



(51) International Patent Classification:
G06F 12/14 (2006.01)

(21) International Application Number:
PCT/EP2019/062077

(22) International Filing Date:
10 May 2019 (10.05.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1807589.5 10 May 2018 (10.05.2018) GB

(71) Applicant: **NORDIC SEMICONDUCTOR ASA**
[NO/NO]; Otto Nielsens veg 12, 7052 Trondheim (NO).

(72) Inventors: **TALVITIE, Hannu**; C/O Nordic Semiconductor ASA, Otto Nielsens veg 12, 7052 Trondheim (NO).

WINBLAD, Marko; C/O Nordic Semiconductor ASA, Otto Nielsens veg 12, 7052 Trondheim (NO).

(74) Agent: **DEHNS**; St Bride's House, 10 Salisbury Square, London Greater London EC4Y 8JD (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH,

(54) Title: MEMORY ACCESS

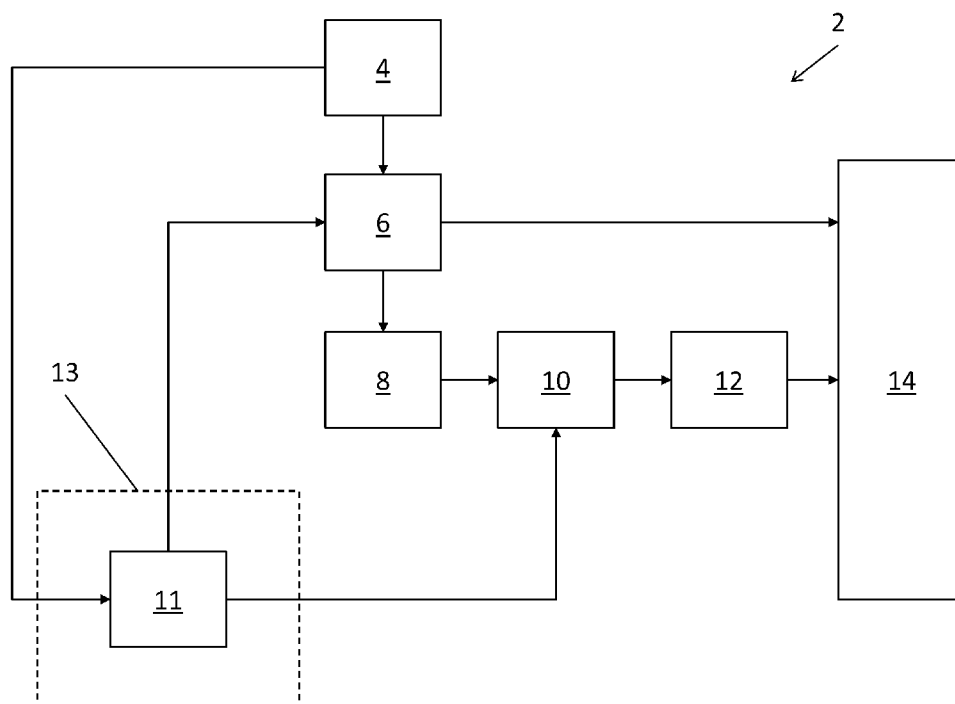


Fig. 1

(57) Abstract: An electronic device (2) comprises a processor (4) operable at a variable processor privilege level and a memory (14) comprising a secure memory area. A hardware module (8) is operable at a variable module privilege level and is arranged to access the memory directly. The secure memory area is accessible by the hardware module only when the module privilege level exceeds a threshold value. The device has a first mode of operation in which said processor privilege level is higher than said threshold value and said module privilege level is lower than said threshold value. A controller (11) is arranged, upon receiving a privilege promotion signal and the device being in the first mode, to move the device to a second mode wherein the module privilege level is higher than said threshold value.

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

Memory Access

Technical Field

5

The present invention relates to memory access, in particular to providing variable levels of privileged memory access to a hardware component, particularly a component having direct memory access, within an electronic device such as a system-on-chip device.

10

Background

In general, electronic devices are typically provided with a microprocessor, memory (volatile and/or non-volatile memory), and one or more peripheral hardware components. While such peripheral devices could, in some implementations, only have access to the memory via the microprocessor, it is preferable in some cases to provide a peripheral device with direct memory access (DMA), wherein the peripheral can access some or all addresses within the memory directly, without having to involve the microprocessor.

20

Within the electronic device, the memory may contain sensitive data, for example private encryption keys, that must be kept secure.

It is known in the art to restrict read, write or execute access to memory on a microprocessor in order to prevent unauthorised access to data or programs. Typically, certain trusted code can always gain full access to restricted and unrestricted memory areas—e.g., by causing a processor on the microprocessor to enter a privileged mode and then accessing a restricted memory area.

25

DMA-capable components may have different privilege and/or security levels (for example user mode *versus* supervisor mode; or secure mode *versus* non-secure mode) that depend on a given configuration. In order to share resources efficiently, the same component may be set to act as either a privileged bus master or an unprivileged bus master. An example of privileged bus accesses are ARM® AXI4 bus accesses, where signal "AxPROT[0]" defines bus access privilege level

30

35

- 2 -

(unprivileged / privileged) and signal "AxPROT[1]" defines bus access security level (non-secure / secure).

5 These settings may be determined statically, for example by hard-wiring the hardware component to use a particular, predetermined combination of privilege level signals. The settings may also be determined dynamically by another privileged bus master, e.g. a processor running in a secure state.

10 However, the Applicant has appreciated that conventional methods of promoting DMA-capable hardware components known in the art *per se* may be susceptible to security issues. Specifically, there may be a risk that, once the hardware component has been promoted to a privileged level such that it can access restricted memory areas, unsecure software may be able to exploit this and access the restricted memory areas that it is not supposed to.

15

Summary of the Invention

When viewed from a first aspect, the present invention provides an electronic device comprising:

- 20 a processor operable at a variable processor privilege level;
 a memory comprising a secure memory area;
 a hardware module operable at a variable module privilege level arranged to access the memory directly, wherein the secure memory area is accessible by the hardware module only when the module privilege level exceeds a threshold value;
- 25 wherein the device has a first mode of operation in which said processor privilege level is higher than said threshold value and said module privilege level is lower than said threshold value, the device further comprising a controller arranged, upon receiving a privilege promotion signal and the device being in the first mode, to move the device to a second mode wherein the module privilege level
- 30 is higher than said threshold value.

This first aspect of the present invention extends to a method of operating an electronic device, the electronic device comprising:

- 35 a processor operable at a variable processor privilege level;
 a memory comprising a secure memory area;

- 3 -

a controller; and

a hardware module operable at a variable module privilege level arranged to access the memory directly, wherein the secure memory area is accessible by the hardware module only when the module privilege level exceeds a threshold value;

5 the method comprising:

operating the device in a first mode of operation in which said processor privilege level is higher than said threshold value and said module privilege level is lower than said threshold value;

10 the controller receiving a privilege promotion signal while the device is in the first mode;

subsequently operating the device in a second mode wherein the module privilege level is higher than said threshold value.

15 This first aspect of the present invention also extends to a non-transitory computer readable medium comprising instructions that, when executed on a suitable processor, cause the processor to carry out a method of operating an electronic device, the electronic device comprising:

a processor operable at a variable processor privilege level;

a memory comprising a secure memory area;

20 a controller; and

a hardware module operable at a variable module privilege level arranged to access the memory directly, wherein the secure memory area is accessible by the hardware module only when the module privilege level exceeds a threshold value;

the method comprising:

25 operating the device in a first mode of operation in which said processor privilege level is higher than said threshold value and said module privilege level is lower than said threshold value;

the controller receiving a privilege promotion signal while the device is in the first mode;

30 subsequently operating the device in a second mode wherein the module privilege level is higher than said threshold value.

35 Thus it will be appreciated by those skilled in the art that in accordance with at least embodiments of the present invention, an improved electronic device (and associated method and non-transitory computer readable medium) is provided

- 4 -

wherein hardware components, e.g. DMA-capable hardware components, may be promoted to a privilege level sufficient to allow them to access the secure memory area as long as the processor itself has a sufficient privilege level to access the secure memory area.

5

Those skilled in the art will appreciate that the hardware module being able to access the memory 'directly' means that the hardware module can make read and/or write accesses to the memory contents without involving the processor. As outlined above, this is typically referred to in the art as 'direct memory access' or 'DMA'. This should be understood to be an entirely separate concept to having the processor or another separate module arbitrate accesses to memory based on a privilege level associated with a given request to access data.

The privilege promotion signal could be issued by an intermediate module – e.g. a dedicated module – or finite state machine which is able to take account of the processor privilege level. Preferably, however, the privilege promotion signal is provided directly by the processor to the controller.

Once the hardware module has been promoted (i.e. its privilege level has been raised above the threshold), the processor may be able to drop to a lower privilege level without affecting the operation of the promoted hardware module. Thus, for example, the processor can promote the hardware module while running privileged software and then switch to running different, unprivileged (or less privileged) software while allowing the hardware module to keep its privilege level and carry on making privileged bus accesses to the secure memory area. However, in a set of embodiments the processor cannot interact with the hardware module or change its operation while the processor privilege level is below the threshold value, i.e. when the processor is running unprivileged (or less privileged) software. This may prevent unwanted accesses to the secure memory area by unprivileged software.

30

In addition to the enhanced security outlined above, embodiments of the present invention may consume less power, respond faster, and/or require less memory accesses than conventional approaches. These advantages are achievable because the hardware module can remain in its privileged state, performing secure bus accesses, while the processor can perform an entirely different task or even go

35

- 5 -

to sleep (i.e. into a low power or idle mode), thus making better use of the resources available.

5 The hardware module may continue making privileged bus accesses to the secure memory area as long as the hardware privilege level remains sufficiently high. In some arrangements, the hardware component may maintain this privilege level indefinitely until the processor changes the privilege level of the hardware component. Thus, in a set of embodiments, the controller is further arranged such that, upon receiving a privilege demotion signal, the controller reduces the module
10 privilege level below said threshold value. Preferably the processor privilege level must be above the threshold for the privilege demotion signal to be issued.

In some potentially overlapping embodiments, the hardware module is arranged to reduce its privilege level below the threshold automatically. This may, in some
15 embodiments, be based on a timer such that the module privilege level is reduced once a predetermined period has elapsed. In some alternative embodiments, however, the module privilege level is reduced when the hardware module no longer needs to access the secure memory area. This advantageously prevents the hardware module remaining at an elevated privilege level for longer than is
20 necessary, further enhancing the security of the device.

In a set of embodiments there are two possible values that the processor privilege level can take: one above the threshold value and one below, i.e. the processor privilege level is switchable between a first processor privilege value above the
25 threshold value and a second processor privilege value below the threshold value. In an overlapping set of embodiments there are two possible values that the module privilege level can take: one above the threshold value and one below, i.e. the module privilege level is switchable between a first module privilege value above the threshold value and a second module privilege value below the threshold value.
30 In either case the respective privilege level may that be binary such that an entity can either be unprivileged or privileged.

However, one or both of the processor and module privilege levels could be set to more than two different values. Thus, in some embodiments, the processor
35 privilege level is switchable between a plurality of processor privilege values,

- 6 -

wherein at least a first of said processor privilege values is above the threshold value and at least a second of said processor privilege values is below the threshold value. Similarly, in a potentially overlapping set of embodiments, the module privilege level is switchable between a plurality of module privilege values, wherein at least a first of said module privilege values is above the threshold value and at least a second of said module privilege values is below the threshold value.

The additional privilege levels could be provided above and/or below the threshold value. Thus, in accordance with such embodiments, a hierarchical (i.e. multi-level) privilege system can be utilised and thus provide for more complex relationships between the software running on the processor and the privilege levels that can be assigned to the hardware module. This allows for more refined control over the privilege levels of the processor and hardware components. For example, normal unprivileged access may be level '0' and 'normal' privileged access may be level '1', however the processor may have secure supervisor (i.e. root or kernel mode) code that runs at a higher privilege level, e.g. at level '2', such that the supervisor may resume control over the hardware module if necessary.

Where, as set out above, additional processor and/or module privilege levels are provided, the device could be arranged such that the module privilege level can be raised above to any available value above the threshold value when the processor privilege level is at any value above the threshold value. In a set of embodiments however the module privilege level can only be raised to a value equal to or lower than the processor privilege level.

In a set of embodiments, the memory comprises a plurality of secure memory areas each being accessible by the hardware module only when the second privilege level exceeds a respective threshold value associated with said secure memory area. At least some of the respective threshold values may be different from each other. Those skilled in the art will appreciate that such embodiments provide a tiered structure where having a certain level of privilege may entitle the hardware module to access some but not all of the secure memory areas.

While having more than two possible values for the processor and module privilege levels may provide for a 'sliding scale' of privilege levels, having more than two

- 7 -

privilege values may additionally or alternatively provide a mechanism to restrict the hardware module to specific sections of the secure memory area or, in embodiments where there are multiple secure memory areas, to one or more specific secure memory areas. Thus in some embodiments, a section of the secure memory area may be accessible by the hardware module only if the module privilege level is set to a specific value. For example, the secure memory area may contain two different private encryption keys, used for unrelated applications, e.g. for two different radio protocols. These may be stored in separate sections of the secure memory area (or, where appropriate, in different secure memory areas) such that the part of memory containing the first private encryption key is accessible if the hardware module privilege level has a value '1A' and the part of memory containing the second private encryption key is accessible if the hardware component privilege level has a value '1B'. Meanwhile, if the hardware module is running at a higher privilege level, e.g. level '2', it may be able to access both parts, i.e. it could access the respective parts of the secure memory that contain each private encryption key at the same time. Other more complex hierarchies are envisioned and fall within the scope of the present invention.

Another possible application of multiple privilege levels is to allow differentiation between read and write access. Thus whilst the processor and /or module privilege levels could apply equally to reading and writing, in other embodiments for at least one of the processor and the hardware module, write access to the secure memory could be subject to a different threshold value to read access.

Brief Description of Drawings

Certain embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 is a block diagram of an electronic device in accordance with an embodiment of the present invention;

Fig. 2 is a schematic diagram of the memory in the device of Fig. 1;

Fig. 3 is a flow chart illustrating memory accesses made by the components in the device of Fig. 1; and

Fig. 4 is a flow chart illustrating a microprocessor controlling the privilege level of a DMA-capable hardware component within the device of Fig. 1.

Detailed Description

Fig. 1 is a block diagram of an electronic device 2 in accordance with an embodiment of the present invention. The device 2 comprises: a microprocessor 4; a first access control module 6; a DMA-capable hardware module 8; an access promotion module 10; a second access control module 12; and memory 14.

The memory 14 is divided into different logical areas as can be seen in Fig. 2. The memory 14 includes a number of memory registers 16, where some of these memory registers 16 collectively form a non-secure memory area 18, while others form a secure memory area 20. As will be described in further detail below, the secure memory area 20 can only be accessed by components having a certain privilege level (or greater), while the non-secure memory area 18 can be accessed by any components.

It will be appreciated that the non-secure memory area 18 is not necessarily continuous with the secure memory area 20, and there may be a separation 22 of one or more registers between these memory areas 20, 22. The memory areas 20, 22 are also not necessarily physically continuous themselves, and may be logically continuous, where each area 20, 22 is defined in memory by, for example, a look up table or other means known in the art *per se*.

For the purpose of this example, the privilege levels that a component may have are '0' or '1', i.e. low or high respectively. The non-secure memory area 18 can be accessed by a component regardless of whether its privilege level is '0' or '1', while the secure memory area 20 can be accessed only by a component having privilege level '1'.

While this example makes use of a simple binary threshold for ease of illustration, it will be appreciated that, in general, there may be many different logical areas within the memory 14 that have different minimum privilege level requirements in order to access their content. There may also be different privilege level requirements for reading and writing operations.

- 9 -

Referring back to Fig. 1, the microprocessor 4 has an associated privilege level that can be varied based on the software it is running. For example, root or kernel level operations may be associated with secure software having a higher privilege level than application level operations that are associated with non-secure software, for example software installed by a user. In the binary privilege system described above, the secure software affords the microprocessor 4 with privilege level '1' while the non-secure software affords the microprocessor 4 with only the privilege level '0'.

The microprocessor 4 accesses the memory 14 via the first access control module 6. If the microprocessor 4 is running non-secure software (and thus has the normal privilege level '0'), it can access only the non-secure memory area 18. Conversely, if the microprocessor 4 is running secure software (and thus has the elevated privilege level '1'), the microprocessor 4 can access both the non-secure memory area 18 and the secure memory area 20.

Similarly, the DMA-capable hardware module 8 also has an associated privilege level which can be varied. The DMA-capable hardware module 8 is arranged to access the memory 14 directly, i.e. without requiring any interaction with the microprocessor 4. If the DMA-capable hardware module 8 has the normal privilege level '0', it can access only the non-secure memory area 18. Conversely, if the DMA-capable hardware module 8 has the elevated privilege level '1', the DMA-capable hardware module 8 can access both the non-secure memory area 18 and the secure memory area 20.

The privilege level of the DMA-capable hardware module 8 may be controlled by the microprocessor 4. There is a controller 11 arranged to receive privilege control signals from the microprocessor 4, where these privilege control signals are used to vary the privilege level of the DMA-capable hardware module 8 by means of the first access promotion module 10. This functionality is described in further detail below with reference to Fig. 4.

The process by which checks are made when the microprocessor 4 or the DMA-capable hardware module 8 attempt to access the memory 14 is illustrated in

- 10 -

Fig. 3, which is a flow chart that shows memory accesses made by the components in the device 2 of Fig. 1.

5 Following initialisation at step 100, the component – which may be the microprocessor 4 or the DMA-capable hardware module 8 – requests access to the memory 14 at step 102. Typically the request to access the memory 14 will specify whether the component wishes to access the non-secure memory area 18 or the secure memory area 20.

10 The respective access control module 6, 12 checks the privilege level of the component (microprocessor or hardware module) 4, 8 to determine whether the privilege level is equal to or greater than the threshold for accessing the secure memory area 20 at step 104. In this particular example, as explained above, the threshold value is '1'.

15 If the privilege level of the component 4, 8 is too low, i.e. if it is '0', the component 4, 8 is granted access only to the non-secure memory area 18 at step 106. However, if the privilege level of the component 4, 8 is sufficiently high, i.e. if it is '1', the component 4, 8 is granted access to both the non-secure memory area 18 and the
20 secure memory area 20 at step 108. The process then ends 110.

As outlined above, the microprocessor 4 may generate privilege control signals in order to vary the privilege level of the DMA-capable hardware module 8. These privilege control signals are passed to a promotion control module 11 which may
25 set the privilege level of the DMA-capable hardware module 8 to a new value above the threshold for secure memory access. The new value will typically be equal to or less than a current value of the privilege level of the microprocessor 4. Fig. 4 is a flow chart illustrating the microprocessor 4 controlling the privilege level of the device 2 of Fig. 1. The promotion control module 11 exists within the 'secure world'
30 13 and so can only be accessed by secure (i.e. privileged) software.

Following initialisation at step 200, the microprocessor 4 issues a privilege control signal, indicating that it wishes to change the privilege level of the DMA-capable hardware module 8, at step 202. Typically the privilege control signal will specify
35 the privilege level that the microprocessor wishes to set the DMA-capable hardware

- 11 -

module 8 to, i.e. it may be a promotion control signal or a demotion control signal, i.e. a signal indicating that the microprocessor 4 wishes to increase or decrease the privilege level of the DMA-capable hardware module 8 respectively.

- 5 The promotion control module 11 checks the privilege level of the microprocessor 4 to determine whether it is above the threshold and may also check whether it is equal to or greater than the privilege level of the DMA-capable hardware module 8 at step 204.
- 10 If the privilege level of the microprocessor 4 is less than that of the DMA-capable hardware module 8, i.e. if the privilege level of the microprocessor is '0' and the privilege level of the DMA-capable hardware module 8 is '1', the request is ignored and the process ends 206. However, if the privilege level of the microprocessor 4 is above the threshold – i.e. greater than or equal to that of the DMA-capable
- 15 hardware module 8, the promotion control module 11, at step 208, sets the privilege level of the DMA-capable hardware module 8 to the level requested in the privilege control signal by passing a suitable control signal to the access promotion module 10 connected between the DMA-capable hardware module 8 and the second access control module 12. The process then ends 206.
- 20 Once the privilege level of the DMA-capable hardware module 8 has been raised, it may remain in its privileged state, performing secure bus accesses to the secure memory area 20. In the meantime, the processor 4 can perform an entirely different task or even go to sleep (i.e. into a low power or idle mode) and may
- 25 reduce its own privilege level below that of the DMA-capable hardware module 8.

The DMA-capable hardware module 8 can continue making privileged bus accesses to the secure memory area 20 as long as the privilege level of the DMA-capable hardware module 8 remains sufficiently high (i.e. so long as it remains '1').

- 30 The DMA-capable hardware module 8 may maintain this privilege level indefinitely, or it may reduce its privilege level automatically when it has finished with its current access to the secure memory area 20.

- 35 However, in the presently described embodiment, so long as the DMA-capable hardware module 8 is in its elevated privilege state, the processor 4 is unable to

- 12 -

revert the privilege level of the DMA-capable hardware module 8 unless its privilege level is equal to or greater than that of the DMA-capable hardware module 8. This enhances the security of the device 2 because unprivileged software is not able to gain access to the secure memory area 20 via the DMA-capable hardware module 8.

5

Thus it will be appreciated by those skilled in the art that embodiments of the present invention provide a power efficient but secure way of allowing a hardware module to access an area of secure memory. It will be appreciated by those skilled in the art that the embodiments described above are merely exemplary and are not limiting on the scope of the invention.

10

Claims

1. An electronic device comprising:
a processor operable at a variable processor privilege level;
5 a memory comprising a secure memory area;
a hardware module operable at a variable module privilege level arranged to access the memory directly, wherein the secure memory area is accessible by the hardware module only when the module privilege level exceeds a threshold value;
wherein the device has a first mode of operation in which said processor
10 privilege level is higher than said threshold value and said module privilege level is lower than said threshold value, the device further comprising a controller arranged, upon receiving a privilege promotion signal and the device being in the first mode, to move the device to a second mode wherein the module privilege level is higher than said threshold value.
15
2. The electronic device as claimed in claim 1, wherein the privilege promotion signal is provided directly by the processor to the controller.
3. The electronic device as claimed in claim 1 or 2, wherein the processor
20 cannot interact with the hardware module or change its operation while the processor privilege level is below the threshold value.
4. The electronic device as claimed in any preceding claim, wherein the controller is further arranged such that, upon receiving a privilege demotion signal,
25 the controller reduces the module privilege level below said threshold value.
5. The electronic device as claimed in claim 4, wherein the processor privilege level must be above the threshold for the privilege demotion signal to be issued.
- 30 6. The electronic device as claimed in any preceding claim, wherein the hardware module is arranged to reduce its privilege level below the threshold automatically.

- 14 -

7. The electronic device as claimed in claim 6, further comprising a timer arranged such that the module privilege level is reduced once a predetermined period has elapsed.
- 5 8. The electronic device as claimed in claim 6 or 7, wherein the module privilege level is reduced when the hardware module no longer needs to access the secure memory area.
- 10 9. The electronic device as claimed in any preceding claim, wherein the processor privilege level is switchable between a first processor privilege value above the threshold value and a second processor privilege value below the threshold value.
- 15 10. The electronic device as claimed in any of claims 1 to 8, wherein the processor privilege level is switchable between a plurality of processor privilege values, wherein at least a first of said processor privilege values is above the threshold value and at least a second of said processor privilege values is below the threshold value.
- 20 11. The electronic device as claimed in any preceding claim, wherein there the module privilege level is switchable between a first module privilege value above the threshold value and a second module privilege value below the threshold value.
- 25 12. The electronic device as claimed in any of claims 1 to 10, wherein the module privilege level is switchable between a plurality of module privilege values, wherein at least a first of said module privilege values is above the threshold value and at least a second of said module privilege values is below the threshold value.
- 30 13. The electronic device as claimed in any preceding claim, wherein the module privilege level can only be raised to a value equal to or lower than the processor privilege level.
14. The electronic device as claimed in any preceding claim, wherein the memory comprises a plurality of secure memory areas each being accessible by

- 15 -

the hardware module only when the second privilege level exceeds a respective threshold value associated with said secure memory area.

15. The electronic device as claimed in claim 14, wherein a section of the
5 secure memory area may be accessible by the hardware module only if the module privilege level is set to a specific value.

16. A method of operating an electronic device, the electronic device
comprising:
10 a processor operable at a variable processor privilege level;
a memory comprising a secure memory area;
a controller; and
a hardware module operable at a variable module privilege level arranged to
access the memory directly, wherein the secure memory area is accessible by the
15 hardware module only when the module privilege level exceeds a threshold value;
the method comprising:
operating the device in a first mode of operation in which said processor
privilege level is higher than said threshold value and said module privilege level is
lower than said threshold value;
20 the controller receiving a privilege promotion signal while the device is in the
first mode;
subsequently operating the device in a second mode wherein the module
privilege level is higher than said threshold value.

25 17. A non-transitory computer readable medium comprising instructions that,
when executed on a suitable processor, cause the processor to carry out a method
of operating an electronic device, the electronic device comprising:
a processor operable at a variable processor privilege level;
a memory comprising a secure memory area;
30 a controller; and
a hardware module operable at a variable module privilege level arranged to
access the memory directly, wherein the secure memory area is accessible by the
hardware module only when the module privilege level exceeds a threshold value;
the method comprising:

- 16 -

operating the device in a first mode of operation in which said processor privilege level is higher than said threshold value and said module privilege level is lower than said threshold value;

5 the controller receiving a privilege promotion signal while the device is in the first mode;

subsequently operating the device in a second mode wherein the module privilege level is higher than said threshold value.

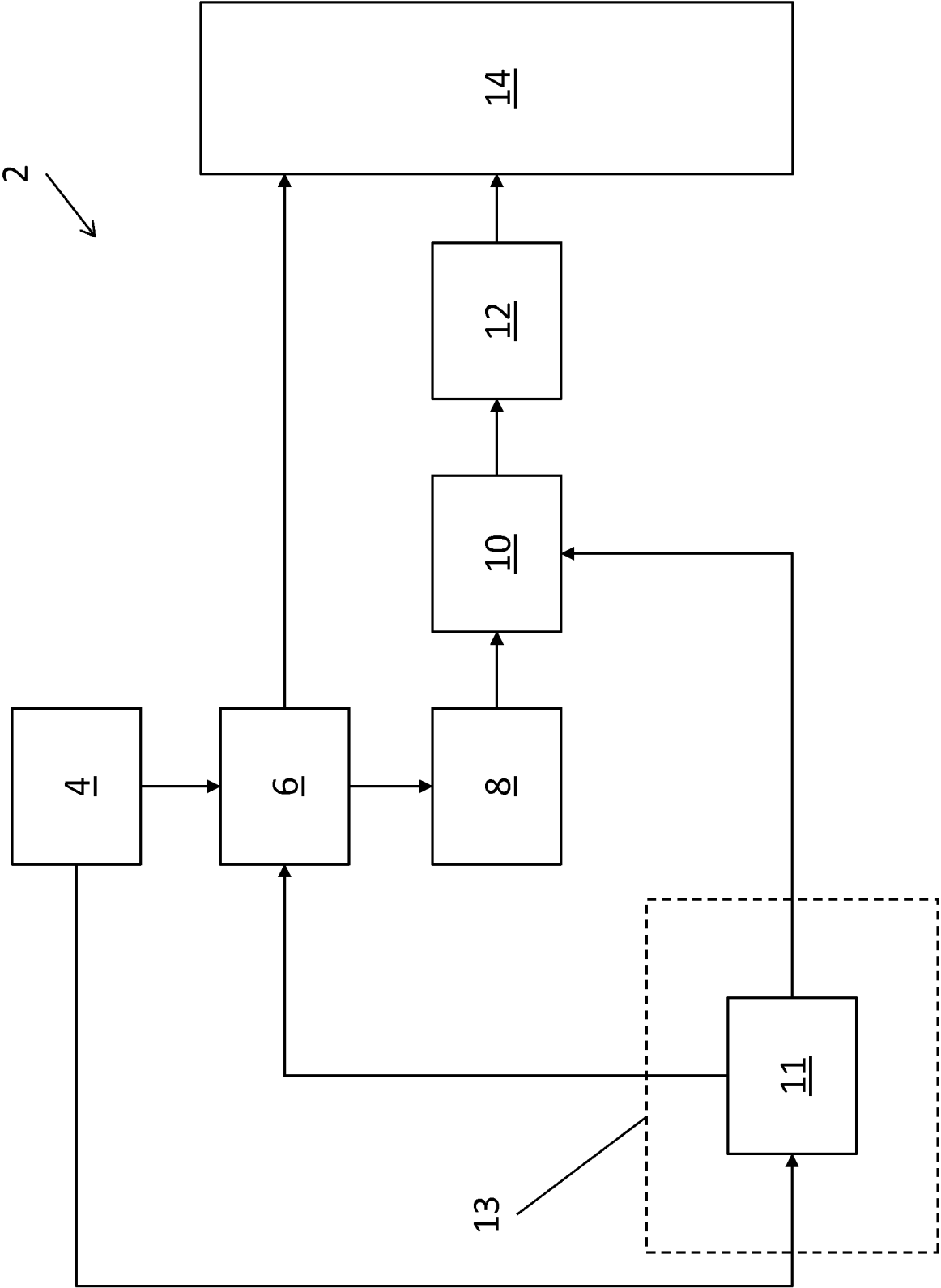


Fig. 1

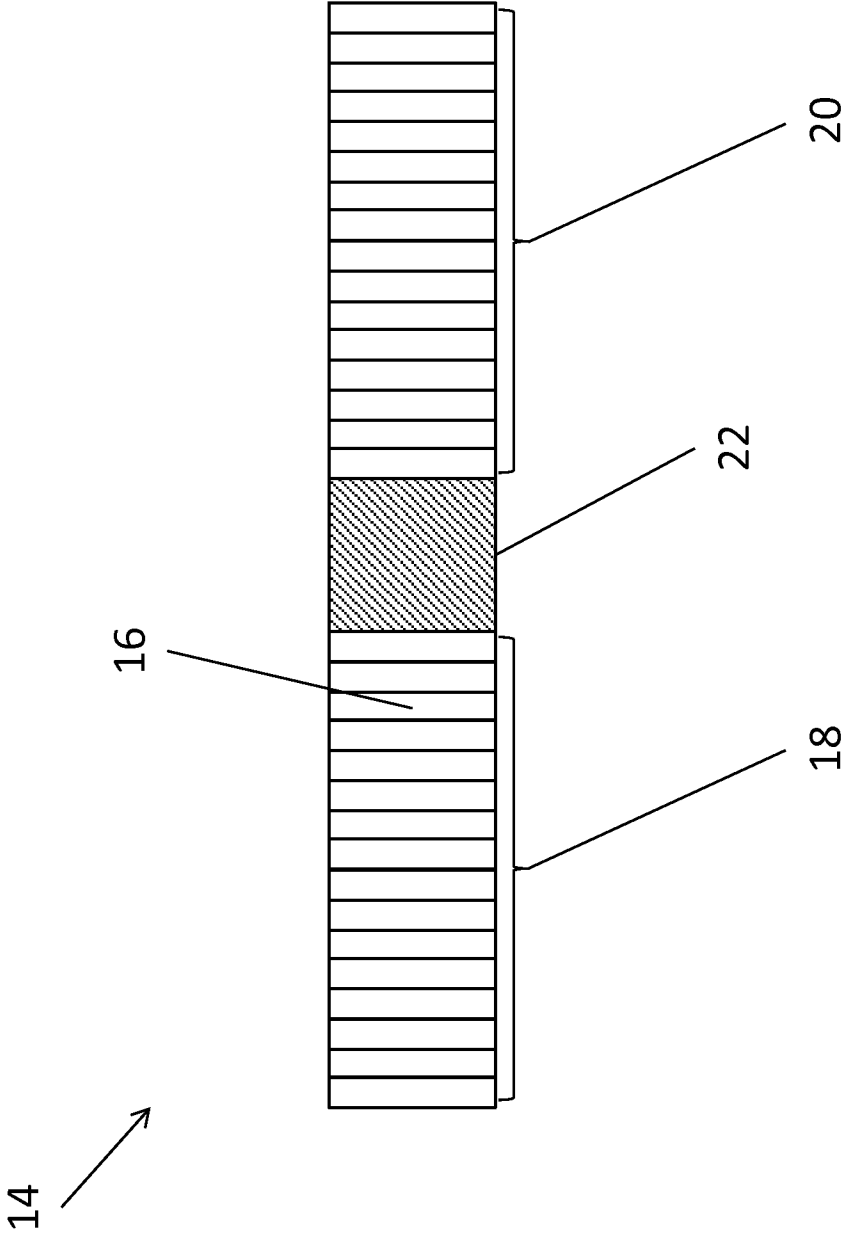


Fig. 2

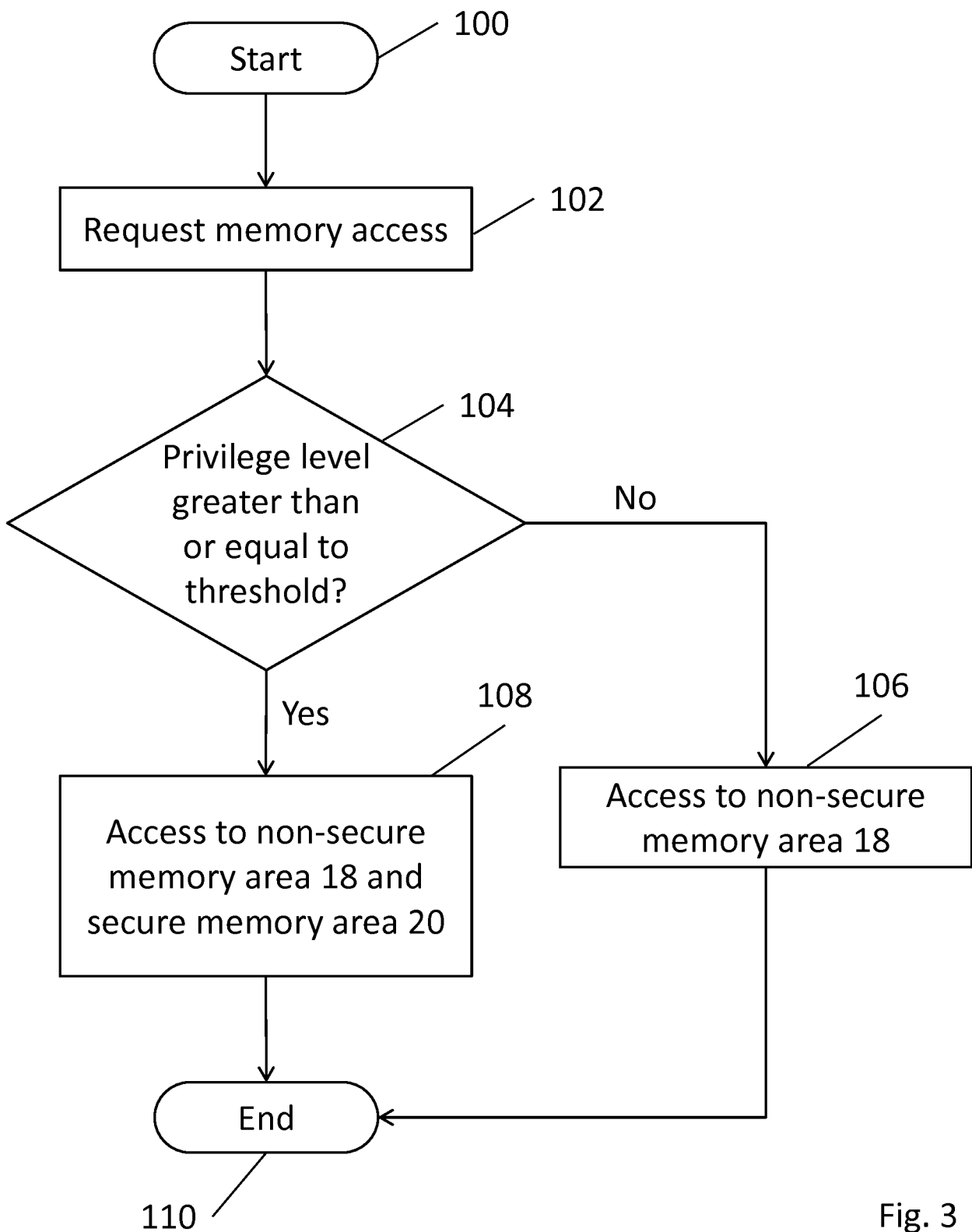


Fig. 3

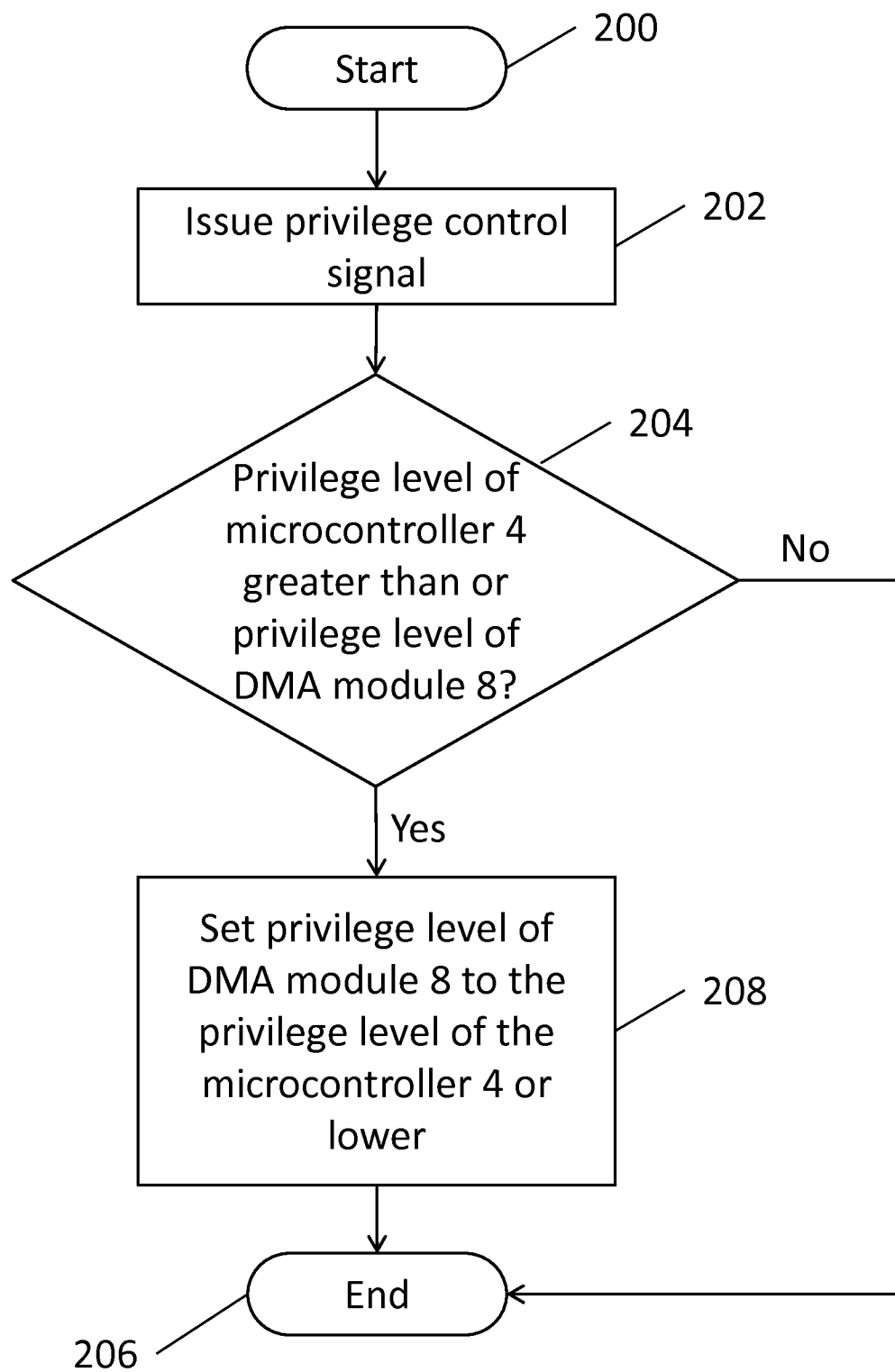


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2019/062077

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F12/14
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/177266 A1 (MOYER WILLIAM C [US] ET AL) 9 September 2004 (2004-09-09) paragraph [0013] - paragraph [0020]; claims 1-5; figures 1-4 paragraph [0025] - paragraph [0037] -----	1-17
A	US 2015/332069 A1 (CIRCELLO JOSEPH C [US] ET AL) 19 November 2015 (2015-11-19) paragraph [0041] - paragraph [0064] -----	1-17
A	US 2002/129299 A1 (MCKEE BRET A [US]) 12 September 2002 (2002-09-12) paragraph [0036] - paragraph [0043] -----	1-17



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

8 August 2019

Date of mailing of the international search report

19/08/2019

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Toader, Elena Lidia

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2019/062077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004177266 A1	09-09-2004	CN 1759557 A	12-04-2006
		EP 1604482 A2	14-12-2005
		JP 2006523347 A	12-10-2006
		KR 20050113638 A	02-12-2005
		TW 200417869 A	16-09-2004
		US 2004177266 A1	09-09-2004
		WO 2004081707 A2	23-09-2004

US 2015332069 A1	19-11-2015	US 2014259149 A1	11-09-2014
		US 2015332069 A1	19-11-2015

US 2002129299 A1	12-09-2002	DE 10206422 A1	19-09-2002
		GB 2375200 A	06-11-2002
		JP 2002268914 A	20-09-2002
		US 2002129299 A1	12-09-2002
