(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 513 665**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/75 (2013.01)
G06F 12/02 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.01.2012 E 12705317 (1)**

(97) Fecha y número de publicación de la concesión europea: **09.07.2014 EP 2689369**

(54) Título: **Procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico y dispositivo que comprende un módulo de control correspondiente**

(30) Prioridad:

21.03.2011 FR 1152313

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.10.2014

(73) Titular/es:

MORPHO (100.0%)
11 Boulevard Gallieni
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

BERTHIER, MAEL y
BARTHE, MICHAEL

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico y dispositivo que comprende un módulo de control correspondiente

La invención se refiere a un procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico, que comprende un puerto de entrada / salida, un microprocesador, una memoria viva, una memoria muerta y una memoria no volátil reprogramable que contiene una variable de estado del fin de la vida útil del dispositivo electrónico gestionada mediante un módulo de control.

Tales dispositivo electrónicos corresponden, de manera no exclusiva, a las tarjetas electrónicas, o a cualquier dispositivo electrónico que comprenda al menos o que esté en relación con, una tarjeta electrónica, tal como, particularmente, una tarjeta con microprocesadores, para la cual se requiere una buena resistencia de seguridad, frente a cualquier intromisión externa.

Para asegurar una buena resistencia de seguridad de las tarjetas citadas anteriormente, se activa un mecanismo de paso al fin de la vida útil, mediante la detección de un cierto número de errores críticos.

El proceso de paso al fin de la vida útil de este tipo de dispositivo, particularmente en lo que se refiere a las tarjetas con microprocesadores, resulta sin embargo problemático, puesto que tal proceso se apoya convencionalmente sobre un proceso de escritura en la memoria reprogramable no volátil, generalmente una memoria EEPROM, teniendo por objeto este proceso de escritura la modificación de los datos y el bloqueo de las aplicaciones.

Tal proceso resulta no obstante vulnerable, puesto que es detectable desde fuera de la tarjeta, por razones principalmente del fuerte consumo de corriente generado por el proceso de escritura en la memoria reprogramable.

Alguien deshonesto tiene por consiguiente toda la libertad para impedir la ejecución de tal proceso, cortando la alimentación eléctrica del dispositivo o de la tarjeta.

Para mejorar esta situación, se ha propuesto en los documentos FR 07 08242 y PCT/FR2008/052106, hacer el proceso de paso al fin de la vida útil de tal dispositivo electrónico un hecho en un periodo de tiempo aleatorio después de que se produzca el evento, error crítico, en el origen del desencadenamiento del paso al fin de la vida útil, enmascarando, principalmente a cualquier tercera persona, la operación de escritura en memoria no volátil correspondiente al paso al fin de la vida útil, lo que impide en la práctica cualquier ataque por canal oculto.

De acuerdo con esta técnica, el enmascaramiento de cualquier escritura de una variable del estado del paso al fin de la vida útil en la memoria no volátil de un dispositivo electrónico se obtiene por dilución de esta operación de escritura en el desarrollo normal del programa de aplicación ejecutado por el dispositivo electrónico.

En la práctica, la operación de escritura de una variable en la memoria no volátil está siempre constituida por dos fases sucesivas: una fase de borrado, que lleva a la variable a tomar un valor vacío (por “valor vacío”, se entiende un valor por defecto predefinido y sobre el cual un usuario de la memoria no volátil no tiene influencia, tal como “00”, “FF” u otro), y después una fase de operación propiamente dicha, en el curso de la cual un valor no vacío (es decir, un valor distinto del valor vacío) es aplicado a la variable en el espacio que le está dedicado en el seno de la memoria no volátil. La escritura de una variable de estado del paso al fin de la vida útil en la memoria no volátil de un dispositivo electrónico, tal como se ha previsto en la técnica anterior mencionada anteriormente, no escapa a esta regla.

Pues bien, cada una de las fases de borrado y de escritura que constituyen la operación de escritura de una variable en la memoria no volátil necesita un cierto tiempo de tratamiento y genera un cierto consumo eléctrico, aproximadamente similar en los dos casos.

A la vista de esta técnica anterior, un objeto de la presente invención es mejorar los rendimientos, manteniendo el nivel de seguridad aportado por el enmascaramiento del paso al fin de la vida útil.

Para ello, la invención propone un procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico que comprende un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil reprogramable que contiene una variable de estado del paso al fin de la vida útil del dispositivo electrónico gestionada por un módulo de control y un puerto de entrada / salida. Este procedimiento comprende las etapas siguientes:

- cargar en la memoria viva, a partir de la citada memoria no volátil, el valor de la citada variable de estado del fin de la vida útil; y, previamente a la ejecución de cualquier orden común para el citado microprocesador:

- verificar el valor de la citada variable de estado del fin de la vida útil memorizada en la memoria viva; y, en caso de valor vacío (es decir, un valor por defecto predefinido para la memoria no volátil): ejecutar las operaciones de paso al fin de la vida útil del dispositivo electrónico; si no, la

citada variable de estado del fin de la vida útil memorizada en la memoria viva que tiene un valor no vacío (es decir, un valor distinto del valor vacío):

- continuar la inicialización y/o la ejecución de la orden común por parte del microprocesador del dispositivo electrónico; y, cuando se detecta un ataque de intromisión:
- proceder a una escritura, en la única memoria viva, de la citada variable de estado del fin de la vida útil del dispositivo electrónico y continuar la inicialización y/o la ejecución de la orden común; y
- proceder a un borrado único de la variable de estado del fin de la vida útil en la citada memoria no volátil de manera diferida para efectuarlo en lugar de una próxima operación de actualización (borrado y/o escritura) en la memoria no volátil.

El hecho de diferir la actualización de la variable de estado del fin de la vida útil en la citada memoria no volátil permite un enmascaramiento eficaz del paso al fin de la vida útil del dispositivo electrónico, puesto que una persona deshonesta no es capaz de distinguir la solicitación de corriente generada por esta actualización de la variable de estado del fin de la vida útil de la generada por el microprocesador del dispositivo electrónico. Se obtiene así un nivel de seguridad del mismo orden que en los documentos FR 07 08242 y PCT/FR2008/052106.

Además, el hecho de proceder a un “borrado único”, es decir a una fase de borrado no seguida por una fase de escritura, de la variable de estado del fin de la vida útil permite limitar el tiempo de tratamiento y el consumo eléctrico necesarios, por ejemplo, en un factor de aproximadamente 2. Los rendimientos durante la ejecución de un programa de aplicación por parte del dispositivo electrónico son así enormemente mejorados.

De acuerdo con modos de realización ventajosos que pueden ser combinados de cualquier manera que se pueda idear, el procedimiento puede además presentar todas o parte de las características que siguen.

Para un conjunto de órdenes ejecutadas por el microprocesador del dispositivo electrónico que incluye órdenes que comprenden una operación sistemática en la memoria no volátil y órdenes que no comprenden ninguna operación en la memoria no volátil, el procedimiento puede comprender además, independientemente de la detección o de la no detección de un ataque de intromisión, ejecutar un borrado único en la memoria no volátil de una variable ficticia. Esto permite enmascarar aún más el borrado de la variable de estado del fin de la vida útil del dispositivo electrónico en la memoria no volátil, introduciendo borrados “de señuelo” con una firma eléctrica similar. Una persona deshonesta puede así de manera aún más difícil identificar el borrado de la variable de estado del fin de la vida útil, a partir sólo de la solicitación de corriente que genera.

El borrado único en la memoria no volátil de la variable ficticia puede ser ejecutado en una misma página de la memoria que la de la variable de estado del fin de la vida útil.

El borrado único en la memoria no volátil de la variable ficticia puede ser ejecutado previamente a cualquier ejecución de operación de transmisión de datos sobre la línea del puerto de entrada / salida del dispositivo electrónico.

Consecutivamente a cualquier borrado único en la memoria no volátil de la variable de estado del fin de la vida útil, una etapa que consiste en verificar si es un valor vacío el valor de la variable de estado del fin de la vida útil, y, si se verifica este valor vacío, una etapa de ejecución de las operaciones de paso al fin de la vida útil del dispositivo electrónico.

Si se verifica que el valor de esta variable de estado del fin de la vida útil es un valor vacío, el citado borrado único en la memoria no volátil de la variable ficticia puede ser sustituido por un borrado único en la memoria no volátil del valor de la variable de estado del fin de la vida útil.

Si se detecta un error de ejecución temporal de una instrucción distinta de un ataque de intromisión que no justifica un paso al fin de la vida útil del dispositivo electrónico, el citado procedimiento puede incluir además:
la actualización mediante incrementación de un contador de error en la memoria viva;
la comparación del valor de conteo de errores con un valor de umbral; y, si el citado valor de conteo de errores sobrepasa el citado valor de umbral:
la escritura en la memoria viva del valor de la citada variable de estado del fin de la vida útil del dispositivo electrónico y el paso al fin de la vida útil del dispositivo electrónico.

La invención propone también un dispositivo electrónico que comprende un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil reprogramable que contiene una variable de estado del fin de la vida útil del dispositivo electrónico gestionada por un módulo de control y un puerto de entrada / salida (I/O – Input/Output, en inglés). El módulo de control incluye un módulo de programa de ordenador de ejecución de las etapas del procedimiento objeto de la invención citadas anteriormente.

La invención propone además un producto de programa de ordenador memorizado sobre un soporte de memorización y que incluye una serie de instrucciones ejecutables mediante un ordenador o mediante el

microprocesador de un dispositivo electrónico. Durante la ejecución de las citadas instrucciones, el citado programa ejecuta las etapas del procedimiento mencionado anteriormente.

El procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico y el dispositivo electrónico que incluye un módulo de control correspondiente, objetos de la invención, encuentran aplicaciones en cualquier tipo de dispositivo electrónico, pero, de manera preferencial no limitativa, en dispositivos electrónicos tales como las tarjetas con microprocesadores que tratan y/o que almacenan datos personales, privados o secretos.

Se comprenderán mejor con la lectura de la descripción y con la observación de las figuras que siguen, en las cuales:

- la figura 1a representa, a título puramente ilustrativo, un organigrama de etapas de puesta en práctica del procedimiento de acuerdo con un modo de realización de la invención;
- la figura 1b representa, a título puramente ilustrativo un cronograma de etapas ejecutadas en el curso de la puesta en práctica del procedimiento ilustrado en la figura 1a;
- las figuras 1c a 1f representan, a título puramente ilustrativo, detalles ventajosos de puesta en práctica de las etapas del procedimiento ilustrado en la figura 1a;
- la figura 2 representa, a título puramente ilustrativo, en forma de esquema funcional, la arquitectura de un dispositivo electrónico provisto de un módulo de control del paso al fin de la vida útil de acuerdo con un modo de realización de la presente invención.

Se proporcionará ahora una descripción más detallada del procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico, de acuerdo con un modo de realización de la presente invención, en conjunción con las figuras 1a a 1f.

De una manera general, se indica que el procedimiento de enmascaramiento del paso al fin de la vida útil de una tarjeta electrónica, objeto de la presente invención, se aplica a cualquier dispositivo electrónico que comprenda un microprocesador, una memoria viva, una memoria muerta y una memoria no volátil reprogramable que contiene una variable de estado del fin de la vida útil del dispositivo electrónico, gestionada mediante un módulo de control. De manera más particular, el dispositivo electrónico puede comprender igualmente un puerto de entrada / salida que permite el intercambio de datos ya sea con un aparato anfitrión o incluso en la red, por ejemplo. La noción de memoria no volátil reprogramable cubre las memorias reprogramables electrónicamente, las memorias EEPROM, las memorias flash, por ejemplo.

El aparato electrónico citado anteriormente, durante su funcionamiento, ejecuta una fase de arranque, denotada ATR (Answer To Reset, en inglés), y después órdenes comunes sucesivas, denotadas COM.

Se comprende, en particular, que el dispositivo electrónico correspondiente puede ventajosamente estar constituido por cualquier tarjeta con microprocesadores, por ejemplo.

En referencia a la figura 1a, el procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico comprende una etapa A que consiste en cargar en una memoria viva del dispositivo electrónico, a partir de la memoria no volátil de este último, el valor denotado FdV_E de la variable de fin de la vida útil memorizada en la memoria no volátil.

La operación correspondiente a la etapa A se denota:

$$FdV_E \longrightarrow FdV_R .$$

En la relación precedente, FdV_R designa el valor de la variable de fin de la vida útil del dispositivo electrónico cargada en la memoria viva.

Debe observarse que, en el caso particular en el que la variable de fin de la vida útil FdV_E memorizada en la memoria no volátil tenga un valor vacío, es decir, un valor por defecto predefinido, por ejemplo a continuación de un borrado único de un valor precedentemente almacenado para cierta variable, la variable de estado del fin de la vida útil FdV_R del dispositivo electrónico cargada en la memoria viva tendrá ventajosamente el mismo valor vacío. En variante, un valor dado no vacío, es decir, distinto del valor vacío, podría ser aplicado a la variable FdV_R cuando la variable FdV_E tiene un valor vacío. Este valor dado puede por ejemplo ser el valor “verdadero” (u “OK”) o cualquier otro valor determinado. En este último caso, la carga en la memoria viva del valor de la variable de estado del fin de la vida útil memorizada en la memoria no volátil se acompaña así de un cambio de valor (o de una aplicación de valor para pasar de un valor vacío a un valor dado no vacío).

A continuación de la etapa A de la figura 1a, y previamente a la ejecución de cualquier orden común COM por parte del microprocesador, el procedimiento consiste entonces, en una etapa B, de verificar el valor de la variable de

estado del fin de la vida útil memorizada en una memoria viva. Esta verificación puede por ejemplo consistir en verificar la existencia de un valor para FdV_R, es decir, en verificar si FdV_R tiene o no un valor vacío. En el caso mencionado anteriormente en el que FdV_R tomaría un valor dado no vacío cuando FdV_E tiene un valor vacío, por ejemplo el valor “verdadero” (u “OK”), la citada verificación podría consistir en comparar el valor de FdV_R con este valor dado no vacío, o por el contrario con un valor distinto de este valor dado no vacío. En la etapa B del ejemplo no limitativo ilustrado en la figura 1a, la verificación está representada por una etapa de prueba:
FdV_R = ø?

En esta relación, ø representa el valor vacío, tal como el definido más arriba, de la variable de estado del fin de la vida útil del dispositivo electrónico memorizado en la memoria viva.

Si la respuesta es positiva en la prueba de la etapa B, el procedimiento consiste en ejecutar C las operaciones de paso al fin de la vida útil del dispositivo electrónico.

Por el contrario, si la respuesta es negativa en la prueba ejecutada en la etapa B, teniendo la variable de estado del fin de la vida útil memorizada en una memoria viva FdV_R un valor no vacío, el procedimiento consiste en continuar la inicialización y/o la ejecución de la orden común COM por parte del microprocesador del dispositivo electrónico. Se indica que la ejecución de la orden común corresponde a cualquier orden de una aplicación ejecutada por el dispositivo electrónico.

En el curso de esta ejecución y mediante la detección, en una etapa E, de un ataque de intromisión, el procedimiento consiste, en una etapa F, en proceder a una escritura en la única memoria viva de la variable de estado del fin de la vida útil del dispositivo electrónico, la variable FdV_R, y en continuar la inicialización y/o la ejecución de la orden común COM. La escritura de la variable FdV_R conduce a esta última a tomar el valor vacío definido anteriormente (es decir, el valor por defecto predefinido para la memoria no volátil), o bien un valor dado no vacío tal como el valor “verdadero” (u “OK”).

En la etapa F del ejemplo no limitativo ilustrado en la figura 1a operación de escritura se denota mediante la relación:
FdVR = ø.

En la relación precedente, se indica que el valor ø designa el valor vacío definido anteriormente.

Finalmente la etapa F citada anteriormente de escritura en la memoria viva es seguida por una etapa G que consiste en proceder a un borrado único de la variable de estado del fin de la vida útil FdV_E en la memoria no volátil de manera diferida para efectuarlo en lugar de una próxima operación de actualización (borrado y/o escritura) en la memoria no volátil. Esto permite enmascarar la modificación operada sobre la variable de estado del fin de la vida útil. Se impide así que una persona deshonesta distinga esta operación, claramente y a tiempo, de una operación de actualización normal realizada en la memoria no volátil, por ejemplo en el marco de una orden clásica.

Por “borrado único”, se entiende una fase de borrado del valor almacenado para la variable FdV_E considerada, que lleva a la citada variable a tomar el valor vacío tal como el definido anteriormente, no siendo esta fase de borrado seguida por una fase de escritura en el curso de la cual un valor no vacío, es decir, distinto del valor vacío, sería aplicado a la citada variable en el espacio que se le dedica en el seno de la memoria no volátil. Dicho de otro modo, en el caso de un borrado único de la variable FdV_E, esta última es almacenada en una memoria no volátil con el valor vacío. Tal valor vacío se distingue por consiguiente de un valor no vacío, incluso particular, porque no necesita ninguna fase de escritura.

Por el hecho de la puesta en práctica de un borrado único de la variable de estado del fin de la vida útil FdV_E, el tiempo de tratamiento y el consumo eléctrico generado por este borrado se reducen con relación a una situación en la que la variable de estado del fin de la vida útil FdV_E sería objeto de una escritura en la memoria no volátil. En efecto, se ahorra el tiempo de tratamiento y el consumo eléctrico que estarían asociados a una fase de escritura. A título ilustrativo, este ahorro puede ser estimado en una reducción del tiempo de tratamiento y del consumo eléctrico en un factor de aproximadamente 2 con relación a la situación descrita en los documentos FR 07 08242 y PCT/FR2008/052106.

La etapa G citada anteriormente está por ejemplo seguida de un retorno en la ejecución de la orden común siguiente por medio de la etapa H. En la etapa citada anteriormente, COM + 1 designa la orden común.

Como se representa en la figura 1a, se efectúa un retorno a la etapa B para la simple ejecución de la orden siguiente.

Sin embargo, de acuerdo con otra posibilidad de puesta en práctica del procedimiento, el retorno puede ser efectuado, así como representado en línea discontinua en la figura 1a, aguas arriba de la carga ejecutada en la etapa A, para la renovación del proceso de carga en la memoria viva del valor de la variable de estado del fin de la vida útil FdV_E de manera sistemática. Tal proceso no es sin embargo indispensable, sino que puede ser puesto en práctica en variante.

En la figura 1b, se ha representado un cronograma de las operaciones de ejecución de las etapas de la figura 1a.

En particular, la etapa A puede ser ejecutada en el arranque ATR o previamente a la ejecución de cada orden COM, como se ha mencionado anteriormente.

La prueba de la etapa B es ejecutada previamente a la continuación con el arranque o la ejecución de la orden común representada con rayado a izquierdas en la figura 1a. Se recuerda que la respuesta positiva en la prueba de la etapa B conduce automáticamente al paso al fin de la vida útil del dispositivo electrónico en la etapa C.

La continuación con el arranque o la inicialización o incluso la ejecución de la orden común en la etapa D corresponde de hecho a la puesta en práctica de procesos algorítmicos que manipulan secretos para el dispositivo electrónico, cuando este último está constituido por una tarjeta de microprocesadores por ejemplo.

La prueba de la etapa E correspondiente a una prueba de detección de ataque de intromisión puede ser puesta en práctica de manera clásica ya sea mediante la ejecución de mecanismos anti-DFA (Differential Fault Analysis, en inglés), procedimiento de ataque que consiste en introducir un error en un tratamiento para deducir informaciones sobre los datos tratados) ya sea mediante procesos de verificación de la integridad de los datos por ejemplo.

La etapa de escritura, en la única memoria viva, de la variable de estado del fin de la vida útil del dispositivo electrónico, etapa F, es ejecutada por el módulo de control del paso al fin de la vida útil del dispositivo electrónico y opera mediante escritura de esta variable de estado de acuerdo con la relación anteriormente mencionada:
$FdV_R = ø$.

La etapa G consistente en el borrado único de la variable de estado del fin de la vida útil FdV_E en una memoria no volátil, es decir, con mucha frecuencia en una memoria EEPROM, es entonces ejecutada de manera diferida, es decir, en lugar de una próxima actualización (borrado y/o escritura) que se va a efectuar en la orden común o en una orden ulterior.

En la figura 1b, esta operación está representada por un pico rayado a derechas que ilustra el aumento de la intensidad de corriente consumida por la memoria citada anteriormente por razones de la operación de borrado único en la memoria citada anteriormente.

La etapa E es entonces seguida de una etapa de retorno ya sea a la etapa B, ya sea a la etapa A, como se ha descrito anteriormente en conjunción con la figura 1a.

Como se ha representado además en la figura 1c, se considera cualquier conjunto de órdenes ejecutadas por el microprocesador del dispositivo electrónico que incluyen órdenes (COM_W) que comprenden una operación sistemática en la memoria no volátil y órdenes $(\overline{COM_W})$ que no comprenden ninguna operación en la memoria no volátil. En esta hipótesis, el procedimiento comprende además, independientemente de la detección o de la no detección de un ataque de intromisión, la ejecución de un borrado único D_2 en la memoria no volátil de una variable ficticia, la cual se denota como VF. Esta variable ficticia puede consistir en cualquier variable almacenada en la memoria no volátil y distinta de la variable de estado del fin de la vida útil FdV_E del dispositivo electrónico. Esto permite enmascarar aún más cualquier borrado eventual de la variable de estado del fin de la vida útil del dispositivo electrónico en la memoria no volátil. En efecto, una persona deshonesta no es fácilmente capaz de distinguir el borrado de la variable de estado del fin de la vida útil y el borrado de una variable ficticia, teniendo estos dos tipos de borrado firmas eléctricas próximas, incluso idénticas.

Preferentemente, el borrado único de la variable ficticia VF es ejecutado en la misma página de memoria que la de la variable de estado del fin de la vida útil.

En la etapa D_2 representada en la figura 1c, la operación de borrado en la misma memoria de página está representada por la relación:
$WAP(VF) = WAP(FdV_E)$.

En la relación precedente, WAP designa la dirección de la página de la memoria de borrado.

La etapa D_2 está seguida por la llamada de la etapa E de la figura 1a.

Además, como se ha representado en la misma la figura 1c, el borrado único en la memoria no volátil de la variable ficticia es ejecutado previamente a cualquier operación de transmisión de datos sobre la línea del puerto de entrada / salida del dispositivo electrónico. En la figura 1c, la operación correspondiente está representada de manera simbólica por la detección de cualquier operación de entrada / salida mediante la relación:
COM = I/O?

La detección de tal operación provoca entonces el borrado sistemático e inmediato de la variable ficticia, como se ha descrito anteriormente en la descripción.

Finalmente, como se ha representado en la figura 1d, el procedimiento incluye ventajosamente, a continuación de cualquier borrado único en la memoria no volátil de la variable de estado del fin de la vida útil FdV_E tal como se representa en la etapa G1, una etapa denotada G2 que consiste en verificar, tal como se ha definido anteriormente,

si el valor de la variable de estado del fin de la vida útil FdV_R memorizada en la memoria viva es un valor vacío. La operación correspondiente a la etapa citada anteriormente se denota de acuerdo con la relación:ppp

FdVR = ø.

Cuando se verifica si la variable de estado del fin de la vida útil FdV_R tiene un valor vacío, se efectúa una etapa de ejecución de las operaciones de paso al fin de la vida útil del dispositivo electrónico mediante llamada a la etapa C representada en la figura 1a.

Por el contrario, en ausencia de verificación de si la variable de estado del fin de la vida útil FdV_R tiene un valor vacío, se efectúa un retorno a la etapa H.

Además, como se ha representado igualmente en la figura 1e, mediante la verificación en la etapa D_{21} de si el valor de la variable de estado del fin de la vida útil FdV_R es un valor vacío, ya sea mediante respuesta positiva a la prueba D_{21} citada anteriormente, en la operación de borrado único en la memoria no volátil de la variable ficticia VF, representada en la etapa D_{22} de la figura 1e, se sustituye el borrado único en la memoria EEPROM del valor de la variable de estado del fin de la vida útil FdV_E mediante la llamada a la etapa G de la figura 1a.

El procedimiento permite además ventajosamente la puesta en práctica de un contador de errores.

De una manera general la actualización de un contador de errores es sometida a la misma restricción que la actualización de una variable de fin de la vida útil.

Debido al hecho de que se trata de una escritura en la memoria no volátil, de tipo EEPROM, tal escritura es normalmente detectable debido a la mayor intensidad consumida por esta última en el curso de la operación de escritura.

El procedimiento puede por consiguiente permitir de manera ventajosa, en el caso de detección de errores que no justifican un paso directo al fin de la vida útil, la implementación de un contador antes de efectuar el borrado normal. El valor de ese contador es a continuación regularmente verificado y cuando se sobrepasa un nivel de umbral permite desencadenar un paso al fin de la vida útil.

Tal modo de operación está representado en la figura 1f, de la manera siguiente:

-- mediante la detección I_1 de un error de ejecución temporal de una instrucción, distinta de un ataque de intromisión y que no justifica un paso al fin de la vida útil del dispositivo electrónico, designándose la detección del error temporal como ∃ TE?, donde TE designa el error de ejecución temporal citado anteriormente, la respuesta positiva en la prueba I_1 llama a una etapa I_2 de actualización por implementación de un contador de errores en la memoria viva. El valor actualizado en la etapa I_2 representada por la relación:
TE = TE + 1 es entonces seguida por una etapa de comparación I_3 del valor de conteo de los valores actualizados a un valor de umbral, denotado STE.

En la etapa de prueba I_3 la operación de comparación se denota:
TE > STE?

Cuando de sobrepasa el valor de umbral por parte del valor de conteo de errores actualizado, es decir cuando se produce una respuesta positiva a la prueba I_3, la escritura en la memoria viva del valor de la variable de estado del fin de la vida útil del dispositivo electrónico y el paso al fin de la vida útil son efectuados mediante la llamada a la etapa F y después la etapa G, como se representa en la figura 1f.

Un dispositivo electrónico que comprende un microprocesador denotado 1_1, una memoria viva denotada 1_2, una memoria no volátil de tipo EEPROM por ejemplo, denotada 1_3, y una memoria muerta denotada 1_4 es ahora descrita en conjunción con la figura 2. Además, como se ha representado en la figura citada anteriormente, el dispositivo comprende un puerto de entrada / salida denotado I/O (Input / Output, en inglés).

Como se ha representado en la figura 2, el dispositivo electrónico en funcionamiento comprende una variable de estado del fin de la vida útil de este dispositivo electrónico, denotada FdV_E, gestionada por un módulo de control CM, el cual puede por ejemplo ser un módulo lógico implantado en la memoria muerta 1_4.

El módulo de control CM incluye un módulo de programas de ordenador SCM que permite la ejecución de las etapas del procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico, como se han descrito anteriormente en conjunción con las figuras 1a a 1f.

Debe entenderse que el módulo de programa de ordenador SCM puede ser implantado en la memoria no volátil de tipo EEPROM, la cual constituye un soporte de memorización. Este módulo de programa de ordenador incluye una serie de instrucciones ejecutables por el microprocesador del dispositivo electrónico y, durante la ejecución de las instrucciones citadas anteriormente, ejecuta las etapas de puesta en práctica del procedimiento, tal como se ha descrito precedentemente en conjunción con cualquier parte de las figuras 1a a 1f.

El procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico, objeto de la invención, ha sido puesto en práctica en tarjetas electrónicas. Estas pruebas muy complejas ejecutadas sobre estas tarjetas electrónicas por entidades de confianza independientes no tienen permiso de impedir el paso al fin de la vida útil de estas tarjetas electrónicas, contrariamente a las tarjetas electrónicas provistas de un proceso de paso al fin de la vida útil clásico, para las cuales es posible repetir ataques de intromisión hasta la puesta en evidencia de un fallo aprovechable. En consecuencia, resulta que el procedimiento objeto de la invención no permite ya diferenciar a tiempo el caso en el que un ataque ha sido detectado y va por consiguiente a conllevar un paso al fin de la vida útil del dispositivo electrónico, del caso en el que el ataque no ha sido detectado o no ha producido ningún efecto.

REIVINDICACIONES

1. Procedimiento de enmascaramiento del paso al fin de la vida útil de un dispositivo electrónico que comprende un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil reprogramable que contiene una variable de estado del fin de la vida útil del dispositivo electrónico gestionada por un módulo de control y un puerto de entrada / salida, comprendiendo el citado procedimiento las etapas siguientes:

- cargar (A) en la memoria viva, a partir de la citada memoria no volátil, el valor (FdV_E) de la citada variable de estado del fin de la vida útil; y, previamente a la ejecución de cualquier orden común por el citado microprocesador;

- verificar (B) el valor de la citada variable de estado del fin de la vida útil memorizada en la memoria viva (FdV_R); y, en caso de valor vacío: ejecutar (C) las operaciones de paso al fin de la vida útil del dispositivo electrónico; si no, teniendo la citada variable de estado del fin de la vida útil memorizada en la memoria viva (FdV_R) un valor no vacío;

- continuar (D) la inicialización y/o la ejecución de la orden común (COM) por parte del microprocesador del dispositivo electrónico; y, cuando se detecta (E) un ataque de intromisión;

- proceder a una escritura (F), en la única memoria viva, la citada variable de estado del fin de la vida útil del dispositivo electrónico (FdV_R) y continuar la inicialización y/o la ejecución de la orden común;

caracterizado por que el procedimiento comprende la etapa siguiente:

- proceder (G) a un borrado único de la variable de estado del fin de la vida útil (FdV_E) en la citada memoria no volátil de manera diferida para efectuarlo en lugar de una próxima operación de actualización en la memoria no volátil.

2. Procedimiento de acuerdo con la reivindicación 1, en el que para un conjunto de órdenes ejecutadas por el microprocesador del dispositivo electrónico (COM Є {COMW, $\overline{COM}_w$}) que incluye órdenes (COM_W) que comprenden una operación sistemática en la memoria no volátil y órdenes ($\overline{COM}_w$) que no comprenden ninguna operación en la memoria no volátil, el citado procedimiento comprende además, independientemente de la detección o de la no detección de un ataque de intromisión, la ejecución de un borrado único en la memoria no volátil de una variable ficticia, distinta de la variable de estado del fin de la vida útil del dispositivo electrónico.

3. Procedimiento de acuerdo con la reivindicación 2, en el cual el borrado único de la variable ficticia es ejecutado en una misma página de memoria que la de la citada variable de estado del fin de la vida útil.

4. Procedimiento de acuerdo con una de las reivindicaciones 2 ó 3, en el cual el borrado único en la memoria no volátil de la variable ficticia es ejecutado previamente a cualquier ejecución de operación de transmisión de datos sobre la línea del puerto de entrada / salida del dispositivo electrónico con microprocesadores.

5. Procedimiento de acuerdo con la reivindicación 4, en el cual, cuando se verifica que el valor de la citada variable de estado del fin de la vida útil (FdV_R) es un valor vacío, en el citado borrado único en la memoria no volátil de la variable ficticia es sustituido un borrado único en la memoria no volátil del valor de la variable de estado del fin de la vida útil (FdV_E).

6. Procedimiento de acuerdo con una de las reivindicaciones 2 a 5, que incluye además, a continuación de cualquier borrado único en la memoria no volátil de la variable de estado del fin de la vida útil (FdV_E), una etapa que consiste en verificar el valor vacío, el valor de la citada variable de estado del fin de la vida útil, memorizada en la memoria viva (FdV_R) y, si se verifica un valor vacío, una etapa de ejecución de las operaciones de paso al fin de la vida útil del dispositivo electrónico.

7. Procedimiento de acuerdo con una de las reivindicaciones precedentes, en el cual, mediante detección de un error de ejecución temporal de una instrucción distinta de un ataque de intromisión que no justifica un paso al fin de la vida útil del dispositivo electrónico, el citado procedimiento incluye además:
la actualización por incrementación de un contador de errores en la memoria viva;
la comparación del valor de conteo de errores con un valor de umbral; y si se sobrepasa el citado valor de umbral por parte del citado valor de conteo de errores:
la escritura en la memoria viva del valor de la citada variable de estado del fin de la vida útil del dispositivo electrónico.

8. Dispositivo electrónico que comprende un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil reprogramable, que contiene una variable de estado del fin de la vida útil del dispositivo electrónico (FdV_E) gestionada por un módulo de control y un puerto de entrada / salida, en el cual el citado módulo de control incluye un módulo de programa de ordenador (SCM) de ejecución de las etapas del procedimiento de acuerdo con una de las reivindicaciones 1 a 7.

9. Producto de programa de ordenador memorizado sobre un soporte de memorización y que incluye una serie de instrucciones ejecutables por un ordenador o mediante el microprocesador de un dispositivo electrónico, en el cual, durante la ejecución de las citadas instrucciones, el citado programa ejecuta las etapas del procedimiento de acuerdo con una de las reivindicaciones 1 a 7.

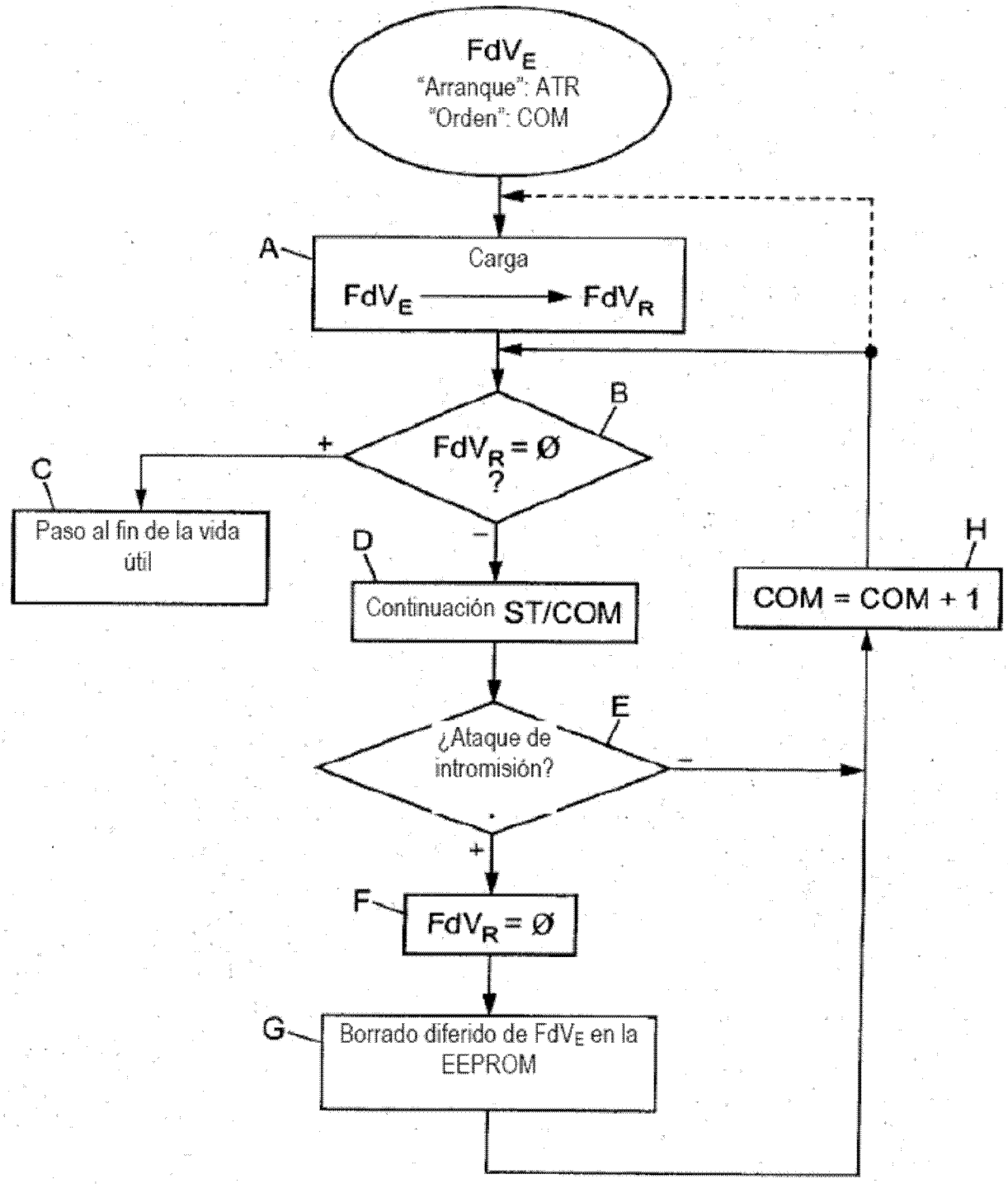
FdV_E
"Arranque": ATR
"Orden": COM
A
Carga
FdV_E → FdV_R
B
FdV_R = Ø ?
+
C
Paso al fin de la vida útil
–
D
Continuación ST/COM
E
¿Ataque de intromisión?
–
+
F
FdV_R = Ø
G
Borrado diferido de FdV_E en la EEPROM
H
COM = COM + 1

FIG. 1a

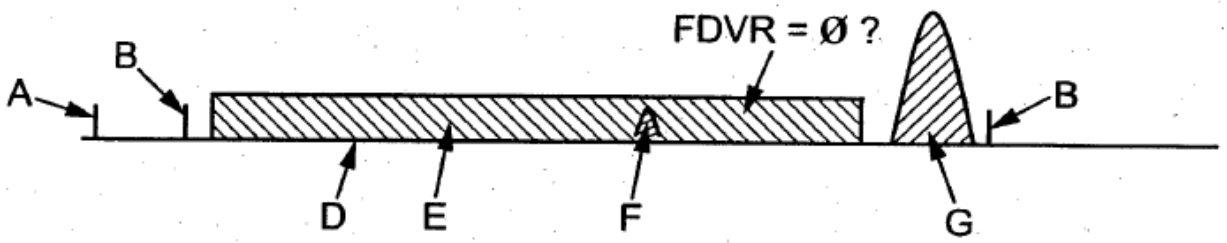
FDVR = Ø ?
A
B
B
D
E
F
G

FIG. 1b

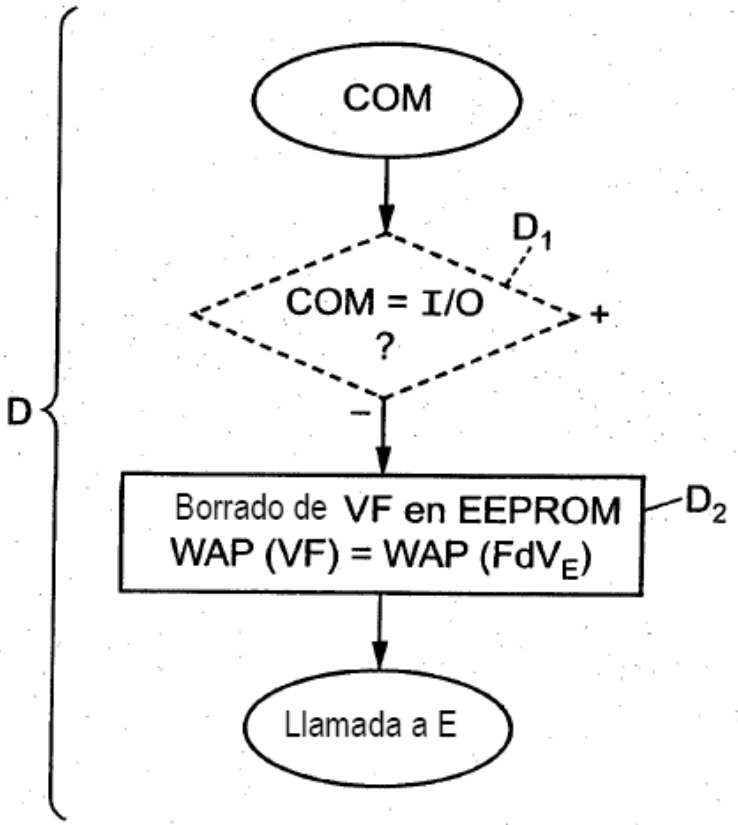
COM
D1
COM = I/O
?
+
–
D
Borrado de VF en EEPROM
WAP (VF) = WAP (FdVE)
D2
Llamada a E

FIG. 1c

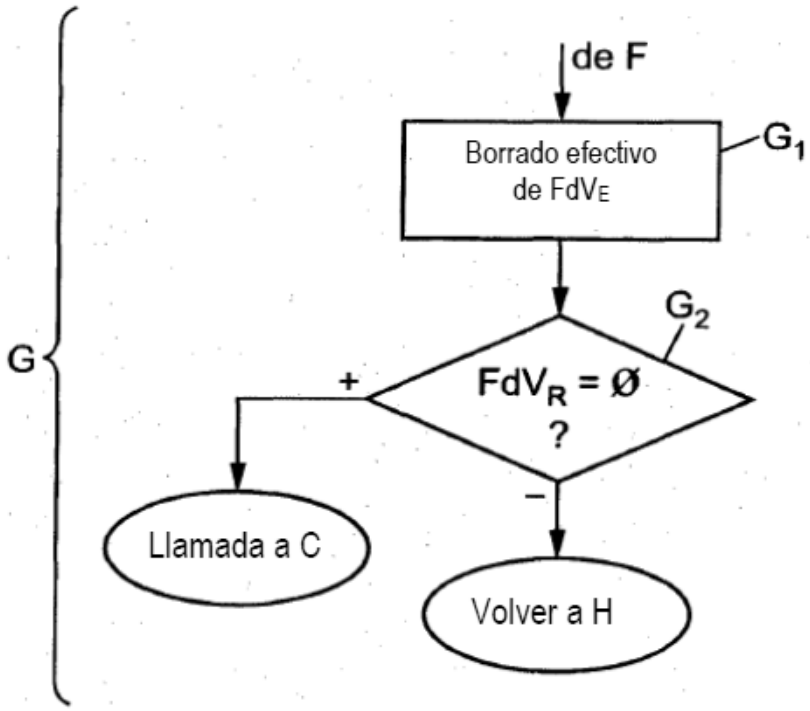
de F
Borrado efectivo de FdVE
G1
G2
FdVR = Ø ?
+
–
Llamada a C
Volver a H
G

FIG. 1d

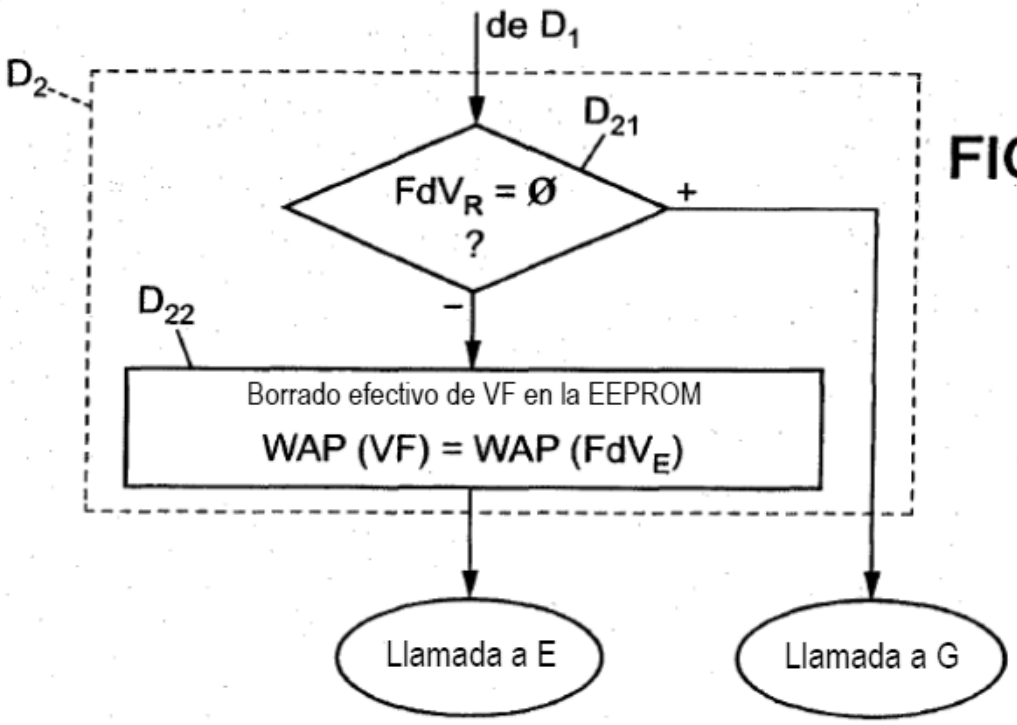
de D1
D2
D21
FdVR = Ø ?
+
–
D22
Borrado efectivo de VF en la EEPROM
WAP (VF) = WAP (FdVE)
Llamada a E
Llamada a G

FIG. 1e

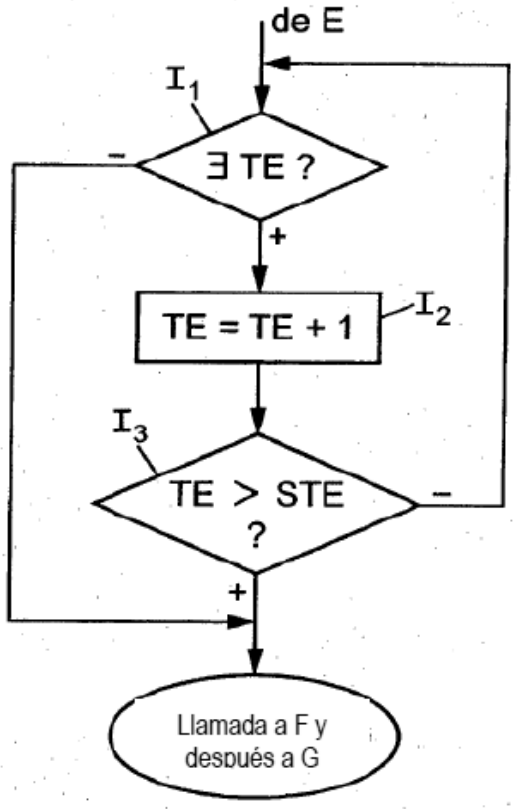
de E
I1
∃ TE ?
-
+
TE = TE + 1
I2
I3
TE > STE ?
-
+
Llamada a F y después a G

FIG. 1f

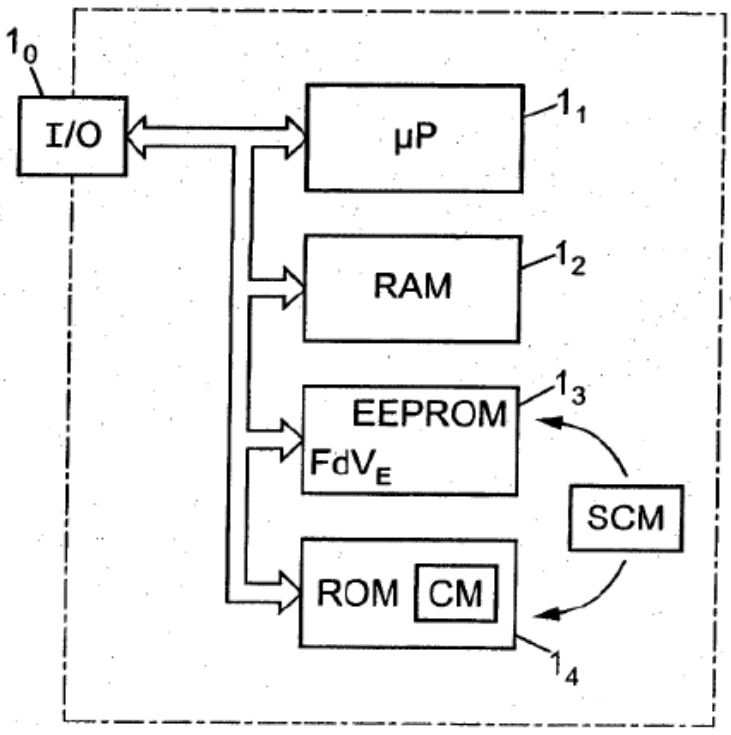
10
I/O
µP
11
RAM
12
EEPROM
FdVE
13
SCM
ROM
CM
14

FIG. 2