



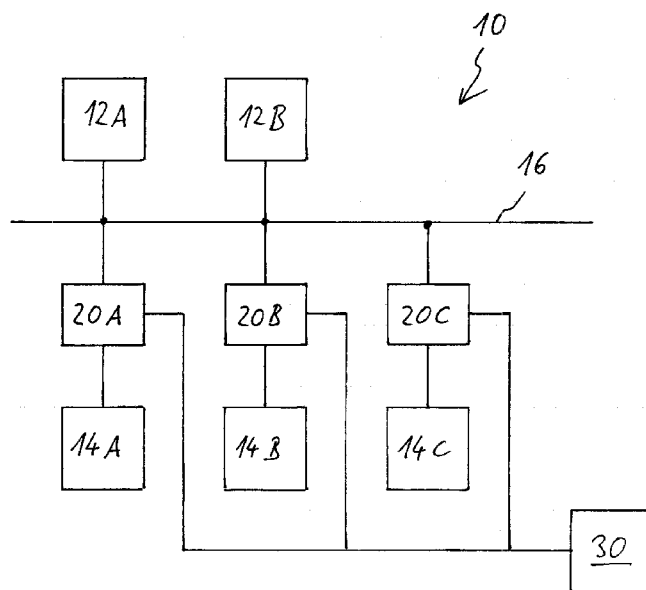
- (51) **International Patent Classification:**  
*G06F 13/38* (2006.01) *G06F 13/14* (2006.01)
- (21) **International Application Number:**  
PCT/IB2012/056675
- (22) **International Filing Date:**  
23 November 2012 (23.11.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant (for all designated States except US):** **FREESCALE SEMICONDUCTOR, INC.** [US/US]; 6501 William Cannon Drive West, Austin, Texas 78735 (US).
- (72) **Inventors; and**
- (71) **Applicants :** **ROHLDER, Michael** [DE/DE]; Kruegerstrasse 37, 85716 Unterschleissheim (DE). **KLUG-MOCANU, Carmen** [RO/DE]; Thomastrasse 34, 85653 Aying (DE). **KRUECKEN, Joachim** [DE/DE]; Felicitas-Füss-Straße 29, 81827 Munich (DE).
- (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, 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, ML, MR, NE, SN, TD, TG).

**Published:**

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

(54) **Title:** DIGITAL DEVICE**Fig. 1**

(57) **Abstract:** A digital device (10) comprising one or more requestor units (12A, 12B), one or more responder units (14A, 14B, 14C), and a bus (16) is described. Each responder unit (14A, 14B, 14C) is connected to the requestor units (12A, 12B) via the bus (16). Each responder unit (14A, 14B, 14C) comprises a plurality of responder elements (18\_1—18\_9) which are accessible by the requestor units (12A, 12B) via the bus (16) and which include one or more critical responder elements (18\_1, 18\_2, 18\_5). The digital device (10) further comprises one or more wrapper units (20A, 20B, 20C). Each wrapper unit (20A, 20B, 20C) connects one of the responder units (14A, 14B, 14C) to the bus (16). Each wrapper unit comprises: an interface unit (22) arranged to enable the requestor units (12A, 12B) to access the responder elements (18\_1—18\_9) of the respective responder unit (14) associated with the respective wrapper unit (20A). Each wrapper unit further comprises a checksum unit (26) arranged to respond to any write access to any one (18\_2) of the critical responder elements (18\_1, 18\_2, 18\_5) by computing and storing a reference checksum; wherein the checksum unit (26) is arranged to

compute the reference checksum by applying a checksum algorithm to a subset of the critical responder elements (18\_1, 18\_2, 18\_5), the subset comprising at least the write-accessed critical responder element (18\_2).

**Title : Digital device****Description**5 Field of the invention

This invention relates to a digital device.

Background of the invention

10 A variety of electronic and optoelectronic memory devices are known in the art. A digital device may comprise a plurality of memory elements. A memory element is a structure for storing one or more information bits. A flip-flop or a group of flip-flops is an example of a memory element. Memory elements that are used in today's devices can be very reliable when the device is sufficiently well protected against perturbations from its environment. Such perturbations may include, for example, photon or neutron impact or collisions with alpha particles. For example, a  
15 neutron colliding with a flip flop may reverse the state of the flip-flop.

Various techniques for helping to ensure the integrity of data stored in a digital device are known in the art. One example includes the use of triple voting flip-flops (TVF). In another approach, a checksum is generated for the data of interest. By recomputing the checksum for the data of interest at a later point in time and comparing it with the original checksum, it may be  
20 determined whether the data has changed or not. For example, US patent application publication no. US 2012/0036400 A1 (Miller) describes a data processing system that includes a plurality of peripherals in which the integrity of configuration information may be checked by means of an error syndrome generated by a peripheral bus interface when a requestor unit of the data processing system has initiated a write operation.

25

Summary of the invention

The present invention provides a digital device as described in the accompanying claims.

Specific embodiments of the invention are set forth in the dependent claims.

These and other aspects of the invention will be apparent from and elucidated with reference  
30 to the embodiments described hereinafter.

Brief description of the drawings

Further details, aspects and embodiments of the invention will be described, by way of example only, with reference to the drawings. In the drawings, like reference numbers are used to  
35 identify like or functionally similar elements. Elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale.

Figure 1 schematically shows an example of an embodiment of a digital device.

Figure 2 schematically shows an example of an embodiment of a responder unit.

Figure 3 schematically shows an example of an embodiment of a wrapper unit.

40 Figure 4 schematically shows an example of an embodiment of a shared unit.

Figure 5 shows a flow chart of an example of an embodiment of a method of operating a digital device.

#### Detailed description of the preferred embodiments

5 Because the illustrated embodiments of the present invention may for the most part, be implemented using electronic components and circuits known to those skilled in the art, details will not be explained in any greater extent than that considered necessary as illustrated above, for the understanding and appreciation of the underlying concepts of the present invention and in order not to obfuscate or distract from the teachings of the present invention.

10 Figure 1 schematically shows an example of a digital device 10. The digital device 10 may comprise, for example, one or more requestor units, one or more responder units, and a bus connecting each responder unit to each requestor unit. For example, the device 10 shown in the Figure comprises a first requestor unit 12A, a second requestor unit 12B, a first, second, and third responder unit 14A, 14B, and 14C, and a bus 16. Each requestor unit may, for instance, be a  
15 microprocessor or processor core, a direct-memory access (DMA) unit, or a peripheral capable to generate bus accesses. The responder units 14A, 14B, and 14C may, for instance, be a static random access memory unit (SRAM), a non-volatile memory (Flash), or peripheral units (peripherals) such as a pulse-width modulation unit (PWM), a wireless interface, a sensor unit, a serial or parallel communication interface or any other kind of digital data processing device  
20 capable of responding to the requestor units. Each of the responder units 14A, 14B, 14C may comprise a set of memory elements. Each memory element may be accessible individually by each or at least one of the requestor units, e.g., by requestor units 12A, 12B, via the bus 16.

An example of a responder unit 14 is schematically shown in Figure 2. The responder unit 14 may be representative of any one of the responder units discussed herein. For example, each of  
25 the responder units 14A, 14B, and 14C in Figure 1 may be arranged as described in reference to Figure 2. The responder unit 14 may notably comprise a set of memory elements 18\_K, where K is an index specifying the respective memory element. In Figure 2, a set of nine memory elements 18\_1 to 18\_9 is shown. The responder unit 14 may, however, comprise a far greater number of memory elements. Each memory element 18\_K may, for instance, be a register. A register may be  
30 composed of a certain number of flip-flops, such as 8, 16, or 32 flip-flops, for example. The register size, i.e., the number of information bits it may store or, equivalently, the number of flip-flops it contains, may coincide with a word size of the digital device 10. Some registers, however, may contain fewer bits than other registers. The memory elements 18\_K of the responder unit 14 may notably include one or more elements that are used for control purposes (control elements). In an  
35 example in which the responder unit 14 is a peripheral unit and the memory elements 18\_K are registers, the control elements may also be referred to as the peripheral control registers. In the example of Figure 2, the memory elements 18\_1, 18\_2, and 18\_5 are control elements. In another example (not shown), any other memory element 18\_K of the responder unit 14 may be a control element. A control element may be defined as a memory element that is arranged to store  
40 configuration data of the responder unit 14. The proper functioning of the responder unit 14 may

therefore be affected if the data stored in one of the control elements is accidentally changed by, for example, an environmental impact. In one example, the control elements, e.g., control elements 18\_1, 18\_2, and 18\_5, are initialized only during a set-up phase of the digital device 10, and from thereon, an application running on the digital device 10 may have to rely on the integrity of the information stored in these registers.

Referring back to the example of Figure 1, each of the responder units 14A, 14B, 14C may thus comprise a plurality of responder elements 18\_K which may be accessible by the requestor units 12A, 12B via the bus 16 and which may include one or more critical memory elements such as the memory elements 18\_1, 18\_2, and 18\_5 in Figure 2. Any memory element among the memory elements of a given responder unit may be defined as a critical memory element to indicate that the integrity of its data content must be ensured.

The digital device 10 may further comprise one or more wrapper units 20A, 20B, 20C. The digital device 10 may comprise fewer or more wrapper units than those shown in Figure 1. Each of the wrapper units 20A, 20B, and 20C may connect one of the responder units 14A, 14B, and 14C to the bus 16. Each of the responder units 14A, 14B, 14C may thus be associated with one of the wrapper units 20A, 20B, and 20C and vice versa. In other words, the responder units and the wrapper units may be arranged in pairs, each pair comprising a responder unit, e.g., responder unit 14A, and a wrapper unit, e.g., wrapper unit 14B, connected between the respective responder unit, e.g., responder unit 14A, and the bus 16. There is not necessarily a wrapper unit for every responder unit. Furthermore, the digital device 10 may comprise further responder units which are not described in this application and which may differ from those described herein.

Each of the wrapper units 20A, 20B, and 20C may comprise an interface unit 22, a configuration unit 24, a checksum unit 26, and a verification unit 28, for example (see Figure 3).

The interface unit 22 of a wrapper unit 20 may be arranged to enable the requestor units of the digital device 10, e.g., the requestor units 12A and 12B, to access the responder elements, e.g., 18\_1 to 18\_9, of the respective responder unit 14 that is associated with this wrapper unit. For example, the requestor units 12A and 12B may thus be enabled to access the responder elements of the responder unit 14A via the wrapper unit 20A. Each wrapper unit may thus be designed so as to pass on any communication between the one or more requestor units 12A, 12B and the respective responder unit 14.

The checksum unit 26 may be arranged to respond to any write access to any of the critical responder elements (e.g., to the critical responder elements 18\_1, 18\_2, and 18\_5 in Figure 2) by computing and storing a reference checksum. The reference checksum may be computed by applying a checksum algorithm to the data content of a subset of the critical memory elements, wherein the subset may comprise at least the critical responder element that is accessed by said write access.

The checksum 26 and the verification unit 28 may be merged in a single unit or comprise shared circuitry. This may be particularly convenient because both the checksum unit 26 and the verification unit 28 may use the same algorithm for computing and re-computing the reference checksum, respectively.

In one example, the mentioned subset comprises only the single critical memory element to which the write access takes place. In this case, the checksum may thus be computed by applying the checksum algorithm to only this single memory element. For example, when one of the requestor units 12A, 12B performs a write access to memory element 18\_2, the checksum unit 26 may compute a checksum for the data that is written into this single memory element 18\_2 and store the computed checksum as a reference checksum.

In another example, the mentioned subset comprises the entire subset of critical memory elements of the given responder unit 14. For example, referring again to Figure 2, when one of the requestor units 12A, 12B performs a write access to the critical memory element 18\_2, the checksum unit 26 may compute a checksum by applying the checksum algorithm to the data content of the entire set of critical memory elements 18\_1, 18\_2, and 18\_5. The checksum unit 26 may further store the thus computed checksum as a reference checksum. In a related example, the checksum may be stored centrally and not in the individual checksum units 26.

The checksum associated with a given subset of critical memory elements may be recomputed at a later instant to check whether the data content of the respective subset has changed. In the above-described first example in which a checksum is provided individually for each critical memory element, such a check (integrity test) may thus be performed individually for each memory element. In the above-described second example, in which a single checksum is provided for the entire set of memory elements 18\_K ( $K=1\dots N$ ), a single integrity test may be performed to check the integrity of the data content of the entire set of critical memory elements.

A checksum, is a data item, e.g., a string or a numerical value, that is computed by applying a checksum algorithm, also known as a checksum function, to an input data item, and which is shorter than the input data item and which is different for two input data items that differ slightly.

In other words, the verification unit 28 may be arranged to perform an integrity test which may comprise: computing a verification checksum by reapplying the checksum algorithm to the data content of the mentioned subset of critical responder elements, and verifying whether the verification checksum is identical to the reference checksum. The integrity test may be performed repeatedly, e.g., in certain intervals of time. The verification unit 28 may be further arranged to trigger an error action if the verification checksum is not identical to the respective reference checksum. The error action may include, for instance, signaling the error to the requestor units, e.g., 12A and 12B, or at least to one of the requestor units, or to another block (not shown) within the device 10 that is responsible collecting and reacting on erroneous conditions within the device. Alternatively or in addition, the error action may include correcting the corrupted data content. In this respect, it is noted that the checksum may be or comprise an error correcting code (ECC). The verification unit 28 may thus use the reference checksum to correct the corrupted data content of the respective subset of critical memory elements.

A major benefit of the architecture described herein may be that the wrapper units, e.g., wrapper units 20A, 20B, and 20C may be nonintrusive for the associated responder units, e.g., 14A, 14B, 14C and do not require a modification of the particular responder unit they are associated with. A wrapper unit as described herein may therefore be easily integrated in an

existing architecture with existing responder units in which one or more requestor units are connected to one or more responder units via a bus. In other words, the same type of responder unit may be implemented within, e.g., a system on chip (SoC), with an associated wrapper unit as well as without. If the respective responder unit, e.g., responder unit 14A lacks an associated  
5 wrapper unit, e.g., wrapper unit 20A, it will, of course, also lack the data integrity monitoring or data correction mechanism provided by the wrapper unit. This may be acceptable if the respective responder unit does not provide any safety relevant function or does not have memory elements for holding control information.

The configuration unit 24 (cf. Figure 3) is an optional unit that may be configurable for  
10 enabling a user to define any memory element among the memory elements of the associated responder units as a critical memory element. This unit is optional, because it is also possible to omit it and provide a static definition of critical memory elements for a particular responder unit type; a static definition refers here to a definition that is specified at design or synthesis time of the associated hardware, which cannot be modified by software at application run time. As such a  
15 static definition allows a SoC designer or system architect to configure the wrapper units before fabrication of the corresponding device. A definition that can be modified by software may thus enable a software developer, customer, or other user to configure the wrapper unit to his specific needs, e.g., to adapt it to a specific application to be executed by the requestor units. The configuration unit 24 may also be one-time configurable. The configuration unit 24 may, for  
20 example, comprise a table specifying the selection of critical memory elements, that table being implemented in a one-time write or flash memory and applied during startup of the device. The selection of critical responder elements may thus be made permanent or configured during startup, for example, before the device 10 is released on the market.

The digital device 10 may further comprise a shared unit 30 (cf. Figure 1) connected to each  
25 wrapper unit 20A, 20B, 20C. The shared unit 30 may be arranged to provide one or more functions that may be common to these wrapper units. Functions provided by other units described herein, such as the verification unit 28, may also be integrated in the shared unit 30. The hardware of the digital device 10 may thus be reduced. The one or more common functions may, for example, include the computation of the reference checksum as well the computation of the verification  
30 checksum. It is noted that the checksum algorithm may be the same for every wrapper unit 14A, 14B, and 14C and for every subset of critical responder elements that has its own reference checksum. The shared unit 30 may, for example, comprise a dedicated arithmetic logic unit 34 for computing the checksum.

Another common functionality that may be performed by the shared unit 30 is the storage of  
35 checksum information for all wrapper units 20 or a subset of these wrapper units. This storage may be done within a set of dedicated memory elements within the shared unit 30, a dedicated RAM element within the shared unit 30, or by using a portion of the "normal" memory within the device 10 for this purpose; in the later case the shared unit 30 will perform the required read and write accesses to record or retrieve the checksum data from memory.

The digital device 10 may be arranged to be clocked by a at least one clock signal. For example, the digital device may comprise a clock unit (not shown) for generating a first clock signal CLK. Alternatively, the digital device may be arranged to receive the first clock signal CLK from an external clock unit (not shown). The digital device 10 may further comprise a clock divider 32 (cf. Figure 4) for generating a second clock signal CLK2 that has a lower clock rate than the first clock signal. The verification unit 28 (cf. Figure 3) may in this case be arranged to repeat the integrity test in response to, e.g., each triggering edge of the second clock signal. A triggering edge may be defined as a rising edge or as a falling edge or as any edge of the respective clock signal. An integrity test may thus be performed for each subset within each responder unit 14A, 14B, and 14C at the frequency of the second clock signal. The integrity tests associated with the various subsets in the various wrapper units may be performed in parallel or sequentially, depending on the details of the design. A design in which the integrity tests are performed sequentially may be less expensive.

The clock divider 32 may be integrated in, for example, the shared unit 30. The shared unit 30 may further comprise a wrapper counter (not shown) arranged to select one of the wrapper units 20A, 20B, and 20C in a specified order and in accordance with, e.g., the second clock signal. The clock divider 32 may be configurable by software; which allows to specify the interval time of the checks by the verification unit. The shared unit 30 may further comprise, e.g., a subset counter (not shown) arranged to select one of the subsets within the wrapper units 20A, 20B, 20C. The shared unit 30 may thus be operated to specify an order and the interval in which the integrity tests may be performed for the subsets within the wrapper units 20A, 20B, 20C. For instance, the integrity test may be performed first for all subsets within the responder unit 14A, then for all subsets within the responder unit 14B, then for all subsets within the responder unit 14C, and then again for all subsets within the responder unit 14A, and so on. In other words, the shared unit 30 may be arranged to count through all subsets within the group of critical responder elements within the digital device 10 in accordance with the second clock signal. The second clock signal may have a lower frequency than the first clock signal, and the frequency of the integrity tests may thus be reduced, and power consumption by the involved units may be reduced accordingly. The frequency of the second clock signal should, however, be sufficiently high so that the interval between two consecutive integrity tests for any subset in any responder unit is not longer than a specific interval; e.g. the process safety time (PST) for a safety device.

Referring now to Figure 5, operation of an example of a wrapper unit, e.g., the wrapper unit 20A of the responder unit 14A, is described. The process flow may start in block S1 with the wrapper unit 20A determining whether there is a read access, a write access, or no access to one of the memory elements of its associated responder unit 14A. If there is a read access, the interface unit 22 may perform this read access. The interface 22 may, to this end, forward a corresponding read access signal from the bus 16 to the responder unit 14A. From block S2, the process flow may return to block S1 with, e.g., the next triggering edge of, e.g., the first clock signal CLK mentioned above.

If, however, there is a write access on the bus 16, the interface 22 may perform the write access (block S3) by, e.g., forwarding the write access signal to the responder unit 14A. The checksum unit 26 may further determine whether the write access is directed to one of the critical memory elements of the responder unit 14A. If the write access is directed to a non-critical memory element, the process flow may return to block S1 with, e.g., the next triggering edge of, e.g., the first clock signal CLK. If, however, the write access is directed to one of the critical memory elements, the checksum unit 26 may compute a new reference checksum for the subset that comprises the critical memory element that was the object of the write access, taking into account the data to be written into at least one of the critical memory elements. It may be recalled that this subset may comprise one or more memory elements depending on the architecture. Block S5, i.e., the computation of the new reference checksum may need to include also critical memory elements that are not modified by the data to be written so that the new reference checksum will account for the new data content that has been written to the critical memory element as well as the content of unmodified critical memory elements. The new reference checksum for the subset that comprises the critical memory element that was the object of the write access, is then stored somewhere, i.e. in the checksum unit 22, the wrapper unit 20, or the shared unit 30, to allow later usage of this value. From block S5, the process flow may return to block S1.

If, however (now referring back to block S1), there is no read access and no write access, the verification unit 28 may perform an integrity test comprising, e.g., blocks S6, S7, and S8. It is noted that block S1 may, for instance, be performed at the frequency of the above-mentioned first clock signal CLK, and the integrity test S6, S7, S8 may be performed at the frequency of, e.g., the second clock signal CLK2. In other words, the integrity test S6, S7, S8 may be performed less frequently than block S1. The integrity test S6, S7, S8 may thus be absent for some iterations of block S1, although this is not indicated in the Figure. In one example, the integrity test S6, S7, S8 may be performed in only one out of, e.g., 100 repetitions of block S1.

The integrity test S6, S7, S8 may comprise computing, checking and eventually correcting the subset referred to above in reference to block S5 based on the stored verification checksum CHS1. For this purpose, the verification unit 28 may use the interface unit 22 to perform a read access (in block S6) to the responder unit 14 to retrieve the actual values of the critical memory elements 18\_K making up this subset. This access may be a "local" access from the wrapper unit 20 to the responder unit 14 that is not forwarded to the bus 16 and thus not visible to other units within the device. The retrieved content of the critical memory elements 18\_K is then used to calculate the verification checksum CHS2 in a subsequent step within block S6.

The integrity test may further comprise comparing the calculated verification checksum CHS2 against the reference checksum CHS1 (block S7) and triggering an error action (block S8) if these two checksums differ. The error action S8 may, for example, comprise correcting the data in the respective subset, or sending a "correction request signal" to another unit (not shown) to request a correction by this unit. It is worth to note that, i.e. when the using an ECC checksum, a certain amount of errors (single bit flips) can be corrected based solely on the actual data and stored checksum; in this particular case the correct content can be calculated and written back into



the associated critical memory elements 18\_K. An additional functionality performed as part of the error action S8 may be setting a flag to identify the detection of erroneous data; which may be further used by the device.

From block S8, the process flow may return to block S1. If, however, the verification  
5 checksum coincides with the reference checksum, the process flow may return from block S7 to block S1.

In the foregoing specification, the invention has been described with reference to specific  
examples of embodiments of the invention. It will, however, be evident that various modifications  
and changes may be made therein without departing from the broader spirit and scope of the  
10 invention as set forth in the appended claims.

The connections as discussed herein may be any type of connection suitable to transfer  
signals from or to the respective nodes, units or devices, for example via intermediate devices.  
Accordingly, unless implied or stated otherwise, the connections may for example be direct  
connections or indirect connections. The connections may be illustrated or described in reference  
15 to being a single connection, a plurality of connections, unidirectional connections, or bidirectional  
connections. However, different embodiments may vary the implementation of the connections.  
For example, separate unidirectional connections may be used rather than bidirectional  
connections and vice versa. Also, plurality of connections may be replaced with a single connection  
that transfers multiple signals serially or in a time multiplexed manner. Likewise, single connections  
20 carrying multiple signals may be separated out into various different connections carrying subsets  
of these signals. Therefore, many options exist for transferring signals.

Each signal described herein may be designed as positive or negative logic. In the case of a  
negative logic signal, the signal is active low where the logically true state corresponds to a logic  
level zero. In the case of a positive logic signal, the signal is active high where the logically true  
25 state corresponds to a logic level one. Note that any of the signals described herein can be  
designed as either negative or positive logic signals. Therefore, in alternate embodiments, those  
signals described as positive logic signals may be implemented as negative logic signals, and  
those signals described as negative logic signals may be implemented as positive logic signals.

Furthermore, the terms "assert" or "set" and "negate" (or "deassert" or "clear") are used  
30 herein when referring to the rendering of a signal, status bit, or similar apparatus into its logically  
true or logically false state, respectively. If the logically true state is a logic level one, the logically  
false state is a logic level zero. And if the logically true state is a logic level zero, the logically false  
state is a logic level one.

Also for example, in one embodiment, the illustrated examples may be implemented as  
35 circuitry located on a single integrated circuit or within a same device. For example, the requestor  
units and the responder units may be located on a single integrated circuit. Alternatively, the  
examples may be implemented as any number of separate integrated circuits or separate devices  
interconnected with each other in a suitable manner. For example, the requestor units and the  
wrapper units may be located on separate integrated circuits.

Also for example, the examples, or portions thereof, may implemented as soft or code representations of physical circuitry or of logical representations convertible into physical circuitry, such as in a hardware description language of any appropriate type.

5 However, other modifications, variations and alternatives are also possible. The specifications and drawings are, accordingly, to be regarded in an illustrative rather than in a restrictive sense.

10 In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word 'comprising' does not exclude the presence of other elements or steps then those listed in a claim. Furthermore, the terms "a" or "an," as used herein, are defined as one or more than one. Also, the use of introductory phrases such as "at least one" and "one or more" in the claims should not be construed to imply that the introduction of another claim element by the indefinite articles "a" or "an" limits any particular claim containing such introduced claim element to inventions containing only one such element, even when the same claim includes the introductory phrases "one or more" or "at least one" and indefinite articles such as "a" or "an." The same holds  
15 true for the use of definite articles. Unless stated otherwise, terms such as "first" and "second" are used to arbitrarily distinguish between the elements such terms describe. Thus, these terms are not necessarily intended to indicate temporal or other prioritization of such elements. The mere fact that certain measures are recited in mutually different claims does not indicate that a combination of these measures cannot be used to advantage.

20

**Claims**

1. A digital device (10) comprising one or more requestor units (12A, 12B), one or more responder units (14A, 14B, 14C), and a bus (16); each of said responder units (14A, 14B, 14C) being connected to said one or more requestor units (12A, 12B) via said bus (16); wherein each of said one or more responder units (14A, 14B, 14C) comprises a plurality of responder elements (18\_1—18\_9) which are accessible by said requestor units (12A, 12B) via said bus (16) and which include one or more critical responder elements (18\_1, 18\_2, 18\_5); said digital device (10) further comprising one or more wrapper units (20A, 20B, 20C); wherein each of said wrapper units (20A, 20B, 20C) connects one of said responder units (14A, 14B, 14C) to said bus (16) and comprises:
- an interface unit (22) arranged to enable said requestor units (12A, 12B) to access the responder elements (18\_1—18\_9) of the respective responder unit (14) associated with the respective wrapper unit (20A);
- a checksum unit (26) arranged to respond to any write access to any one (18\_2) of said critical responder elements (18\_1, 18\_2, 18\_5) by computing and storing a reference checksum; wherein said checksum unit (26) is arranged to compute said reference checksum by applying a checksum algorithm to a subset of said critical responder elements (18\_1, 18\_2, 18\_5), said subset comprising at least said write-accessed critical responder element (18\_2).
2. The digital device (10) of claim 1, wherein each of said wrapper units (20A, 20B, 20C) further comprises a configuration unit (24) which is configurable to define any one of said responder elements (18\_1—18\_9) as a critical responder element (18\_1; 18\_2; 18\_5)
3. The digital device (10) of claim 2, wherein said configuration unit (24) is hardwired at synthesis time or one-time configurable at device startup.
4. The digital device (10) of claim 1, 2, or 3, wherein said subset comprises only said write-accessed responder element (18\_2).
5. The digital device (10) of claim 1, 2, 3, wherein said subset comprises any combination of critical responder elements among said critical responder elements (18\_1, 18\_2, 18\_5).
6. The digital device (10) of one of the preceding claims, further comprising a shared unit (30) connected to each of said one or more wrapper units (20A, 20B, 20C) and arranged to provide one or more functions which are common to said one or more wrapper units (20A, 20B, 20C).
7. The digital device (10) of one of the preceding claims, wherein said one or more common functions include generating said reference checksum.

8. The digital device (10) of one of the preceding claims, wherein each of said wrapper units (20A, 20B, 20C) further comprises a verification unit (28) arranged to perform an integrity test (S6, S7, S8) which comprises:

operating the interface unit (22) for reading the data content of a group of critical memory elements consisting of at least one critical responder elements 18\_K

computing a verification checksum (S6) by re-applying said checksum algorithm to the data content of said group of critical responder elements;

verifying whether said verification checksum is identical to said reference checksum (S7); and

triggering an error action (S8) if said verification checksum is not identical to the respective reference checksum.

9. The digital device (10) of claim 8, wherein said reading of said data content is not visible to any other block than the involved wrapper unit (20) and the corresponding responder unit (14).

10. The digital device (10) of claim 8 or 9, arranged to be clocked by a first clock signal (CLK) and comprising a clock divider (32) for generating a second clock signal (CLK2) having a lower clock rate than said first clock signal (CLK), wherein said verification unit (28) arranged to repeat said integrity test at a triggering edge of said second clock signal (CLK2).

11. The digital device (1) of claim 8, 9, or 10, arranged to repeat said integrity test in parallel or in series

for any subset of the wrapper units (14) and

for any subset of the critical memory elements (18\_K) of a wrapper units 14 within the said subset of wrapper units.

12. The digital device (10) of claim 8, 9, 10, or 11, wherein said verification unit (28) is arranged to perform said integrity test while none of said requestor units (12A, 12B) is accessing the respective responder unit (14).

13. The digital device (10) of one of the preceding claims, wherein said checksum is or comprises an error detection and correction code.

14. The digital device (10) of one of the preceding claims, wherein said digital device (10) is a system on chip.

15. The digital device (10) of one of the preceding claims, wherein said responder elements (18\_1—18\_9) are registers.

Fig. 1

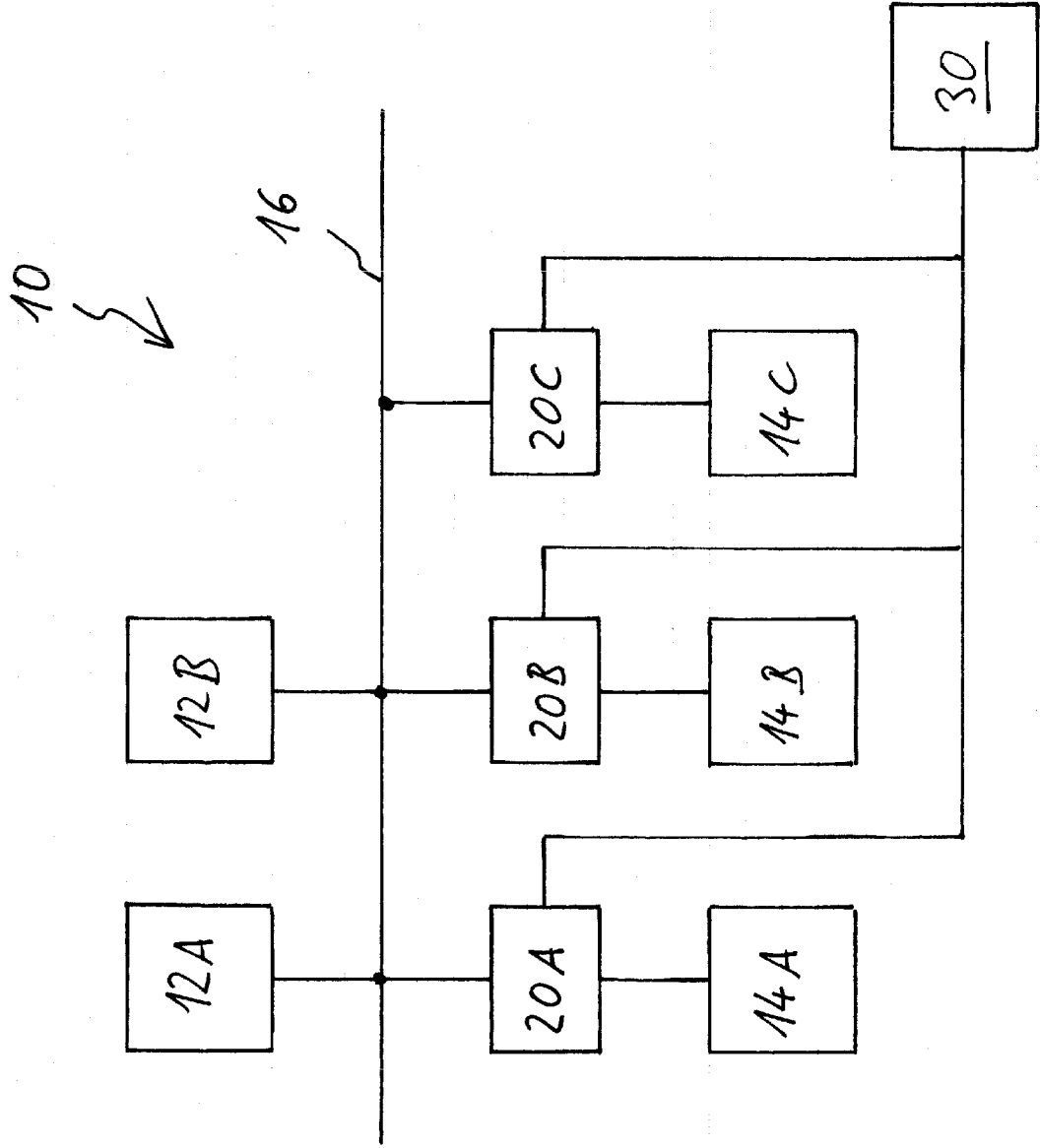
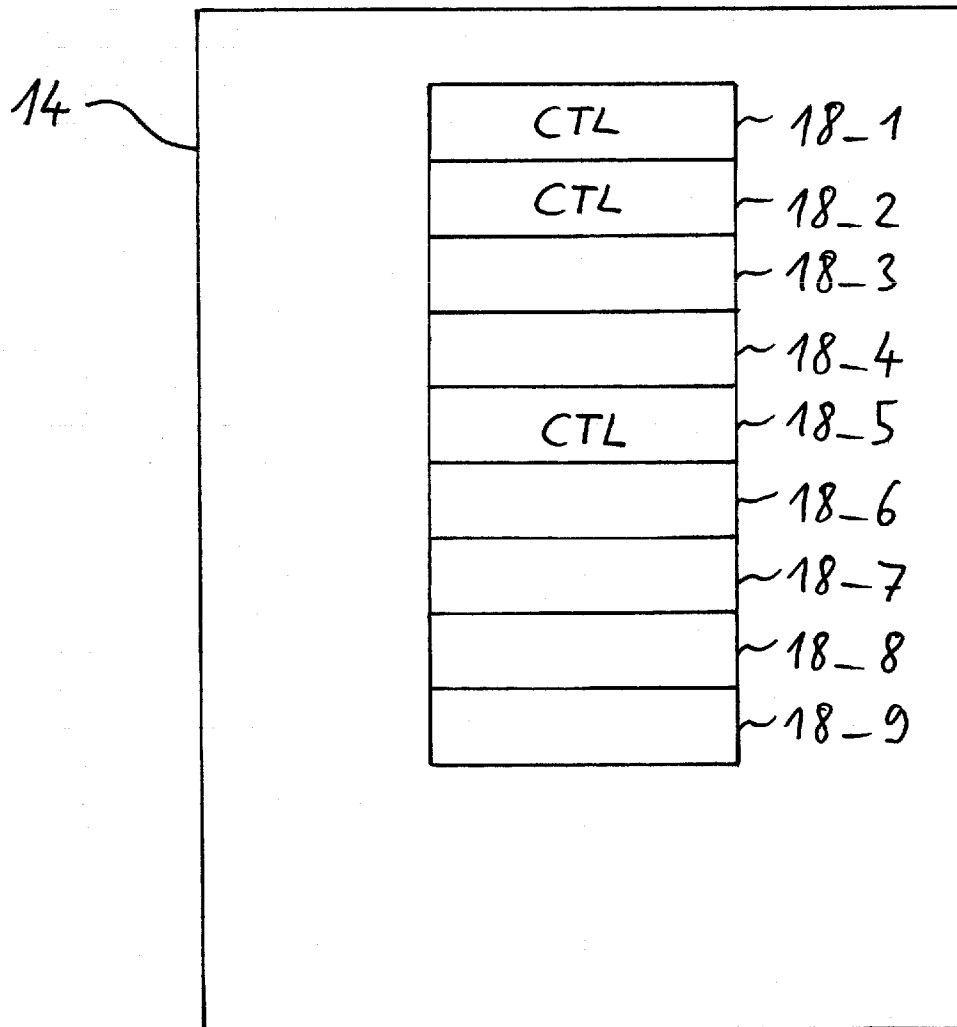


Fig. 2



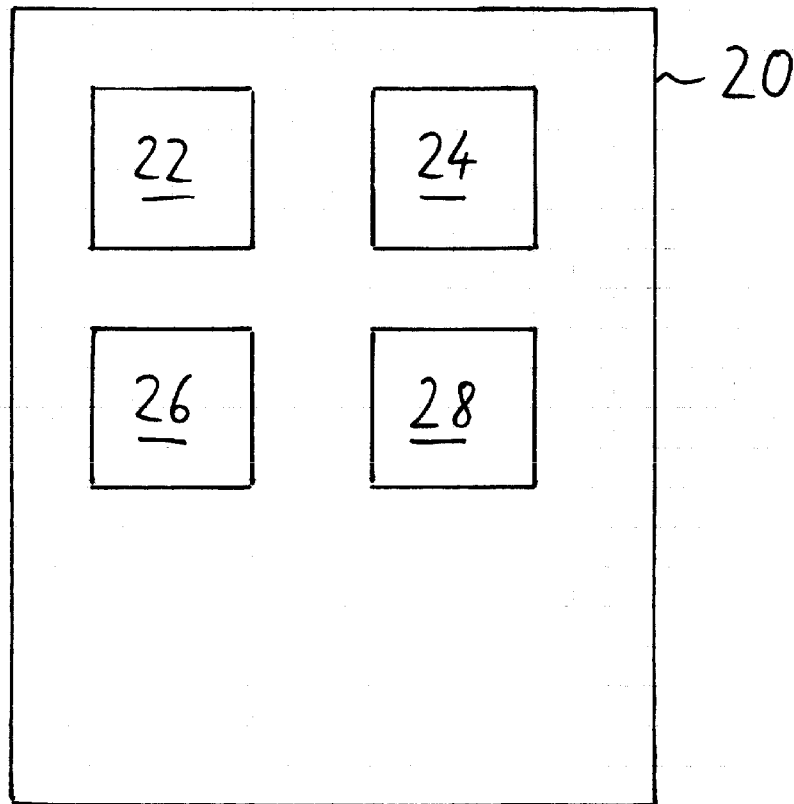
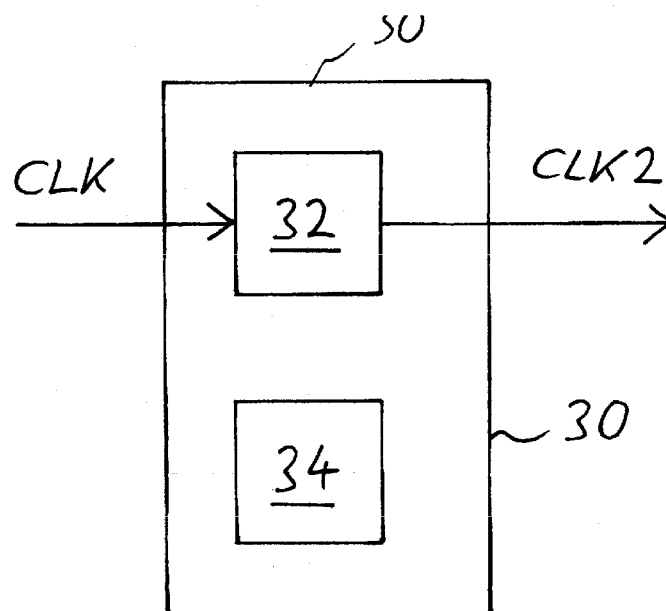
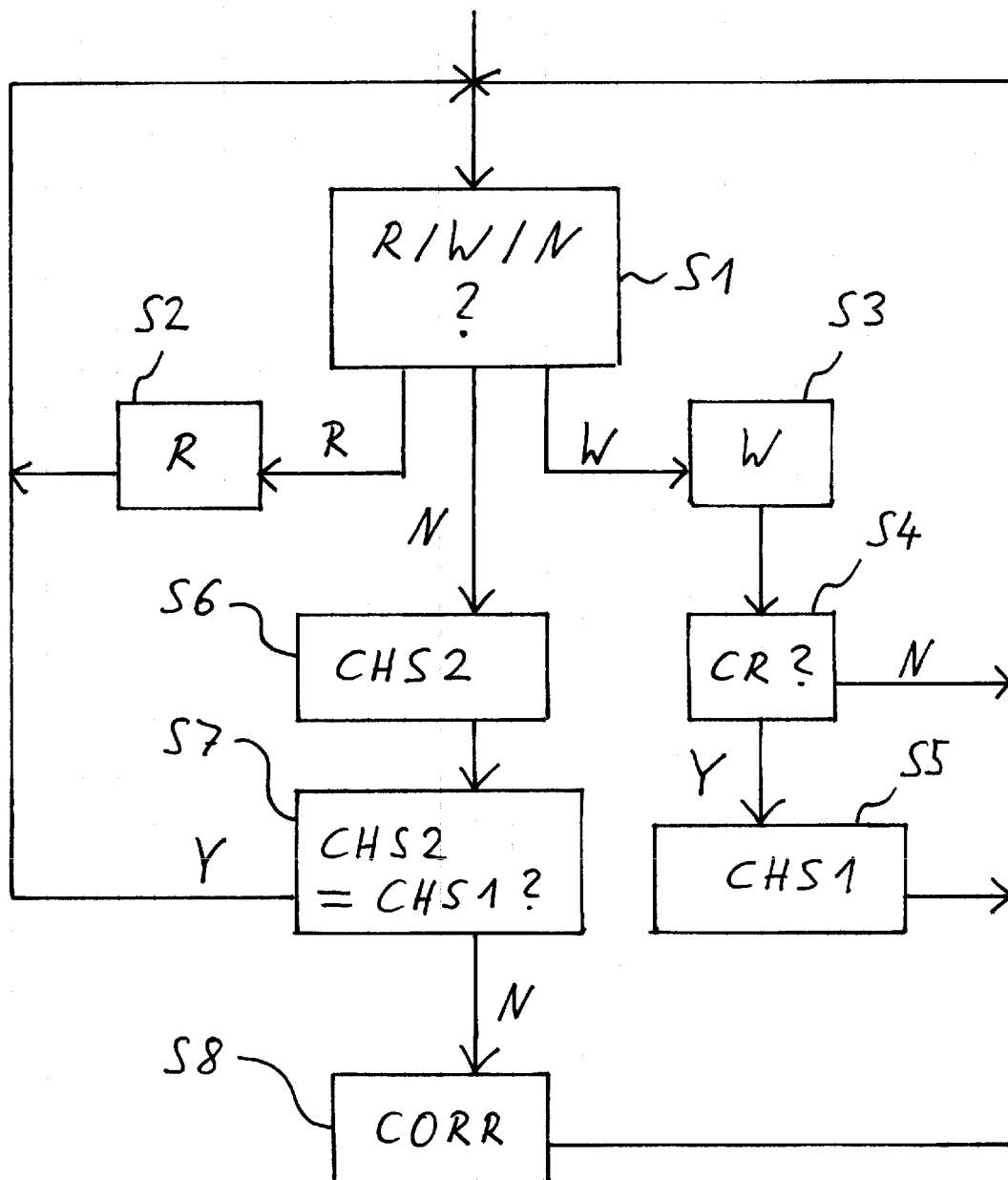
**Fig. 3****Fig. 4**

Fig. 5





## INTERNATIONAL SEARCH REPORT

International application No.  
**PCT/IB2012/056675****A. CLASSIFICATION OF SUBJECT MATTER****G06F 13/38(2006.01)i, G06F 13/14(2006.01)i**

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 13/38; H03M 13/09; G06F 9/44; G06F 12/00; G06F 13/36; G06F 13/24; G06F 11/00; G06F 11/16; G06F 13/00; G06F 13/14**

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) &amp; Keywords: computer, processor, bus, memory, clock(CLK), peripheral, checksum

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                                                                          | Relevant to claim No. |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | US 7080188 B2 (LARRY L. BYERS et al.) 18 July 2006<br>See column 1, lines 50-56; column 2, lines 25-26, 31-34; column 5, lines 13-14, 34-38; column 6, lines 55-61; column 7, lines 4-6; column 8, lines 6-8, 38-39, 60-61; column 9, lines 24-25; column 17, lines 63-64; and figures 1-2. | 1-3                   |
| A         |                                                                                                                                                                                                                                                                                             | 4                     |
| Y         | US 2011-0202996 A1 (ANTOINE MONSIFROT et al.) 18 August 2011<br>See paragraphs [0009], [0016], [0020], [0031], [0055].                                                                                                                                                                      | 1-3                   |
| A         | US 05581715 A (PHIL VERINSKY et al.) 03 December 1996<br>See column 6, lines 19-54; and figure 2.                                                                                                                                                                                           | 1-4                   |
| A         | US 2011-0055638 A1 (JULIEN LEROUGE et al.) 03 March 2011<br>See paragraph [0021]; and figure 1.                                                                                                                                                                                             | 1-4                   |
| A         | US 2002-0016896 A1 (FRIDTJOF SIEBERT) 07 February 2002<br>See paragraphs [0044]-[0045]; and figure 5.                                                                                                                                                                                       | 1-4                   |



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 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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

20 August 2013 (20.08.2013)

Date of mailing of the international search report

**21 August 2013 (21.08.2013)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office  
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City,  
302-701, Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

BYUN Sung Cheal

Telephone No. +82-42-481-8262



# INTERNATIONAL SEARCH REPORT

International application No.

**PCT/IB2012/056675**

## Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 9  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:  
Claim 9 does not comply with PCT Article 6 because it is referring to unsearchable claim 8.
3. ☒ Claims Nos.: 5-8, 10-15  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

### Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/IB2012/056675**

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|-------------------------------------------|---------------------|----------------------------|---------------------|
| US 7080188 B2                             | 18/07/2006          | US 2004-0181620 A1         | 16/09/2004          |
|                                           |                     | US 2004-0199695 A1         | 07/10/2004          |
|                                           |                     | US 2004-0199711 A1         | 07/10/2004          |
|                                           |                     | US 2004-0199718 A1         | 07/10/2004          |
|                                           |                     | US 2006-0129704 A1         | 15/06/2006          |
|                                           |                     | US 2006-0230214 A1         | 12/10/2006          |
|                                           |                     | US 2007-0226392 A1         | 27/09/2007          |
|                                           |                     | US 7099963 B2              | 29/08/2006          |
|                                           |                     | US 7219182 B2              | 15/05/2007          |
|                                           |                     | US 7457903 B2              | 25/11/2008          |
|                                           |                     | US 7853747 B2              | 14/12/2010          |
|                                           |                     | US 7870320 B1              | 11/01/2011          |
|                                           |                     | WO 2004-081738 A2          | 23/09/2004          |
|                                           |                     | WO 2004-081738 A3          | 15/12/2005          |
| US 2011-0202996 A1                        | 18/08/2011          | CN 102163268 A             | 24/08/2011          |
|                                           |                     | EP 2362314 A1              | 31/08/2011          |
|                                           |                     | JP 2011-170847 A           | 01/09/2011          |
| US 05581715 A                             | 03/12/1996          | EP 0689207 A1              | 27/12/1995          |
|                                           |                     | US 05581715 A              | 03/12/1996          |
|                                           |                     | US 2002-0032808 A1         | 14/03/2002          |
|                                           |                     | US 2002-116552 A2          | 22/08/2002          |
|                                           |                     | US 2003-0037230 A1         | 20/02/2003          |
|                                           |                     | US 2004-0158658 A1         | 12/08/2004          |
|                                           |                     | US 2006-0036787 A1         | 16/02/2006          |
|                                           |                     | US 2006-0101161 A1         | 11/05/2006          |
|                                           |                     | US 6546440 B1              | 08/04/2003          |
|                                           |                     | US 6584527 B2              | 24/06/2003          |
|                                           |                     | US 6721828 B2              | 13/04/2004          |
|                                           |                     | US 6968404 B2              | 22/11/2005          |
|                                           |                     | US 7124216 B2              | 17/10/2006          |
|                                           |                     | US 7124217 B2              | 17/10/2006          |
| US 2011-0055638 A1                        | 03/03/2011          | US 8412953 B2              | 02/04/2013          |
| US 2002-0016896 A1                        | 07/02/2002          | DE 10120615 A1             | 20/12/2001          |
|                                           |                     | DE 10120615 B4             | 19/08/2004          |
|                                           |                     | US 6704851 B2              | 09/03/2004          |