(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/44911 A1

(51) International Patent Classification[7]: G06F 13/00, 11/16

(21) International Application Number: PCT/SE01/02660

(22) International Filing Date:
30 November 2001 (30.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0004421-4 1 December 2000 (01.12.2000) SE

(71) Applicant *(for all designated States except US)*: **SAAB AB** [SE/SE]; S-581 88 Linköping (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **JOHANSSON, Rikard** [SE/SE]; Middagsgatan 96, S-589 53 Linköping (SE).

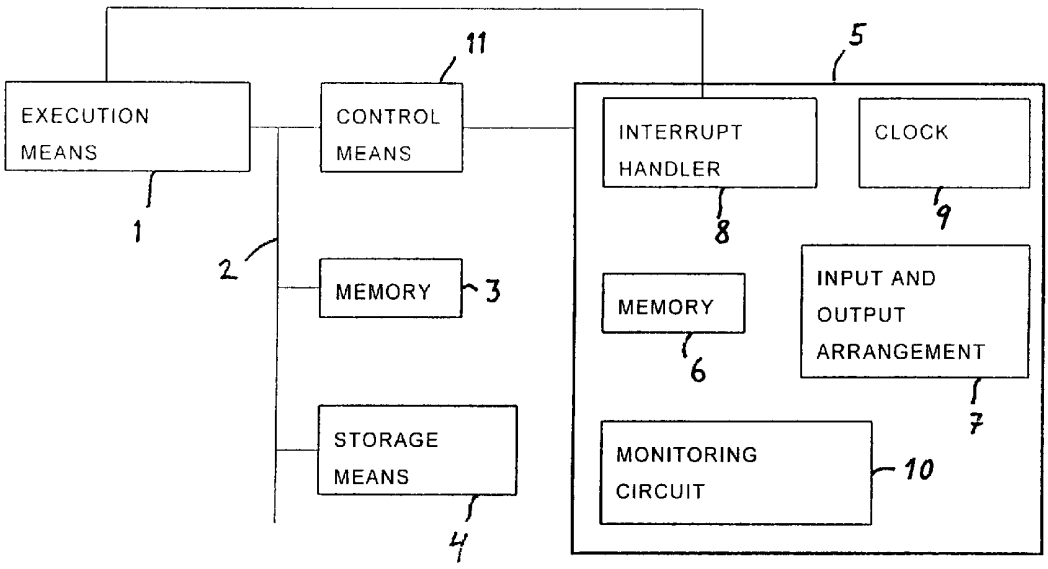
(74) Agents: **OLSSON, Jan** et al.; Bjerkéns Patentbyrå KB, P.O. Box 1274, S-801 37 Gävle (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent

[Continued on next page]

(54) Title: METHOD AND COMPUTER DEVICE WITH DIFFERENT CRITICALITY



(57) Abstract: A computer device comprises storage means (4) containing a first software of a first higher critically and a second software of a second lower critically, means (1) for executing the first and second software and an arrangement (7) for data input to and data output from the device. Said execution means (1) is a Central Processing Unit (CPU). The device is adapted to fetch input data stored in a first memory (6) included in the computer device and store output data in the first memory when executing the first software and fetch input data stored in a second memory (3) included in the computer device and store output data in the second memory when executing the second software. The first software is adapted to control which output data that are transferred from the first and second memory (6, 3) to said arrangement (7). The invention is also related to a method for executing softwares of different critically.

WO 02/44911 A1

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND COMPUTER DEVICE WITH DIFFERENT CRITICALITY

FILED OF THE INVENTION AND PRIOR ART

The present invention is related to a computer device according to the preamble of claim 1 and a method for executing softwares of different criticality.

Different kinds of computer devices and softwares are used to an increasing extent within many different fields for performing more and more tasks. This use increases also within fields with very high security requirements, such as for instance nuclear power and avionics. As the performance of such computer devices has increased also the number of softwares installed in and executed by the same computer device has increased as well as the complexity for each individual software. However, all softwares in a computer device are not equally critical as regards security. In such situations the criticality of the software is usually classified according to some standard. The term "criticality" in this description and the following claims is related to how critical to the security it is that a certain software works, that is how serious the consequences are when the software does not work. Software of high criticality is very important and essentially always has to work, whereas the function of a software with lower criticality not is as critical to the security. Development of software of high criticality is, however, very costly compared to development of software of lower criticality. When there are softwares of different criticality in a computer device, there is a risk of software of lower criticality affecting software of higher criticality. This implies that software of lower criticality, which in a computer device is intended to co-operate with soft-

ware of higher criticality, also has to be developed to comply with the requirements for the higher criticality, which results in large development costs for software.

SUMMARY OF THE INVENTION

The object of the present invention is to provide a computer device of the initially mentioned kind, which enables execution of softwares of different criticality in the same computer device with high security level, without software of lower criticality having to comply with the security requirements for the higher criticality.

According to the invention, this object is achieved in that the execution means is a Central Processing Unit (CPU), that the device is adapted to fetch input data stored in a first memory included in the computer device and store output data in the first memory when executing the first software, and fetch input data stored in a second memory included in the computer device and store output data in the second memory when executing the second software, the second software being prevented from affecting data stored in the first memory, and that the first software is adapted to control which output data that are transferred from the first and second memory to said arrangement to thereby prevent the second software from independently changing any state outside the device. Thus, such a device enables introduction of software of high criticality in computer devices comprising software of lower criticality in an economically favourable manner, since costly qualification of software of low criticality into the higher criticality not is necessary. Accordingly, the computer device according to the present invention makes it possible to handle a plurality of softwares of different criticality in one and the same computer device using one single Central Processing Unit (CPU), without software of lower criticality having to comply with the security requirements for the higher criticality. This is cost efficient as well as space–saving.

According to a preferred embodiment of the present invention, the device has means for controlling access to data in the first memory, the control means being adapted to be in a first position when executing the first software, in which access to data in the first memory is enabled for the first software, and be in a second position when executing the second software, in which access to data in the first memory is disabled for the second software. In its second position, the control means prevents the second software from accessing data in the first memory and, accordingly, it is ensured that the second software cannot affect data stored in the first memory, and especially not input data to or output data from the first software.

According to another preferred embodiment of the invention, the control means is adapted to control access also to other components included in the computer device than the first memory in such a manner that access to said components is enabled when the control means is in the first position but disabled when the control means is in the second position. This results in the second software being prevented from independently changing any state inside the device.

The invention is also related to a method for executing software of different criticality according to claim 14.

Further advantages and advantageous features of the invention are apparent from the following description and the other dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Below follows a description of preferred embodiments of the invention cited as examples with reference to the appended drawings, on which:

Fig 1 is a block diagram illustrating a computer device according to a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

In fig 1 is shown a block diagram of the main components in a computer device according to a preferred embodiment of the present invention. The device comprises a means 1 for executing software, preferably a Central Processing Unit (CPU), which via a data bus 2 communicates with a memory 3, preferably of the type Random Access Memory (RAM). Included in the device is also a storage means 4, for instance in the form of a memory of the type Programmable Read Only Memory (PROM), with which the execution means 1 communicates via the data bus 2. All software in the computer device is stored in the storage means 4, comprising at least a first software of a first criticality and a second software of a second criticality, the first criticality being higher than the second criticality. The first software thus has a classification implying that errors in the function of the first software have a larger influence on the security compared to the influence on the security that errors in the function of the second software have. Thus, it is more critical to the security that the first software functions correctly than that the second software functions correctly. As an explaining example may be mentioned that in a conceivable use of the present invention in an aircraft, software of higher criticality may for instance be software being necessary for the control system of the aircraft, whereas software of lower criticality for instance may be software for providing different kinds of information, for example concerning weather conditions. It is pointed out that this is not at all limiting the invention in any way, it is only to consider as an example cited for the purpose of explanation.

Furthermore, the device comprises a group 5 of hardware components, comprising a memory 6, preferably of the type Random

Access Memory (RAM), an arrangement 7 for data input to and data output from the device, an interrupt handler 8 and a clock 9. A monitoring circuit 10 may also be included in the device as shown in fig 1, but it is pointed out that this circuit 10 may be omitted as well. The arrangement 7 may for instance comprise conventional units for data input/output such as for instance keyboard, monitor, different types of sensors and switch members etc. However, the invention is not in any way limited to the number or type of units for data input/output being comprised in the arrangement 7.

Different kinds of interrupts generated in the computer device are supplied to the execution means 1 via the interrupt handler 8. These interrupts may for instance be caused by the arrangement 7, the clock 9 and the monitoring circuit 10. Although only one clock 9 is illustrated in fig 1, it is to be understood that the number of clocks included in the device may be varied. It is also to be understood that the number of monitoring circuits is optional. The different interrupts are preferably divided into Maskable Interrupts and Non Maskable Interrupts (NMI). Each time an interrupt is generated in the computer device and supplied to the execution means 1 via the interrupt handler 8, the execution means 1 take a predetermined measure, which also includes ignoring the interrupt in question. In this description and in the following claims "Maskable Interrupts" relates to a type of interrupts which temporarily may be ignored by the execution means 1, for instance in order to finish the task in progress, and "Non Maskable Interrupts" or "interrupts of the type NMI" relates to interrupts which cannot be ignored by the execution means 1 and thus have to be attended to immediately.

The computer device is adapted to fetch input data stored in the memory 6 and store output data in the memory 6 when executing the first software, and fetch input data stored in the memory 3 and store output data in the memory 3 when executing the second software. In this manner, output data from the second

software is prevented from affecting input data to or output data from the first software.

The first software is adapted to control which output data that are transferred from the memory 6 and the memory 3 to the arrangement 7 to thereby prevent the second software from independently changing any state outside the device. For example, this is achieved in that the first software checks the output data generated by the second software which are to be transferred from the memory 3 to the arrangement 7.

Furthermore, the computer device comprises means 11, for instance in the form of at least one logic circuit, for controlling access to data in the memory 6. The control means 11 is adapted to be in a first position when executing the first software, in which access to data in the first memory 6 is enabled for the first software, and be in a second position when executing the second software, in which access to data in the first memory 6 is disabled for the second software. This implies that the execution means 1 is allowed the read, write and delete data in the memory 6 when executing the first software, but is not allowed to read, write or delete data in the memory 6 when executing the second software. Hereby, it is ensured that output data from the second software actually cannot affect data stored in the memory 6 and thus cannot affect input data to or output data from the first software.

In the embodiment according to the invention illustrated in fig 1, the control means 11 is adapted to control access also to other components included in the computer device than the memory 6, for instance the components included in the group 5: the arrangement 7, the clock 9 and the monitoring circuit 10, in such a manner that access to said components is enabled when the control means 11 is in the first position but disabled when the control means 11 is in the second position. Thus, the execution means 1 does not have access to said components when exe-

cuting the second software, whereby the execution means 1 is prevented from changing any state inside the computer device while executing the second software. It is to be understood that said components, to which the control means 11 controls access, comprise every component included in the computer device being able to affect the security critical operation of the device in any way. Consequently, the control means 11 may control access to more or fewer components than illustrated in fig 1.

Preferably, the control means 11 is adapted to be manoeuvrable into its first position by means of an interrupt generated in the computer device, preferably of the type NMI, and manoeuvrable into its second position by means of the first software. The control means is, accordingly, manoeuvrable into the first position by the execution means 1 at supply of an interrupt, which preferably is of the type NMI, via the interrupt handler 8 to the execution means 1 and manoeuvrable into the second position by the execution means 1 when executing the first software. Furthermore, the first software is preferably adapted to be activatable by an interrupt, preferably of the type NMI, generated in the computer device.

As mentioned hereinabove, the interrupts in the preferred embodiment of the present invention, by means of which the control means 11 is manoeuvrable into its first position and by means of which the first software is adapted to be activatable, are preferably of the type NMI. This is, however, by no means any limitation of the invention, it is only one possible preferred embodiment. It is emphasised that also other interrupts may be utilised for achieving manoeuvring of the control means and activation of the first software. If other interrupts than interrupts of the type NMI are used, it has to be made sure that the first and second software does not use instructions which disable the interrupts, which could obstruct activation of the first software and manoeuvring of the control means. Furthermore, in this case it has to be ensured that upon interrupts, which manoeuvre the control

means into its first position, execution of the first software is started immediately in order to in that way eliminate the possibilities for the second software to get access to the components to which the control means controls access, since then the first software can manoeuvre the control means into its second position before execution of the second software is started.

The preferred use of interrupts of the type NMI is further advantageous from a security point of view, as thereby it is ensured that activation of the first software always will take place irrespective of what the execution means 1 is doing or has done when such an interrupt occurs, since the execution means 1 cannot ignore such an interrupt. Thus, the execution means 1 will always execute the first software when an interrupt of the type NMI generated in the computer device is supplied to the execution means 1 from the interrupt handler 8. Accordingly, it is possible to prevent the computer device from being put in a state, which it is incapable of changing, i.e. that the computer device "gets stuck" in an infinite loop or corresponding state. For example, this may be prevented in that the first software causes the clock 9 to generate an interrupt of the type NMI if a certain number of time steps elapses without any events occurring.

Furthermore, the second software is adapted to be activatable by means of the first software, which implies that the first software is able to instruct the execution means 1 to start execution of the second software.

Below follows a description of the function of a computer device according to the present invention.

The computer device is started, usual start-up and built-in tests being performed. During these built-in tests also the function of the control means is tested. At this start, the control means 11 is in the first position, but after the built-in tests it is brought to the second position and the first software waits in an infinite loop.

When an interrupt, preferably of the type NMI, is generated in the computer device, the control means 11 is manoeuvred into the first position and execution of the first software is started, input data to the first software being read into the memory 6 from the arrangement 7 at first, and then input data is fetched from the memory 6 and output data is stored in the memory 6 during the execution. Input data required for execution of the second software is read into the memory 3 from the arrangement 7, after which the control means 11 is manoeuvred by the first software into the second position and the second software is activated by the first software, that is the first software makes sure that execution of the second software is started. At this execution of the second software, input data is fetched from the memory 3 and output data is stored in the memory 3. At next generation of an interrupt, preferably of the type NMI, at which the control means 11 is manoeuvred into the first position, output data are transferred from the memory 6 and the memory 3 to the arrangement 7, the first software controlling which output data that are transferred and thereby preventing the second software from independently changing any state outside the device. This control may for instance comprise that the first software checks output data generated by the second software which shall be transferred from the memory 3 to the arrangement 7. Subsequently thereto, the control means 11 is manoeuvred into the second position by the first software and a new interrupt, preferably of the type NMI is waited for, at which the execution method described above is repeated.

In this way it is efficiently and with high reliability ensured that, at execution of the second software, output data therefrom cannot affect either input data to or output data from the first software and it is also ensured that the second software independently cannot change any state outside the device.

The invention is not in any way limited to the embodiments described above, but many possibilities to modifications thereof

will be apparent for a person with ordinary skill in the art without departing from the basic idea of the invention.

It is emphasised that although only one first software of a first criticality and one second software of a second criticality, which is lower than the first criticality, have been described in the preferred embodiments above, it is to be understood that of course an optional number of softwares may exist. For example, a usual use of the present invention will probably include one software of a first criticality and a plurality of second softwares of another criticality, which for each of the plurality of second softwares is lower than the first criticality.

Claims:

1. A computer device comprising storage means (4) containing at least a first software of a first criticality and a second software of a second criticality, the first criticality being higher than the second criticality, means (1) for executing the first and second software and an arrangement (7) for data input to and data output from the device, **characterized** in that said execution means (1) is a Central Processing Unit (CPU), that the device is adapted to fetch input data stored in a first memory (6) included in the computer device and store output data in the first memory (6) when executing the first software, and fetch input data stored in a second memory (3) included in the computer device and store output data in the second memory (3) when executing the second software, the second software being prevented from affecting data stored in the first memory, and that the first software is adapted to control which output data that are transferred from the first and second memory to said arrangement (7) to thereby prevent the second software from independently changing any state outside the device.

2. A computer device according to claim 1, **characterized** in that it comprises means (11) for controlling access to data in the first memory (6), the control means (11) being adapted to be in a first position when executing the first software, in which access to data in the first memory (6) is enabled for the first software, and be in a second position when executing the second software, in which access to data in the first memory (6) is disabled for the second software.

3. A computer device according to claim 2, **characterized** in that the control means (11) is adapted to control access also to other components (7, 9, 10) included in the computer device than the first memory (6) in such a manner that access to said components (7, 9, 10) is enabled when the control

means (11) is in the first position but disabled when the control means (11) is in the second position.

4. A computer device according to claim 2 or 3, **characterized** in that the control means (11) is adapted to be manoeuvrable into its first position by means of an interrupt generated in the computer device.

5. A computer device according to claim 4, **characterized** in that said interrupt is of the type Non Maskable Interrupt (NMI).

6. A computer device according to any of the claims 2-5, **characterized** in that the control means (11) is adapted to be manoeuvrable into its second position by means of the first software.

7. A computer device according to any of the claims 2-6, **characterized** in that the control means (11) comprises at least one logic circuit.

8. A computer device according to any of the preceding claims, **characterized** in that the first software is adapted to be activatable by means of an interrupt generated in the computer device.

9. A computer device according to claim 8, **characterized** in that said interrupt is of the type Non Maskable Interrupt (NMI).

10. A computer device according to any of the proceeding claims, **characterized** in that the second software is adapted to be activatable by means of the first software.

11. A computer device according to any of the preceding claims, **characterized** in that the first memory (6) is of the type Random Access Memory (RAM).

12. A computer device according to any of the preceding claims, **characterized** in that the second memory (3) is of the type Random Access Memory (RAM).

13. A computer device according to any of the preceding claims, **characterized** in that the storage means (4) is a memory of the type Programmable Read Only Memory (PROM).

14. A method for executing softwares of different criticality, **characterized** in that execution of said softwares is performed by a Central Processing Unit (CPU), that input data stored in a first memory (6) is fetched and output data is stored in the first memory (6) when executing a first software of a first criticality and input data stored in a second memory (3) is fetched and output data is stored in the second memory (3) when executing a second software of a second criticality, which is lower than the first criticality, the second software being prevented from affecting data stored in the first memory, and that output data are transferred from the first and second memory to an arrangement (7) for data input and output, the first software controlling which output data that are transferred and thereby preventing output via the arrangement (7) of output data from the second software which have not been checked by the first software.

1/1

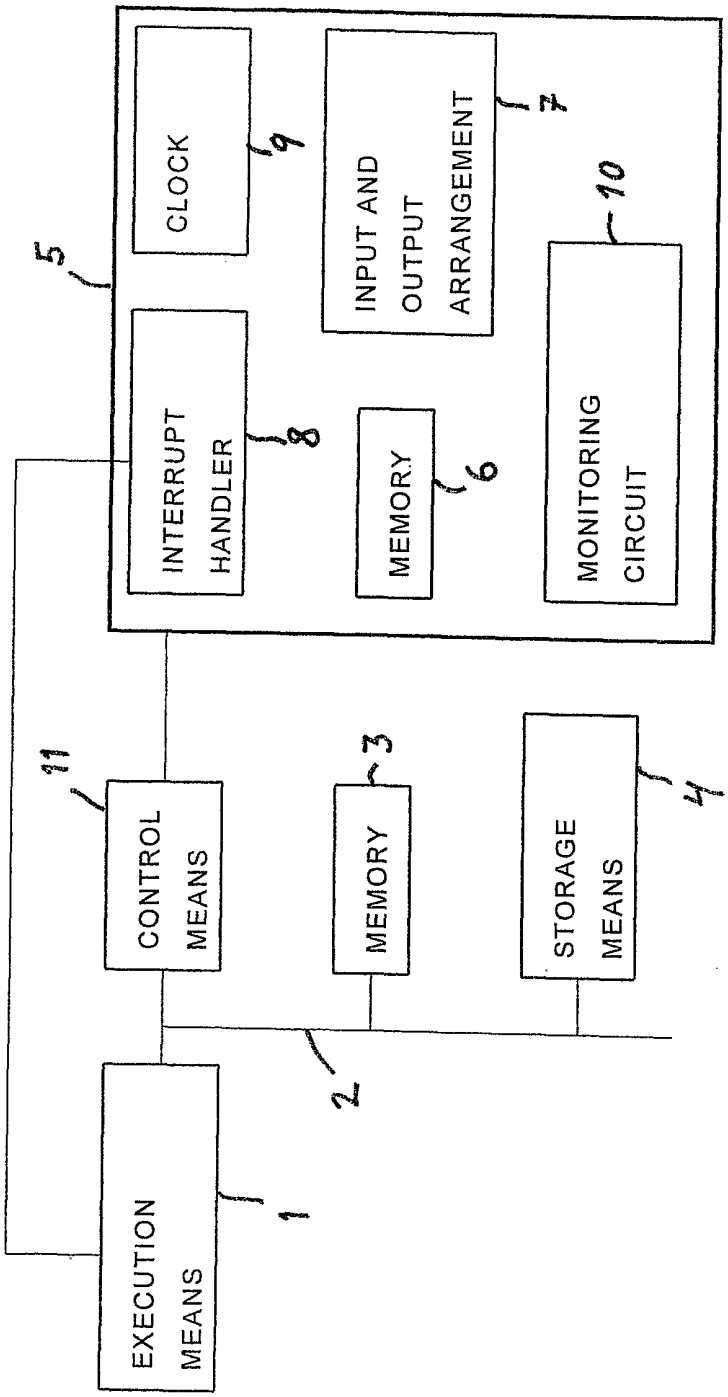

EXECUTION MEANS
1
2
CONTROL MEANS
11
MEMORY
3
STORAGE MEANS
4
5
CLOCK
9
INPUT AND OUTPUT ARRANGEMENT
7
INTERRUPT HANDLER
8
MEMORY
6
MONITORING CIRCUIT
10

Fig 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/02660

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 13/00, G06F 11/16
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)

IPC7: G06F

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

SE,DK,FI,NO classes as above

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5630057 A (HAIT), 13 May 1997 (13.05.97), column 6, line 3 - line 45	1,8-14
A	US 4698785 A (DESMOND ET AL), 6 October 1987 (06.10.87)	1,8-14
A	US 5822511 A (KASHYAP ET AL), 13 October 1998 (13.10.98), figure 5	1,8-14
A	US 5421006 A (JABLON ET AL), 30 May 1995 (30.05.95), claims 1-19	1-14

☐ 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	Date of mailing of the international search report
11 March 2002	12 -03- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Fernando Farieta/BS Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SE 01/02660

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5630057 A	13/05/97	AU 3840689 A	12/01/90
		CA 1340351 A	26/01/99
		EP 0382811 A	22/08/90
		US 5581763 A	03/12/96
		WO 8912864 A	28/12/89
US 4698785 A	06/10/87	DE 3485511 A	26/03/92
		EP 0144226 A,B	12/06/85
US 5822511 A	13/10/98	NONE	
US 5421006 A	30/05/95	NONE	