



MARIO DELGADO ECHEVERRY E HIJOS SAS
IP LAWYERS

BOGOTA - COLOMBIA

AK. 24 No. 37 31 Of. 202
TEL. (571) 2444096 – 3690624 –
2444938 - Fax (571) 2442496
E-mail: mde@mdelaw.com
MIEMBROS
INTA – ASIP – AIPPI – ACPI
AAAPI – ABPI – ABAPI

Bogotá D.C., 11 de julio de 2018

Señores
DIVISIÓN DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Ciudad

REFERENCIA: Expediente No. 16 – 119.034

TÍTULO: “MÉTODO Y DISPOSITIVO DE DETECCIÓN DE INTERFERENCIA DELIBERADA”

SOLICITANTE: VERISURE SÀRL

TRÁMITE: Respuesta a Concepto Técnico notificado mediante Oficio No. 4.216 del 12 de abril de 2018.

JAIME EDUARDO DELGADO VILLEGAS, en mi condición de apoderado de la sociedad **VERISURE SÀRL**, dentro del término legal, presento respuesta a Concepto Técnico notificado mediante Oficio No. 4.216 del 12 de abril de 2018.

1. REIVINDICACIONES

El solicitante en primer lugar, procedió a **modificar las reivindicaciones**, de la siguiente forma:

- La **nueva Reivindicación 1** incluye materia de las **Reivindicaciones originales 2, 4 y 5**. Además, la **Reivindicación 1** se ha **modificado** para **definir un sistema de seguridad que comprende varios elementos** (un periférico 1, un panel de control 3 y un sistema de gestión central 5)



MARIO DELGADO ECHEVERRY E HIJOS SAS
IP LAWYERS

BOGOTA - COLOMBIA

AK. 24 No. 37 31 Of. 202
TEL. (571) 2444096 – 3690624 –
2444938 - Fax (571) 2442496
E-mail: mde@mdelaw.com
MIEMBROS
INTA – ASIP – AIPPI – ACPI
AAAPI – ABPI – ABAPI

conectados entre sí a través de diferentes bandas de frecuencia de diferentes redes de comunicación.

Este sistema de seguridad además **comprende un dispositivo de detección de interferencia deliberada** con unas características específicas, que se definen en esta **Reivindicación 1**.

Soporte para las modificaciones realizadas en la **Reivindicación 1** puede encontrarse en la pág. 4, líneas 1-26 de la solicitud originalmente presentada.

- De forma similar se ha **modificado la Reivindicación 11 de método**.

Soporte para las modificaciones realizadas en la reivindicación 11 puede encontrarse en la pág. 4, líneas 1-26 de la solicitud originalmente presentada.

Se ha **añadido la Reivindicación dependiente 14 de método**. Soporte para esta **nueva Reivindicación 14** puede encontrarse en la pág. 5, líneas 23-25 de la solicitud originalmente presentada.

- En el **resto de reivindicaciones se ha modificado la numeración y su dependencia con otras reivindicaciones**, para mantener coherencia.

Respecto a las **modificaciones realizadas en las reivindicaciones**, estas están basadas en las **modificaciones realizadas en la solicitud prioritaria EP 15382243**. Con relación con esta solicitud EP, adjuntamos también la acción



MARIO DELGADO ECHEVERRY E HIJOS SAS
IP LAWYERS

BOGOTA - COLOMBIA

AK. 24 No. 37 31 Of. 202
TEL. (571) 2444096 – 3690624 –
2444938 - Fax (571) 2442496
E-mail: mde@mdelaw.com
MIEMBROS
INTA – ASIPI – AIPPI – ACPI
AAAPI – ABPI – ABAPI

oficial emitida por la Oficina Europea de Patentes (EPO) en la que la División de Examen muestra su intención de concesión, si las reivindicaciones se modifican según su propuesta. Las reivindicaciones anexas están basadas en esa propuesta de la División de Examen de la EPO.

Por lo expresado anteriormente, el solicitante pone a consideración del Examinador Técnico de Patentes un **NUEVO CAPITULO REIVINDICATORIO** el cual consta de **catorce (14) nuevas reivindicaciones** en cuatro folios.

2. ANÁLISIS DE PATENTABILIDAD.

Nivel Inventivo (Art 18 D486)

El Examinador objeto el nivel inventivo de las reivindicaciones 1 – 5, 7 y 14 con los documentos **D1 (GB2457102)** y **D2 (US4117405)** porque:

“En consecuencia, la persona del oficio normalmente versada en la materia incluiría un transceptor que envía una señal de alarma por medio de una red de banda ultra estrecha, con frecuencias menores a 200 Hz del documento D2 en el dispositivo divulgado en el documento D1 para llegar así al objeto de la reivindicación 1 de la solicitud. Por lo cual se considera obvia”.

“En consecuencia, la persona del oficio normalmente versada en la materia incluiría un transceptor que explora distintas bandas ISM, según las frecuencias del sistema donde vaya a funcionar la invención, en el dispositivo divulgado en el documento D1 para llegar así al objeto de la reivindicación 2 de la solicitud. Por lo cual se considera que no posee nivel inventivo”.

“En consecuencia, la persona del oficio normalmente versada en la materia incluiría un transceptor que explora una primera banda ISM centrada en 868 MHz, debido a que la frecuencia del sistema donde vaya a funcionar la invención es esta, en el dispositivo divulgado en el documento D1 para llegar así al objeto de la reivindicación 3 de la solicitud. Por lo cual se considera que no posee nivel inventivo”.

“En consecuencia, la persona del oficio normalmente versada en la materia incluiría la

Visite nuestra página web: www.mdelaw.com



MARIO DELGADO ECHEVERRY E HIJOS SAS
IP LAWYERS

BOGOTÁ - COLOMBIA

AK. 24 No. 37 31 Of. 202
TEL. (571) 2444096 – 3690624 –
2444938 - Fax (571) 2442496
E-mail: mde@mdelaw.com
MIEMBROS
INTA – ASIPI – AIPPI – ACPI
AAAPI – ABPI – ABAPI

etapa de enviar una señal de alarma por medio de una red de banda ultra estrecha, con frecuencias menores a 200 Hz del documento D2 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 14 de la solicitud. Por lo cual se considera que no posee nivel inventivo”.

R/: Nuestro poderdante se permite manifestar en cuanto a las objeciones de **falta de nivel inventivo** de la solicitud, por parte del Examinador, lo siguiente:

Novedad

Ya fue reconocida la novedad del capítulo reivindicatorio anteriormente bajo examen. Las nuevas reivindicaciones que se presentan ahora incluyen características adicionales, por lo que estas nuevas reivindicaciones también son nuevas.

Nivel inventivo

En la **nueva Reivindicación 1**, se han **añadido una serie de características relativas a bandas de comunicación y tecnologías**. Esta combinación de bandas de comunicación y tecnologías tiene **un efecto sinérgico de protección contra ataques e interferencias resistentes**, a la vez que optimiza el uso del ancho de banda.

En los documentos **D1 y D2** citados **no se muestra que la señal de alarma (tras la detección de interferencia deliberada) se haga a través de una frecuencia de la red UNB que esté solapada parcial o totalmente con la red ISM**.

De hecho, la **materia reivindicada** difiere de los sistemas conocidos en los documentos **D1 y D2** en que:

Visite nuestra página web: www.mdelaw.com



MARIO DELGADO ECHEVERRY E HIJOS SAS
IP LAWYERS

BOGOTÁ - COLOMBIA

AK. 24 No. 37 31 Of. 202
TEL. (571) 2444096 – 3690624 –
2444938 - Fax (571) 2442496
E-mail: mde@mdelaw.com
MIEMBROS
INTA – ASIP – AIPPI – ACPI
AAAPI – ABPI – ABAPI

- el **sistema de seguridad** incluye además un dispositivo de detección de interferencia deliberada que está conectado a un servicio de gestión central a través de una red de banda ultra estrecha (UNB); y
- este **dispositivo de detección de interferencia deliberada** comprende un transceptor configurado para escanear periódicamente las bandas de frecuencia utilizadas por el sistema de seguridad;
- cuando se detecta una interferencia deliberada, el **transceptor del dispositivo de detección** envía una señal de alarma al servicio de gestión central a través de la red de banda ultra-estrecha (UNB) que está solapada parcial o totalmente con primera banda de frecuencia de la red IMS.

El **efecto técnico de estas diferencias** es la **capacidad de enviar la señal de alarma de una manera resistente a la interferencia deliberada**, en un sistema de seguridad que normalmente no funciona con la frecuencia de la red de banda ultra-estrecha (UNB), y que no afecta al sistema cuando no hay interferencias deliberadas.

Esta **combinación de bandas de comunicación y tecnologías** tiene un **efecto sinérgico de protección contra ataques e interferencias resistentes**, a la vez que optimiza el uso del ancho de banda.

Por ello, la **Reivindicación 1 es también inventiva** frente a los documentos del estado de la técnica.



MARIO DELGADO ECHEVERRY E HIJOS SAS
IP LAWYERS

BOGOTA - COLOMBIA

AK. 24 No. 37 31 Of. 202
TEL. (571) 2444096 – 3690624 –
2444938 - Fax (571) 2442496
E-mail: mde@mdelaw.com
MIEMBROS
INTA – ASIPI – AIPPI – ACPI
AAAPI – ABPI – ABAPI

Por lo expresado anteriormente, el **Dispositivo de detección de interferencia deliberada para un sistema de seguridad**, tal como se describe en la presente solicitud de patente de invención de nuestro poderdante, **no está comprendida en el estado de la técnica o anticipada**, ni se encuentran definidas ni mucho menos divulgada en los documentos **D1 y D2** citados por el Examinador. Por lo tanto, la invención es **NOVEDOSA**, tiene **NIVEL INVENTIVO Y APLICACIÓN INDUSTRIAL**, es decir cumple con los requisitos de exigidos por la Decisión 486 del Acuerdo de la Comisión de la Comunidad Andina; además, estamos dando respuesta al Concepto Técnico notificado mediante Oficio No. 4.216 del 12 de abril de 2018.

Por lo anteriormente mencionado, solicito respetuosamente se proceda a **CONCEDER** la Patente de Invención titulada: **“MÉTODO Y DISPOSITIVO DE DETECCIÓN DE INTERFERENCIA DELIBERADA”** a nombre de **VERISURE SÀRL**, para las nuevas Reivindicaciones 1 a 14 inclusive.

Atentamente,

JAIME EDUARDO DELGADO VILLEGAS
C.C. No. 19.270.955 Bogotá
T.P. No. 43.308 C.S.J.

Anexo:
Nuevas Reivindicaciones (14) en cuatro folios.
Acción oficial emitida por la Oficina Europea de Patentes (EPO) en cuatro folios.

NUEVAS REIVINDICACIONES

1. Dispositivo de detección de interferencia deliberada (7) para un sistema de seguridad, comprendiendo el sistema de seguridad un periférico (1) y un panel de control (3) conectados a través de una primera banda de frecuencia (201) de una red de radio Industrial, Científica y Médica (2); estando el panel de control (3) conectado a un servicio de gestión central (5) a través de una tercera banda de frecuencia (401,402) de una red de GSM (4),
- en el que dispositivo de detección de interferencia deliberada (7) comprende un transceptor (701) configurado para explorar periódicamente una banda de frecuencia (201, 401, 402) del sistema de seguridad para detectar interferencia deliberada, incluyendo la primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2) y la tercera banda de frecuencia (401, 402) de la red de GSM (4),
- en donde, si se detecta interferencia deliberada en la primera banda de frecuencia (201) o en la tercera banda de frecuencia (401, 402), el transceptor (701) está configurado para enviar una señal de alarma al servicio de gestión central (5) a través de una segunda banda de frecuencia (801) de una red de banda ultra estrecha (8) que comprende canales de ancho de banda menor o igual de 200 Hz, estando la segunda banda de frecuencia solapada parcial o completamente con la primera banda de frecuencia de la red de radio Industrial, Científica y Médica (2).
2. Dispositivo de detección de interferencia deliberada (7) de acuerdo con la Reivindicación 1, **CARACTERIZADO PORQUE** la primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2) está centrada en 868 MHz.
3. Dispositivo de detección de interferencia deliberada (7) de acuerdo con una cualquiera de las Reivindicaciones 1-2, **CARACTERIZADO PORQUE** el transceptor (701) está configurado para explorar periódicamente una banda de frecuencia (401) de 900 MHz y una banda de frecuencia (402) de 1800 MHz de la red del Sistema Global para Comunicaciones Móviles (4).

4. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las Reivindicaciones anteriores, **CARACTERIZADO PORQUE** el transceptor (701) comprende un oscilador local (702) configurado para generar una pluralidad de armónicos, explorándose la banda de frecuencia (201, 401, 402) con un armónico de tercer orden.
5. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las Reivindicaciones anteriores, **CARACTERIZADO PORQUE** el transceptor (701) comprende medios de modulación configurados para aplicar salto de frecuencia aleatoria a la señal de alarma cuando se accede a la red de banda ultra estrecha (8).
6. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las Reivindicaciones anteriores, **CARACTERIZADO PORQUE** el transceptor (701) comprende medios de modulación configurados para aplicar una modulación por desplazamiento de fase binaria a la señal de alarma cuando se accede a la red de banda ultra estrecha (8).
7. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las Reivindicaciones anteriores, **CARACTERIZADO PORQUE** el dispositivo (7) comprende adicionalmente un acelerómetro (705), y porque el transceptor (701) está configurado para enviar una señal de alarma al servicio de gestión central (5) a través de la red de banda ultra estrecha (8) cuando una medición del acelerómetro (705) supera un primer umbral predefinido.
8. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las Reivindicaciones anteriores, **CARACTERIZADO PORQUE** el dispositivo (7) comprende adicionalmente un termómetro (706), y por que el transceptor (701) está configurado para enviar una señal de alarma al servicio de gestión central (5) a través de la red de banda ultra estrecha (8) cuando una medición del termómetro (706) supera un segundo umbral predefinido.
9. Dispositivo de detección de interferencia deliberada (7) de acuerdo con

5 cualquiera de las Reivindicaciones anteriores, **CARACTERIZADO PORQUE** el dispositivo (7) comprende adicionalmente una interfaz de usuario (704), y porque el transceptor (701) está configurado para enviar una señal de alarma al servicio de gestión central (5) a través de la red de banda ultra estrecha (8) cuando un usuario introduce un comando a través de la interfaz de usuario (704).

10. Sistema de seguridad que comprende:

- 10
- al menos un periférico (1) y un panel de control (3) conectados a través de una primera banda de frecuencia (201) de una red de radio Industrial, Científica y Médica (2);
 - el panel de control (3) está conectado a un servicio de gestión central (5) a través de una tercera banda de frecuencia (402,402) de una red de GSM (4);

15 **CARACTERIZADO PORQUE** el sistema de seguridad además comprende:

- un dispositivo de detección de interferencia deliberada (7) según cualquiera de las Reivindicaciones 1-9.

20 11. Método de detección de interferencia deliberada que comprende:

- medir una primera potencia de RF periódicamente en una banda de frecuencia (201, 401, 402) de un sistema de seguridad;
- medir una segunda potencia de RF en la banda de frecuencia (201, 401, 402) y comprobar si la segunda potencia de RF supera una media móvil de la primera potencia de RF;
- si la segunda potencia de RF supera la media móvil, esperar un periodo de tiempo, medir una tercera potencia de RF en la banda de frecuencia (201, 401, 402) y comprobar si la tercera potencia de RF supera la media móvil;
- si la segunda potencia de RF y la tercera potencia de RF superan la media móvil, enviar una señal de alarma a un servicio de gestión central (5) a través de una red de banda ultra estrecha (8) que comprende canales de ancho de banda menor o igual de 200 Hz.

35 12. Método de detección de interferencia deliberada para un sistema de seguridad que comprende al menos un periférico (1) y un panel de control

(3) conectados a través de una primera banda de frecuencia (201) de una red de radio Industrial, Científica y Médica (2); estando el panel de control (3) conectado a un servicio de gestión central (5) a través de una tercera banda de frecuencia (401,402) de una red de GSM (4);

5 en donde el método de detección de interferencia deliberada comprende:

- explorar periódicamente una banda de frecuencia (201, 401, 402) del sistema de seguridad, comprendiendo la frecuencia explorada la primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2) y la tercera banda de frecuencia (401,402) de la red de GSM (4);

10 **CARACTERIZADO PORQUE** el método comprende adicionalmente:

- si durante la etapa de explorar se detecta interferencia deliberada en la primera banda de frecuencia (201) o en la tercera banda de frecuencia (401, 402), enviar una señal de alarma al servicio de gestión central (5) a través de una segunda banda de frecuencia (801) de una red de banda ultra estrecha (8) que comprende canales de ancho de banda menor o igual de 200 Hz, estando la segunda banda de frecuencia solapada parcial o completamente con la primera banda de frecuencia de la red de radio Industrial, Científica y Médica (2).

13. Método de detección de interferencia deliberada según la Reivindicación 12, **CARACTERIZADO PORQUE** la etapa de enviar la señal de alarma comprende adicionalmente enviar un identificador (904) de la banda de frecuencia (201, 401, 402) y un primer valor numérico que representa una intensidad de interferencia deliberada (906).

14. Método de detección de interferencia deliberada según la Reivindicación 13, en el que el método comprende adicionalmente enviar un segundo valor numérico que indica la duración de la interferencia deliberada, una vez que el dispositivo detecta que la interferencia deliberada ha finalizado.

The examination is being carried out on the **following application documents**

Description, Pages

1-14 as originally filed

Claims, Numbers

1-12 filed in electronic form on 09-05-2017

Drawings, Sheets

1/2, 2/2 as originally filed

1 Article 123(2) EPC

1.1 The present application does not meet the requirements of Article 123(2) EPC as the amended set of claims sent with letter of 09-05-2017 contains subject-matter extending beyond the contents of the application as filed. The newly filed independent claim 1 contains the following features:

...the transceiver (701) is further configured to:

...if jamming is not detected in the at least one first frequency band (201) nor in the at least one third frequency band (401, 402), connect at least a peripheral (1) to a control panel (3) through the at least one first frequency band (201), being the control panel (3) connected to a back-service (7) through the at least one third frequency band (401, 402);

1.2 This added feature implies that a) the transceiver of the jamming detection device connects the control panel to the peripheral devices and b) this connection occurs if jamming is not detected in the at least one frequency band.

1.3 Neither the connection between control and peripherals by the transceiver of the jamming detection device nor the condition for the connection to occurs in case of no jamming detection is disclosed in the present application as filed. According to the disclosure on page 8, lines 22 to 25. The control panel and the peripherals are connected through the frequency of an ISM network. Also claims 3 and 5 do not disclose the added features.

2 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

- D1 GB 2 457 102 A (SCHAAR GEORGE [GB]) 5 August 2009 (2009-08-05)
- D2 WO 2005/119609 A2 (KATES LAWRENCE [US]) 15 December 2005 (2005-12-15)
- D3 US 4 117 405 A (MARTINEZ LOUIS) 26 September 1978 (1978-09-26)
- D4 US 2004/121731 A1 (WALKER HAROLD R [US]) 24 June 2004 (2004-06-24)
- D5 US 2006/072684 A1 (FEHER KAMILO [US]) 6 April 2006 (2006-04-06)
- D6 US 2010/295672 A1 (HYLAND GREGORY E [US] ET AL) 25 November 2010 (2010-11-25)
- D7 US 4 737 771 A (COASH RONALD J [US]) 12 April 1988 (1988-04-12)

3 The following document is cited by the Examiner. A copy of the document is annexed to the communication and the numbering will be adhered to in the rest of the procedure.

- D8 EP 2 515 282 A1 (SECURITAS DIRECT AB [SE]; CROW ELECTRONIC ENGINEERING LTD [IL]) 24 October 2012 (2012-10-24)

4 Suggestion

4.1 The examining division would like to propose the following text for an allowable independent claim which overcomes the objection on added subject-matter.

A jamming detection device for a security system (or a security system comprising a jamming detection device); the security system comprising a control panel connected to peripherals through a frequency band of an ISM network, the control panel connected to a back-end service through a frequency band of a GSM network;

the jamming detection device connected to the back-end service through an Ultra-narrow band network (UNB);

the jamming detection device comprising a transceiver configured to periodically scan all the frequency bands used by the security system;

when jamming is detected, the transceiver of the jamming detection device is configured to send an alert signal to the back-end service through a UNB network overlapped with the frequency band of the ISM network.

- 4.2 The above claim would be considered as allowable for the following reasons: The document D8 discloses a security system comprising a control panel connected to peripherals through a frequency band of an ISM network, the control panel connected to a back-end service through a frequency band of another network (paragraphs 82, 83 and 93).
- 4.3 The subject-matter claimed as above differs from the known system in that the system further comprises a jamming detection device connected to the back-end service through an Ultra-narrow band network (UNB) the jamming detection device comprising a transceiver configured to periodically scan all the frequency bands used by the security system; when jamming is detected, the transceiver of the jamming detection device is configured to send an alert signal to the back-end service through a UNB network overlapped with the frequency band of the ISM network.
- 4.4 The effect is the ability to send the jam signal in a jamming resistant way in a security system which does not normally work with UNB signal and without affecting the system when jamming is not present (see also page 7, lines 6 to 9).

- 4.5 The document D1 discloses detecting jamming and changing the frequency to send a jam signal to the back-end service, but there is no disclosure of sending the jam signal via UNB overlapped with the ISM network. Although the documents D3 to D5 do disclose that UNB signal are jamming resistant, the skilled person would need this extra teaching plus the incentive to overlap the UNB signal with the ISM band to fill the gap and arrive at the claimed invention.
- 4.6 Starting from D1, there would still be the difference of the security system using two networks as claimed, both networks being scanned and the sending of the jam signal via UNB overlapped with the ISM network. Combining the teaching of D8 for the security system and one of D3 to D5 for the UNB signal, the skilled person still needs the overlap of the UNB signal with the ISM network.
- 5 It is noted that this suggestion is only for assisting the applicant in his decision on how to proceed. It in no way precludes consideration of alternative solutions submitted by the applicant. The responsibility for determining the text of the application (Article 113(2) EPC) and in particular for defining the subject-matter for which protection is sought remains with the applicant.