección 8.

**[0067]** Así, el sistema 1 permite proteger eficazmente el equipo contra ataques físicos con un formato de malla simple y económico que no complica las fases de desarrollo y fabricación del sistema 1. La superficie de interconexión 4 está programada para renovarse en función del tiempo, lo que aporta una notable ganancia para el nivel de protección de la malla.

**[0068]** En particular, la reconfiguración a lo largo del tiempo de las interconexiones de los conectores 24 entre las celdas 3 de las superficies de malla 2 permite limitar los ataques por ingeniería inversa y así inutilizar el uso de shunts para cortocircuitar los circuitos eléctricos de la malla. Además, el conocimiento adquirido por un atacante en el sistema es solo parcialmente reutilizable para el desarrollo de un ataque a otro sistema.

**[0069]** Además, la superficie de malla 2 y la superficie de interconexión 4 forman una barrera de protección física para el equipo protegido por el sistema 1, para el módulo de configuración 6 y para el módulo de detección 8.

50

**[0070]** Además, la función de ajuste de la malla en las zonas susceptibles de ser atacadas permite reforzar la protección del equipo que se va a proteger.

**[0071]** Además, el ajuste de la malla a nivel de una zona de interés es particularmente útil en el caso de una gestión optimizada del número de recursos disponibles, es decir, optimización del número de entradas y salidas de la superficie de interconexión 4.

**[0072]** El sistema 1 resuelve por tanto el problema de aumento de la complejidad de las mallas del estado de la técnica por reconfiguración de las interconexiones de los conectores 24 de la superficie de interconexión 4 a lo largo del tiempo. La geometría de la malla es, por tanto, específica de un equipo que se va a proteger y es variable en el tiempo.

60

**[0073]** La frecuencia de reconfiguraciones, por el módulo de configuración 6, de las interconexiones de los conectores 24 de la superficie de interconexión 4 puede adaptarse igualmente en función del nivel de protección deseado para el equipo o de los riesgos estimados de ataques.

65

**[0074]** El sistema 1 permite mantener igualmente el consumo de energía a un nivel aceptable y hacer que la protección sea duradera, incluso cuando el equipo del sistema 1 está alimentado por una fuente de energía de emergencia durante mucho tiempo.

5

**[0075]** El experto en la materia comprenderá que la invención no se limita a las realizaciones descritas, ni a los ejemplos particulares de la descripción.

**[0076]** Por ejemplo, además, el sistema 1 comprende un módulo para medir una variación de una magnitud entre al menos dos de las superficies de malla 2 del sistema 1. La magnitud se elige, por ejemplo, entre una impedancia, una resistencia, una capacitancia y una inductancia. Las variaciones en la magnitud permiten detectar intentos de intrusión y activar entonces el módulo de configuración 6 y/o el módulo de reacción 10.

**[0077]** En otro ejemplo, el sistema 1 comprende además al menos una superficie de blindaje dispuesta alrededor de la(s) superficie(s) de malla 2. La superficie de blindaje permite, por ejemplo, proteger el equipo de ataques químicos o electromagnéticos.

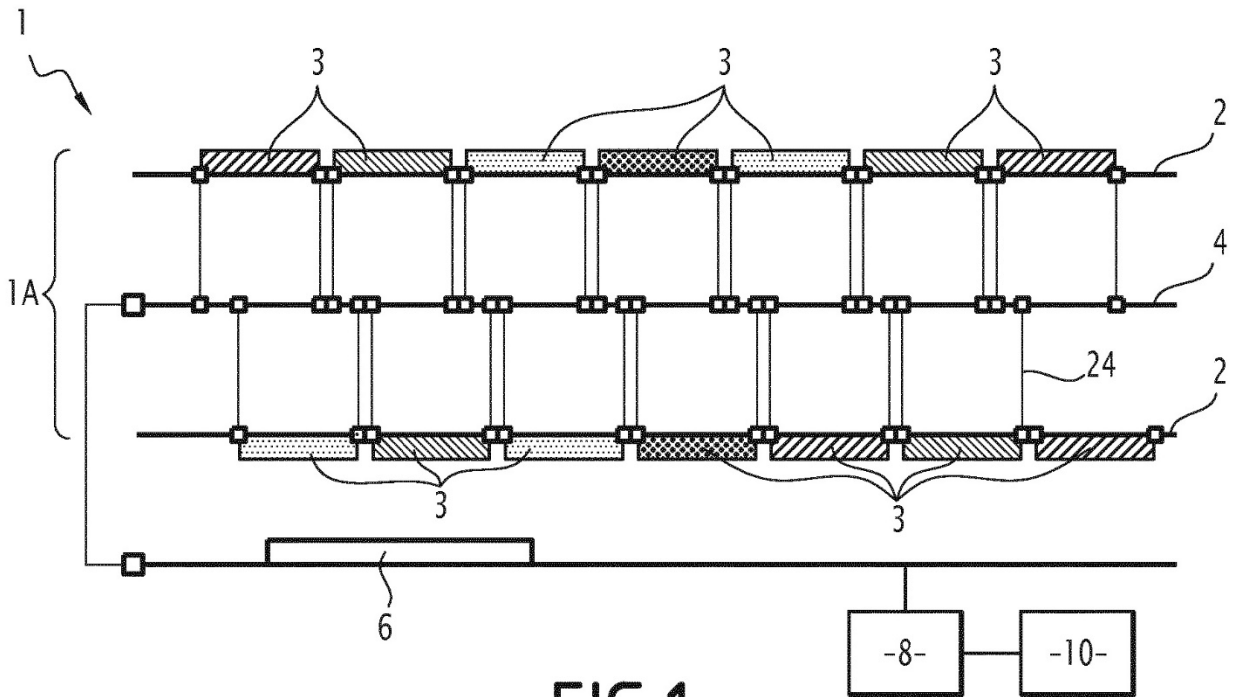
**[0078]** En otro ejemplo más, al menos un circuito eléctrico está formado por la conexión, que no puede ser reconfigurada por el módulo de configuración 6, de al menos dos celdas adyacentes 3 de una superficie de malla 2 a través de un componente previamente configurado de forma estática en fábrica. Un componente configurado previamente de forma estática es un componente integrado de manera inalterable en el sistema 1 durante su fabricación. Cada grupo de celdas conectadas entre sí por un componente previamente configurado de forma estática forma una macrocelda. Las macroceldas presentan la ventaja de limitar el número de interconexiones de los conectores 24 de la superficie de interconexión 4. En este caso, como se ilustra en la figura 7, el procedimiento para detectar intrusiones comprende además una etapa 150 de construcción en fábrica de interconexiones no reconfigurables que forman las macroceldas.

**[0079]** En este último ejemplo, las interconexiones de los conectores 24 de la superficie de interconexión 4 se definen parcialmente estáticamente para ciertos grupos de celdas y dinámicamente para otros.

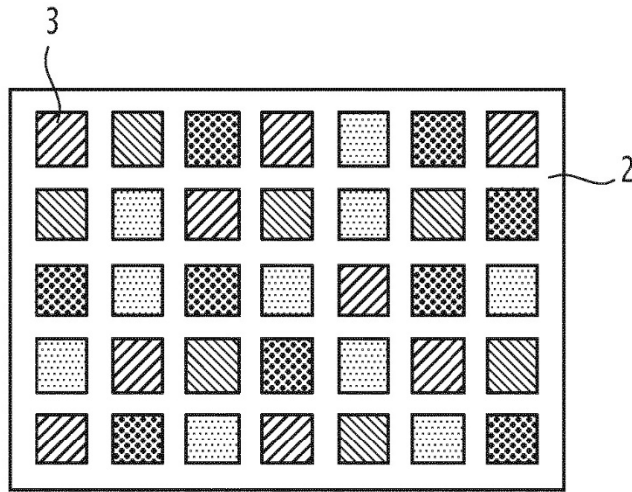
REIVINDICACIONES

1. Sistema de detección de intrusiones (1), para la protección de un equipo por el que pasa información sensible, comprendiendo el sistema (1):
- 5
- al menos una superficie de malla (2), comprendiendo cada superficie de malla (2) al menos dos celdas (3), comprendiendo cada celda (3) un patrón (20), siendo un patrón (20) una parte de un circuito eléctrico continuo,
  - al menos una superficie de interconexión (4) que comprende una pluralidad de conectores (24), siendo los conectores (24) adecuados para interconectar celdas (3) de la(s) superficie(s) de malla (2) según una primera configuración de la superficie de interconexión (4) para formar grupos de celdas conectadas eléctricamente (3), formando los patrones (20) de las celdas (3) de cada grupo un circuito eléctrico continuo de patrones (20),
  - un módulo de detección (8) apto para detectar una modificación de una impedancia característica de cada grupo de celdas conectadas eléctricamente,
  - un módulo de configuración (6) de las interconexiones de los conectores (24), pudiendo el módulo de configuración (6) modificar la primera configuración a lo largo del tiempo para obtener al menos una segunda configuración de la superficie de interconexión (4),
- 10
- caracterizado porque** el módulo de configuración (6) es capaz de modificar la configuración de la superficie de interconexión (4) cuando el módulo de detección (8) detecta un intento de intrusión, cuando se produce una interrupción de la continuidad eléctrica de al menos un circuito continuo detectado en una zona de una superficie de malla (2), pudiendo el módulo de configuración (6) modificar la configuración de la superficie de interconexión (4) para aumentar el número de grupos de celdas conectadas presentes en la zona.
- 15
2. Sistema (1) según la reivindicación 1, en el que el módulo de configuración (6) es capaz de determinar de manera aleatoria la segunda configuración entre una pluralidad de configuraciones de la superficie de interconexión (4) y reconfigurar el conjunto de las interconexiones de los conectores (24) según la segunda configuración.
- 25
3. Sistema (1) según la reivindicación 1 o 2, en el que el sistema (1) comprende al menos dos superficies de malla (2) y un módulo para medir variaciones de magnitud entre dos de las superficies de malla (2), eligiendo la magnitud entre una impedancia, una resistencia, una capacitancia y una inductancia.
- 30
4. Sistema (1) según cualquiera de las reivindicaciones 1 a 3, en el que al menos un circuito eléctrico está formado por la conexión no reconfigurable por el módulo de configuración (6), de al menos dos celdas adyacentes (3) de una superficie de malla (2) a través de un componente previamente configurado de forma estática.
- 35
5. Sistema (1) según cualquiera de las reivindicaciones 1 a 4, en el que el módulo de configuración (6) es capaz de desplazar a lo largo del tiempo, sobre una o sobre cada superficie de malla (2), una zona de la superficie de malla (2) que presenta el número de grupos de celdas conectadas más elevado.
- 40
6. Sistema (1) según cualquiera de las reivindicaciones 1 a 5, en el que el sistema (1) comprende un órgano capaz de activar en momentos elegidos aleatoria o pseudoaleatoriamente el módulo de configuración (6) y/o el módulo de detección (8).
- 45
7. Sistema (1) según cualquiera de las reivindicaciones 1 a 6, en el que la superficie de interconexión (4) comprende un componente programable, siendo el módulo de configuración (6) y el módulo de detección (8) unas aplicaciones de software integradas en el componente programable.
- 50
8. Sistema (1) según cualquiera de las reivindicaciones 1 a 6, en el que la superficie de interconexión (4) comprende un microsistema electromecánico controlado por actuadores, siendo el módulo de configuración (6) adecuado para el accionamiento de los actuadores.
- 55
9. Sistema (1) según cualquiera de las reivindicaciones 1 a 8, en el que la superficie de malla (2) y la superficie de interconexión (4) forman una barrera de protección física para el módulo de configuración (6) y para el módulo de detección (8).
- 60
10. Sistema (1) según cualquiera de las reivindicaciones 1 a 9, en el que, tras la detección de una interrupción de la continuidad eléctrica de un grupo de celdas conectadas, el módulo de detección (8) es capaz de aplicar una política de seguridad, comprendiendo la seguridad política el borrado de datos sensibles, la implementación de pruebas de integridad y/o la reconfiguración de las interconexiones de los conectores (24) de la superficie de interconexión (4).
- 65
11. Sistema (1) según cualquiera de las reivindicaciones 1 a 10, en el que el módulo de detección (8) incluye varios procedimientos para detectar la rotura o la alteración de cada grupo de celdas conectadas eléctricamente y es apto para utilizarlas de forma combinada según un entrelazado temporal definido, pseudo-aleatorio o aleatorio.
12. Procedimiento de detección de intrusiones, comprendiendo el procedimiento las etapas de:

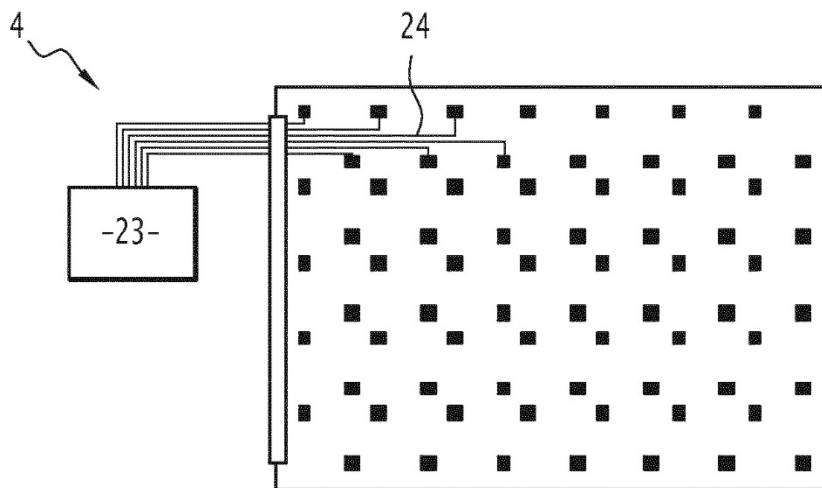
- suministro (100) de un sistema de detección de intrusos (1) según cualquiera de las reivindicaciones 1 a 11,
- determinación (110) por el módulo de configuración (6) de una primera configuración de la superficie de interconexión (4),
- 5 - configuración (120) por el módulo de configuración (6) de las interconexiones de los conectores (24) de la superficie de interconexión (4) según la primera configuración determinada,
- activación (130) del módulo de detección (8) para detectar una modificación de una impedancia característica de cada grupo de celdas conectadas eléctricamente,
- 10 - posible detección (140) por el módulo de detección (8) de una modificación de una impedancia característica de un grupo de celdas conectadas eléctricamente, y
- modificación de la primera configuración de la superficie de interconexión (4) por el módulo de configuración (6) para interconectar los conectores (24) de la superficie de interconexión (4) según una segunda configuración, siendo realizada la modificación de la configuración de la superficie de interconexión (4) cuando el módulo de detección (8) detecta un intento de intrusión, cuando se detecta una interrupción de la continuidad eléctrica de al
- 15 menos un circuito continuo en una zona de una superficie de malla (2), siendo modificada la configuración de la superficie de interconexión (4) para aumentar el número de grupos de celdas conectadas presentes en la zona.



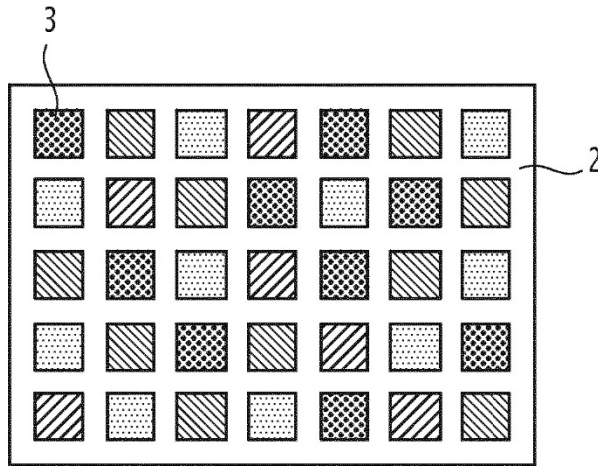
**FIG. 1**



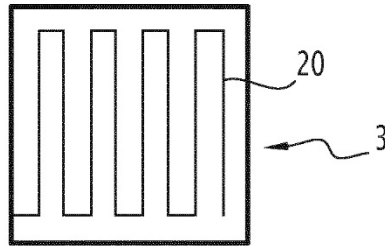
**FIG. 2**



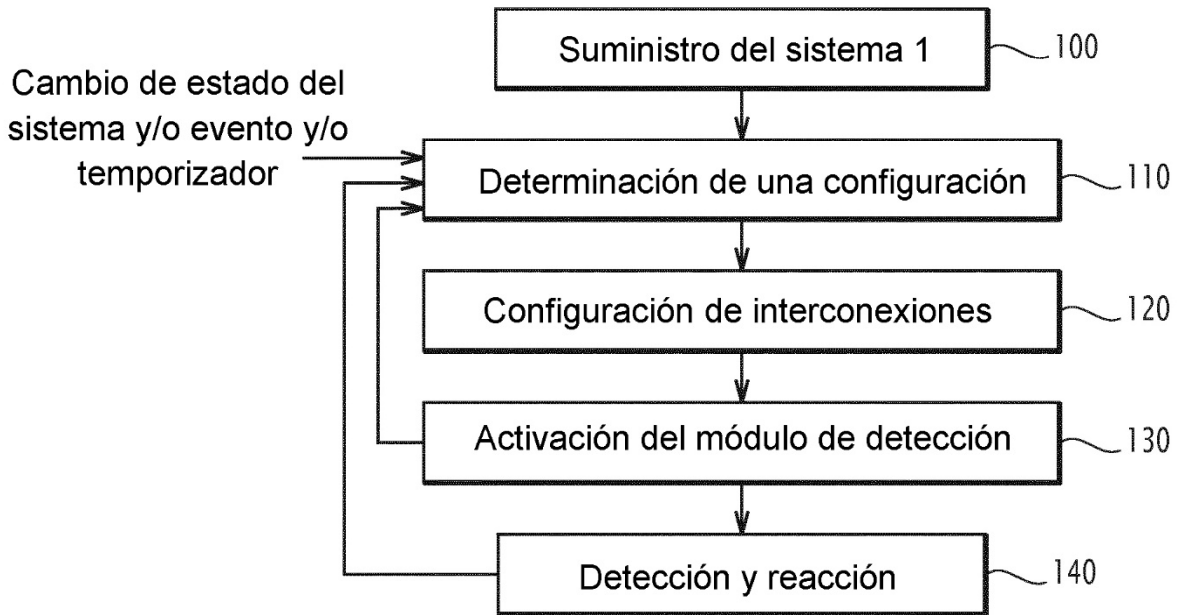
**FIG. 3**



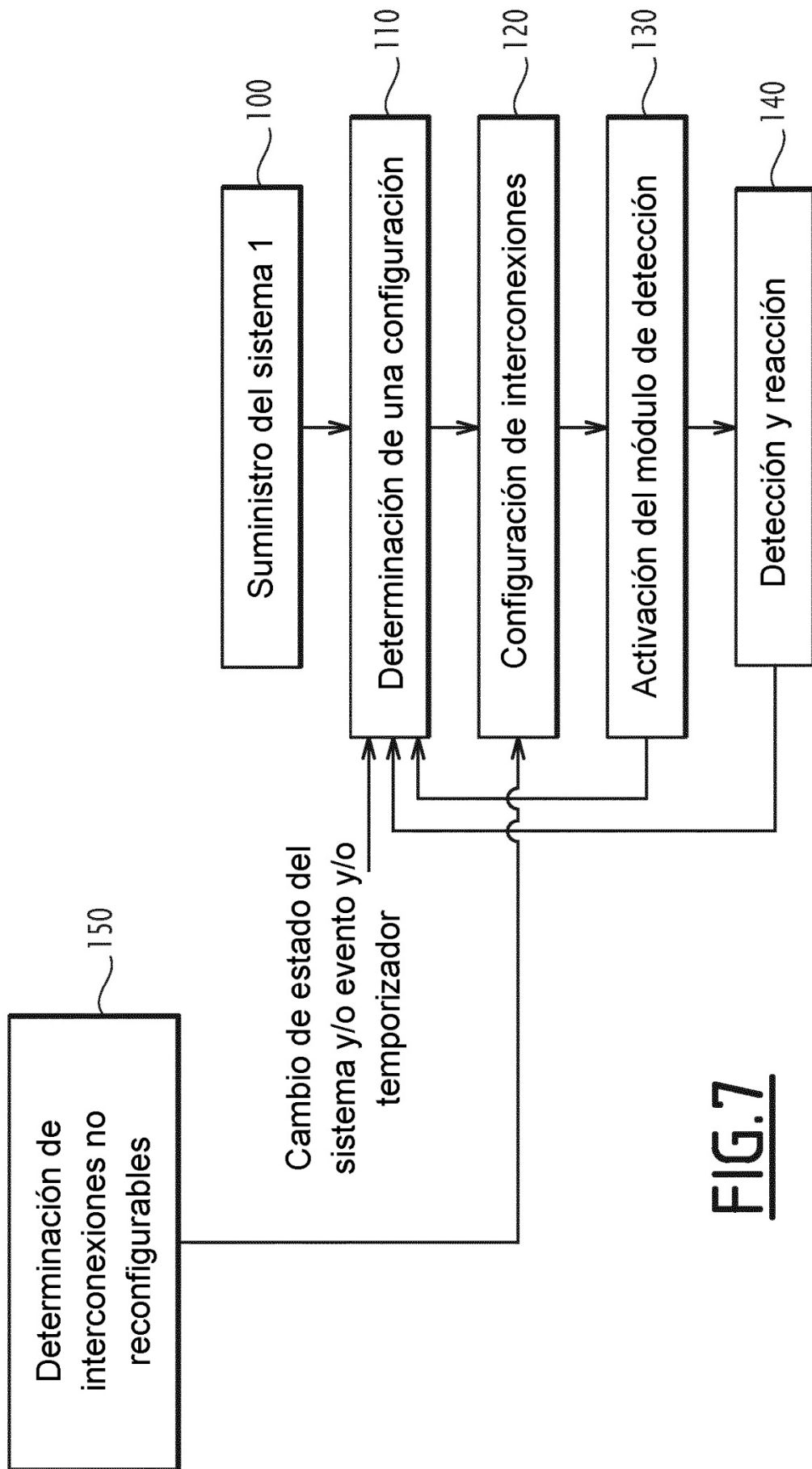
**FIG.4**



**FIG.5**



**FIG.6**



**FIG. 7**