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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
18 October 2007 (18.10.2007)

PCT

(10) **International Publication Number**
WO 2007/117172 A1

(51) **International Patent Classification:**
G05B 19/04 (2006.01) ***G05B 19/05*** (2006.01)

(21) **International Application Number:** PCT/RU2006/000172

(22) **International Filing Date:** 7 April 2006 (07.04.2006)

(25) **Filing Language:** English

(26) **Publication Language:** English

(71) **Applicant** *(for all designated States except US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 Muenchen (DE).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only)*: **KRUCHININ, Andrei Alexandrovich** [RU/RU]; Dundicha Street 36-1-366, St.Petersburg, 192289 (RU). **MISYUCHENKO, Igor** [LT/RU]; Komendantsky r. 23-1-6, St.Petersburg, 199406 (RU).

(74) **Agent: LAW FIRM "GORODISSKY & PARTNERS" LTD**; EGOROVA Galina Borisovna , B.Spasskaya Str., 25, Stroenie 3, Moscow, 129010 (RU).

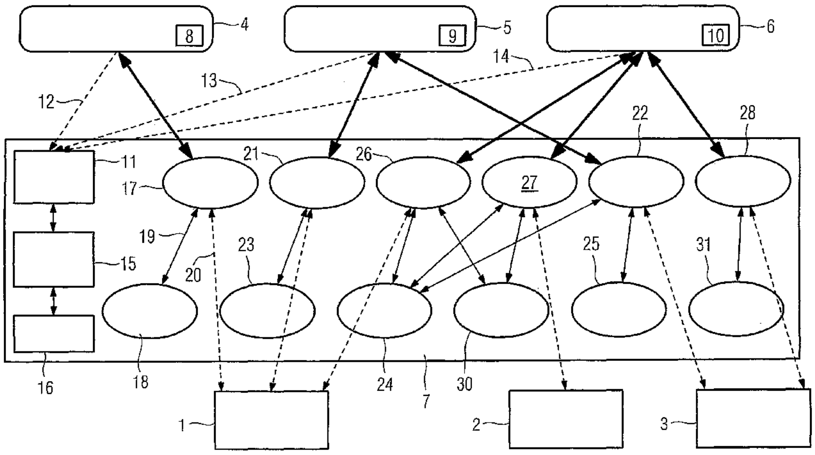
(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (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.

(54) **Title:** AUTOMATION NETWORK, REMOTE ACCESS SERVER FOR AN AUTOMATION NETWORK AND A METHOD FOR TRANSMITTING OPERATING DATA BETWEEN AN AUTOMATION SYSTEM AND A REMOTE COMPUTER



(57) **Abstract:** The invention relates to an automation network, a remote access server (7) for an automation network and a method for transmission of operating data between an automation system with one or more automation devices (1..3) and a remote computer (4...6) with the operating data of the automation device (1..3) being transmitted via the Internet or an intranet and displayed and/or changed on the remote computer (4...6) by an Internet browser (8...10). The remote access server (7) provides the operating data for the remote computer (4...6) and, for a session-oriented access, creates a software object (17, 21, 22, 26...28) as an image of the automation device (1...3) and, if changes are to be made to the operating data by the access, a software object (18, 23...25, 30, 31) for simulation of the automation device (1...3) and/or of the process to be controlled by the automation device, so that any changes can be checked for permissibility and/or validity before being forwarded to the automation device (1...3).

Description

Automation network, remote access server for an automation network and a method for transmitting operating data between an automation system and a remote computer.

The invention relates to an automation network with at least one automation device and at least one remote computer in accordance with the preamble of claim 1, a remote access server for an automation network in accordance with the preamble of claim 7 and a method for transmission of operating data between an automation system and a remote computer in accordance with the preamble of claim 8.

The term automation device is understood to be a device that processes a control program for controlling a process. Such devices are frequently known as programmable logic controllers (PLC) or controllers, or soft PLC. An automation device can be of modular construction and have a programmable central unit and intelligent modules that undertake individual automation functions, for example, weighing, axes control, closed-circuit control etc.. To connect to a communication network used to exchange data with other components of an automation network, such as network components or field units or other automation devices, an additional module, known as a communication processor, can be provided. Several automation devices participating in an automation project and networked with each other via a communication network are known as an automation system.

From US 6,151,625 A, a programmable logic controller is known that has a web interface for communication via the Internet or intranet. In this way, a client/server system was created that offered operators a similar user-friendly user interface as general access services in the web. The web is a network of documents, also known as pages and stored on server computers distributed throughout the world. Normally a page contains text, multimedia offerings, such as graphic images, video or audio data as well as Hypertext links to other documents. A browser enables the user to read the pages and interactively select from the possibilities offered on the page. The browser is a graphics program that transmits the Internet requests to a page and displays information which are available on the page. The web interface integrated into the programmable logic controller enables a user to call up and display the operating data of the programmable logic controller by means of a browser. The operating data can be data on control configurations, process data such as input and output values, register states, statistical data, diagnostic data or configuration data of input-output interfaces. To operate and monitor the automation device with a Human Machine Interface (HMI), a remote computer with an Internet connection and a browser, for example Navigator from Netscape Communications or Internet Explorer from Microsoft, is sufficient.

The known arrangement for transmission of data between an automation device and a remote computer for operating and monitoring the automation device has the disadvantage that high data transmission rates are required on the communication network, particularly where video data is used. Furthermore, it is possible to make changes via the remote computer to the operating data of the automation system, that could jeopardize a secure operation or lead to damage to the controlling process. Even when intentional changes may lie within a permissible range for an individual automation device, unfavorable combinations with the operating data of other automation devices and the process environment can cause damage to the process to be controlled. A further disadvantage is to be seen in that access conflicts can occur if several remote computers want to access the operating data of the same automation device at the same time. A part of the computing power of the automation device is also taken up for communication with the remote computer. Therefore, it can occur in a disadvantageous manner that a remote computer wants to access the operating data of an automation device at a timepoint at which the particular automation device does not have sufficient free computing power available to communicate with the remote computer. An automation device that is accessible via the Internet to a remote computer also has the disadvantage that unauthorized access, hacker attacks, can be perpetrated against the automation device.

The object of the invention is therefore to provide an automation network, a remote access server for such an automation network and a method for transmission of operating data between an automation system and a remote computer, by means of which changes to the operating data of the automation system, that are made from a remote computer and could possibly be damaging to the process or the process control, can be avoided.

To achieve this objective, the automation network of the type mentioned in the introduction is provided with the features given in the characterizing portion of claim 1. A corresponding remote access server for an automation network and a method for transmission of operating data between an automation system and a remote computer are described in claims 7 and 8. Advantageous further developments of the invention are given in the dependent claims.

One or more automation devices are thus arranged downstream a remote access server, so that the communication of a remote computer must initially be carried out with the remote access server before changes to the operating data can affect the automation functions and the controlling process. The remote access server can be a device that is allocated to one or more automation devices, but separated from them. In an advantageous manner, the connection for data transmission between the automation device and remote access server can be designed as a network of automation field communication and be connected to several automation devices at this network. This has the advantage that an individual remote access server can be used for several automation devices. The remote access server can thus be used in a wide range of different network architectures and equally enables a data link to an automation device in the simplest architecture and operation in a network with several connected automation devices, i.e. an automation system.

As an alternative to this, it is of course also possible to integrate the remote access server as a component in an automation device or something called an Applet in the browser of the remote computer.

The invention also has the advantage that in the automation device, the task of the communication with the remote computer is separate from the actual control task. This leads to an improved, faster communication service for operators located distant from the automation device and has advantages for protecting the automation device from attacks. By means of the invention, access by a remote operator to the automation device is substantially accelerated because the remote access server is not engaged in the actual control task.

A software object as an image of the automation device is a simplified model of the real automation device that is called up by the remotely-located operator. The degree of detail of the model can depend on the access authorizations of the particular operator. Similarly, a software object with simulation of the automation device or of the process to be controlled by the automation device is a simplified model of the real industrial process to be controlled. Operating data from various automation devices and project information can be used to simulate the process behavior. The model of the process to be controlled by the automation device can be "comprehensive" or "small" or also "blank", depending on the access authorizations of the operator. In the latter case, the created software object does not include the simulation of the process to be controlled by the automation device. In an advantageous manner, the created software objects as an image of the automation device or for simulation of the automation device and/or of the process to be controlled by the automation device are essentially of a simpler design than models that are used for troubleshooting and testing the control software of automation devices. The software objects need merely to provide the operator with a general overview of comparatively few parameters of the automation device. For this purpose, the data of the software objects can be periodically updated by the automation device. The rate of updating for such software objects can, however, in an advantageous manner be set substantially lower than would be necessary for operating and monitoring functions.

The use of software objects in this case has the advantage that the scope of the interaction between the remote operator and the automation device can be scaled to a wide range. Pre-processing of data from several automation devices is thus possible, to create a view of the system for the remote operator.

The simplified models of the automation device and/or process can be session-oriented and created according to the access authorizations of the operator. In this way, the degree of modeling can be matched to the particular security and quality requirements. Visualization can be restricted to the details of the controlling process which are critical for the particular session.

If the inputs of the operator are impermissible, the software object can output a corresponding notice in an advantageous manner to the user as an image of the automation device or for simulation of the automation device and/or of the process to be controlled by the automation device.

If changes to the operating data of the automation device are buffer stored before being transmitted to the automation device by the remote access server, this has the advantage that a session-oriented access of the operator can be ended without the changes being effective on the real automation device.

If a software object created for simulation of the process to be controlled by the automation device is not cancelled at the end of the operator access, this has the advantage that it can be used for the purposes of system control, for example to create a short-term prognosis of the dynamic process behavior or to detect any dangerous process development. A continuous software object of this kind can be created at the instigation of the remote operator. A permanent software object as an image of the automation device in a similar manner can, for example, be used to back up the operating data of the automation device.

Furthermore, it is possible that a software object can itself after its reliability has been established, make changes to the process. The software object in this case undertakes actual control tasks.

Furthermore, the remote access server can be advantageously provided with a security unit by means of which operators wishing to access the operating data of automation devices behind the remote access server can be identified and authorized. The security checks therefore take place at a point before the automation devices and the automation devices locating behind it are therefore better protected against attacks. The operating programs of the remote access server can be designed to be safer against attacks than those of the automation device, because the remote access server does not perform any control functions. Moreover, various solutions can be used to identify and authorize users. It is possible in a simple manner to integrate further security devices in the remote access server. The security unit can be realized by a portal to the automation system that has a program permanently running on the remote access server and is responsible for identification, authentication and authorization of the remote operator. As one of many possible ways of realizing a deposit of credentials, as they are called, a list of devices the operating data of which can be accessed, a list of authorized operators, including their passwords and access authorizations can be stored in a service database. Additional information on other available network nodes, the computing power of which is not completely utilized and that can still undertake computing-intensive tasks, can be collected and stored in this database.

The availability of operating data can be limited in a simple manner to the particular existing access authorizations of an operator, if the remote access server has a list of services from which available services can be chosen depending on the authorization of the operator.

This list of services can, for example, be presented as an image of a production line with links to the individual production cells and the automation devices contained therein, that an operator can access via the remote access server. The advantage of this is that project information that is not present on an individual automation device is accessible to the user. By means of session-oriented visualization of selected details of the process to be controlled, the data traffic to be transmitted via the communication network during a session can also be reduced. A pre-processing of data from various automation devices provides the remote operator with a view of the production sequence controlled by an automation system.

The degree of detailing and the complexity of the software objects can be advantageously matched to the scope of the particular access if the software objects are created corresponding to the particular services.

By means of the simplified modeling of the automation device and of the process, and also due to the reduced updating rate, the data traffic and consumption of resources within the automation network, connected to a session-oriented access, is reduced.

Furthermore, in an advantageous manner, the remote access server can be designed in such way that other nodes of the automation network are monitored for the availability of unused computing power and software objects created on a node with sufficient existing, free computing power. An agent for resource monitoring, located on the remote access server and/or the node, as a program permanently running in the background, can be created for this purpose. This is responsible for updating the information stored in the service database, regarding the unused computing power of the nodes arranged in the automation network. By better use of the computing power present in the automation network, a fast reaction to session-oriented access is enabled, even if the computing power of the automation device to which access is required is engaged in other tasks.

If an operator wants to carry out a test and a fault rectification or a video-supported operation on an automation system, this requires a higher rate of data flow to the remote computer. In this case, it is possible to use protocols on the intranet or Internet with a high data throughput. For example, a high data throughput with the known Realtime Transport Protocol (RTP) with realtime protocol conversion on the remote access server can be achieved. A plug-in to enable the high data rate to be realized is used in the standard browser of the remote computer for this purpose.

Using the drawings showing an example of an embodiment of the invention, configurations and advantages are explained in more detail in the following.

The illustrations are as follows.

Figure 1 An automation network with a remote access server.

Figure 2 A flow diagram of a session-oriented access through a remote computer

In the example of an embodiment shown, an automation network has three automation devices 1, 2 and 3 and three remote computers 4, 5 and 6 that are connected to each other via the Internet or an intranet as a communication network. The topology of the communication network can moreover be configured as required. Access by the remote computer 4, 5 or 6 to operating data of the automation devices 1, 2 or 3 takes place via a remote access server 7, that for example can be formed as an additional device in the automation network. As an alternative to this, it is possible to realize the remote access server by a permanently running software module that is located at any node of the automation network. The remote computers 4, 5 and 6 are each provided with a web browser 8, 9 or 10 to display the operating data on the remote computer 4, 5 or 6. The function of the remote access server 7 is similar to that of a gateway arranged between the Internet and the local area network (LAN). Accesses of the remote computers 4...6 are initially controlled by something called a control system portal 11, as shown by arrows 12, 13 and 14, indicated by broken lines. By means of a service database 15, the access authorizations are checked by the portal 11. The portal 11 is responsible for identification, authentication and authorization of a user who wants to gain access via one of the remote computers 4, 5 or 6. For this purpose, authorization rights stored in the service database 15 in a list of authorized users, with their passwords, is checked to determine whether the particular operator is authorized to make the required access. The nodes of the automation network on which unused computing power is available are also stored in the service database 15. It is thus possible to react comparatively quickly to access requests because bottlenecks due to computing power can be almost completely precluded. The monitoring of free resources is carried out by an agent 16 that belongs to the remote access server 7 and continuously updates the service database 15. For a clear representation of the services available, there is also a list of services on the remote access server 7, that consists of a block diagram of the production line with links to the individual production cells and to the automation devices that can be reached via the remote access server 7. This diagram can be realized by a web page, displayed by means of accesses 12, 13, 14 to the portal 11 with the aid of browser 8, 9, 10. Accesses to operating data of the automation devices 1…3 are processed, session oriented, in the remote access server 7. For example with an access 12 of the remote computer 4 to operating data of the automation device 1, the portal 11, after checking the necessary access authorizations, creates a software object 17 as an image of the automation device 1 and a software object 18 for simulation of the automation device 1 and the process controlled by the automation device 1. As shown by an arrow 19, a data exchange takes place between the software objects 17 and 18 for validation, i.e. for checking the validity of changes carried out to operating data. Only after validation do the changes become effective by transmission to the automation device 1 as shown by arrow 20. This avoids impermissible changes being made to operating data and damage that could occur to the controlling process. After creation of the software object 17, the data exchange takes place between the remote computer 4 and only the software object 17, because it contains an image of the operating data of the automation device 1. The operating security of the automation device 1 is improved in this way. The complexity and degree of detailing of the software objects 17 and 18 depend on the particular access authorizations and the extent of the intended changes or requests for operating data. It can therefore be a comparatively simple model of the automation device and the process to be controlled. The data of the automation device 1 required in the modeling is periodically updated. The updating rate required for this is essentially lower than for normal operating and monitoring systems. In a corresponding manner to access 12, with access 13 by the remote computer 5 a software object 21 as an image of the automation device 1, a software object 22 as an image of the automation device 3, a software object 23 and a software object 24 for simulation of the automation device 1 and of the process to be controlled by the automation device 1 and a software object 25 for simulation of the automation device 3 and the process to be controlled by the automation device 3 is created. In the same way, in the event of an access 14 by the remote computer 6 to the portal 11, software objects 26, 27 and 28 are created as images of the automation devices 1, 2 or 3 and software objects 30 and 31 for simulation of the automation devices 2 and 3 and the processes controlled by these. When accesses 12…14 by remote computers 4…6 are completed, the software objects 17, 18, 21…28, 30, 31 created to process the accesses are again cancelled, to release the required computing power.

The sequence of an access by a remote computer to operating data of an automation device or an automation system consisting of several devices is explained in more detail in the following with the aid of the flow diagram in figure 2. Access begins at step 40 with an access request by a remote computer to a portal of a remote access server. In step 41, the portal receives the access request, identifies and authenticates the operator that made the access request and allocates him/her the access authorizations that are stored in a database. During an enquiry 42, the access authorizations are checked to determine whether they are sufficient for the required extent of the access. If this is not the case, the process ends here. Otherwise, a transition to step 43 takes place in which the portal specifies the distribution of the necessary software objects to nodes of the automation network and creates the accorded access rights corresponding to the called-up automation devices. The session-oriented access is then switched to the created software objects. If absolutely no changes to the operating data are intended during an access request, a direct transition through a branch 44 to step 45 takes place, in which after completion of the access, the software objects created for the access are again deleted. If changes are intended, a transition to step 46 takes place in which additional software objects for simulation of the called-up automation devices and/or the process to be controlled by the automation device are created. In an enquiry 47, a check is first performed to determine whether the intended changes to the operating data lie within a permissible range. If this is not the case, then in step 48 a notice is output to the operator that the change to the operating data is not permissible. The operator can then correct his/her inputs and a return to branch 44 takes place. If, however, the intended changes are within a permissible range, a simulation with the changed operating data is carried out in step 49 by the created software objects. This simulation serves to validate the changes. If the simulation shows that the intended changes to the operating data are invalid, for example would lead to damage to the controlling process, a skip in branch 50 to step 48 takes place in which a corresponding notice is output to the operator. If on the other hand the intended changes prove to be valid, the new operating data is transferred in steps 51 to a waiting queue, containing any other existing changed operating data for transmission to the relevant automation device(s). After the requested changes to the operating data have been carried out by the relevant automation devices, the software objects created for the session-oriented access are cancelled in step 45 and the process ends in step 52. The resources required for the access are thus released.

Claims

1. Automation network with at least one automation device (1…3) and with at least one remote computer (4…6), with the operating data of the automation device (1…3) being transmitted via the Internet or an intranet and represented and/or changed on the remote computer (4…6) by an Internet browser (8…10), characterized in that a remote access server(7)is present for the provision of operating data of the automation device (1…3) for the Internet browser (8…10) of the remote computer (4…6), with the remote access server (7) being configured to create, for a session-oriented access, a software object (17, 21, 22, 26…28) as an image of the automation device (1…3) and, if changes to the operating data are to be undertaken by the access, a software object (18,23…25, 30, 31) for simulation of the automation device (1…3) and/or the process to be controlled by the automation device, so that any changes can be checked for permissibility and/or validity before forwarding to the automation device (1…3).

2. Automation network in accordance with claim 1, characterized in that the remote access server (7) has a security unit (11) for identification and authorization of operators accessing the operating data of the automation device (1…3).

3. Automation network in accordance with claim 1 or 2, characterized in that the remote access server (7) contains a list of services from which available services can be chosen according to the authorization of the operator.

4. Automation network in accordance with claim 3, characterized in that the software objects (17, 18, 21…28, 30, 31) can be created corresponding to the particular available services.

5. Automation network in accordance with one of the preceding claims, characterized in that the remote access server (7) is designed to monitor other nodes of the automation network for availability of unused computing power and to create software objects on a node with sufficient unused computing power.

6. Automation network in accordance with one of the preceding claims, characterized in that its functions can be carried out on several nodes of the automation network for a distributed or redundant realization of the remote access server.

7. Remote access server for an automation network with at least one automation device (1…3) with at least one remote computer (4…6) with operating data of the automation device (1…3) being transmitted via the Internet or an intranet and displayed on the remote computer (4…6) by an Internet browser (8…10) and/or changed, characterized in that the remote access server (7) is designed so as to provide operating data of the automation device (1..3) for the Internet browser (8…10) of the remote computer (4…6) and, for a session-oriented access, to create a software object (17, 21, 22, 26…28) as an image of the automation device (1…3) and, if changes to the operating data are to be carried out by the access, a software object (18, 23…25, 30, 31) for

simulation of the automation device (1…3) and/or of the process to be controlled by the automation device, so that any changes can be checked for permissibility and/or validity before forwarding to the automation device (1…3).

8. Method for transmission of operating data between an automation system with one or more automation devices (1…3) and a remote computer (4…6), with operating data of the automation device (1…3) being transmitted via the Internet or an intranet and displayed and/or changed on the remote computer (4…6) by an Internet browser (8…10), characterized in that a remote access server (7) is used to provide the operating data of the automation device (1…3) for the Internet browser (8…10) of the remote computer (4…6), with the remote access server (7) creating, for a session-oriented access, a software object (17, 21, 22, 26…28) as an image of the automation device (1…3) and, if changes are to be made to the operating data by the access, a software object (18, 23…25, 30, 31) for simulation of the automation device (1…3) an/or the process to be controlled by the automation device, so that any changes can be checked for permissibility and/or validity before being forwarded to the automation device (1…3).

FIG 1

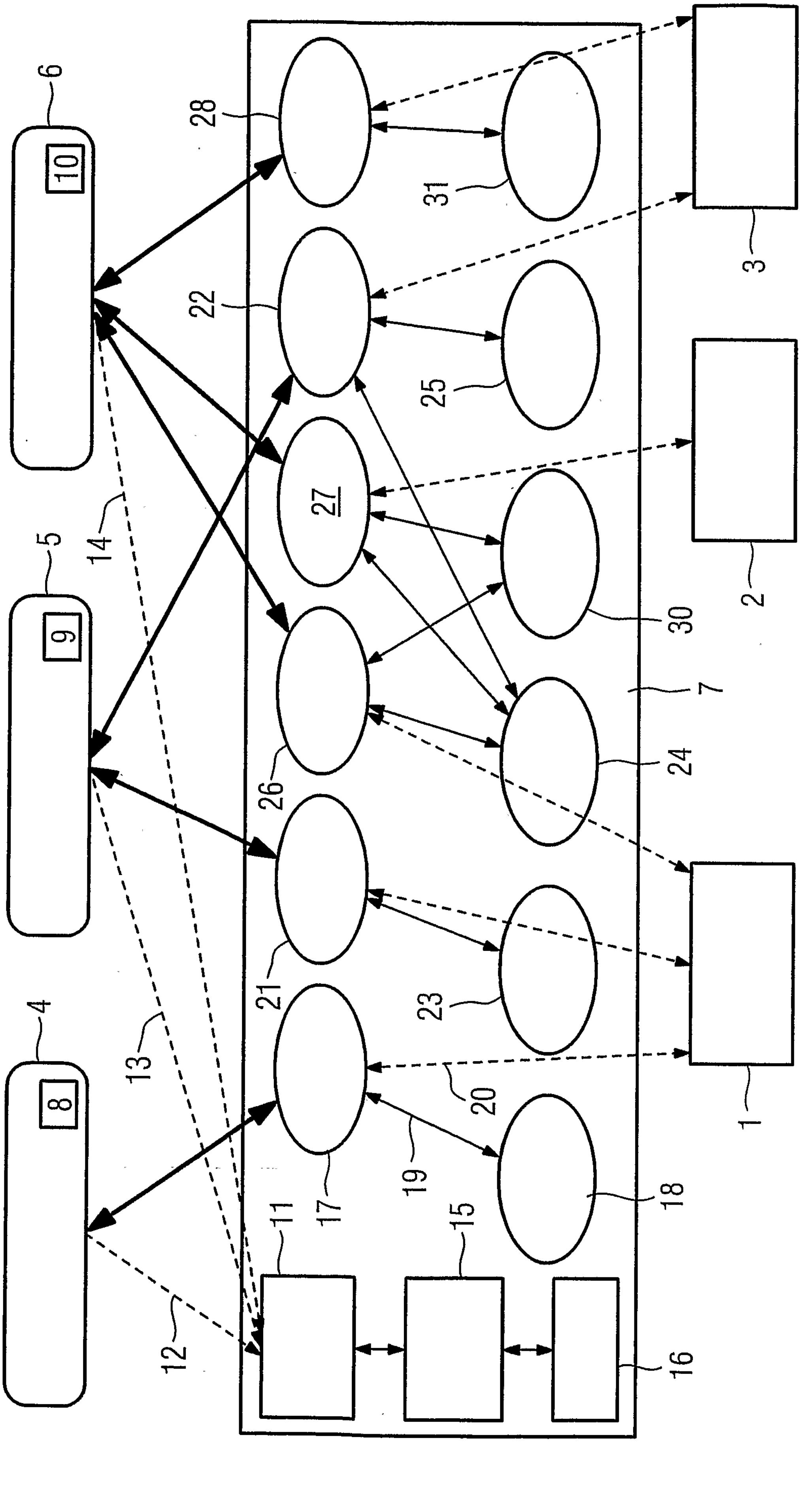
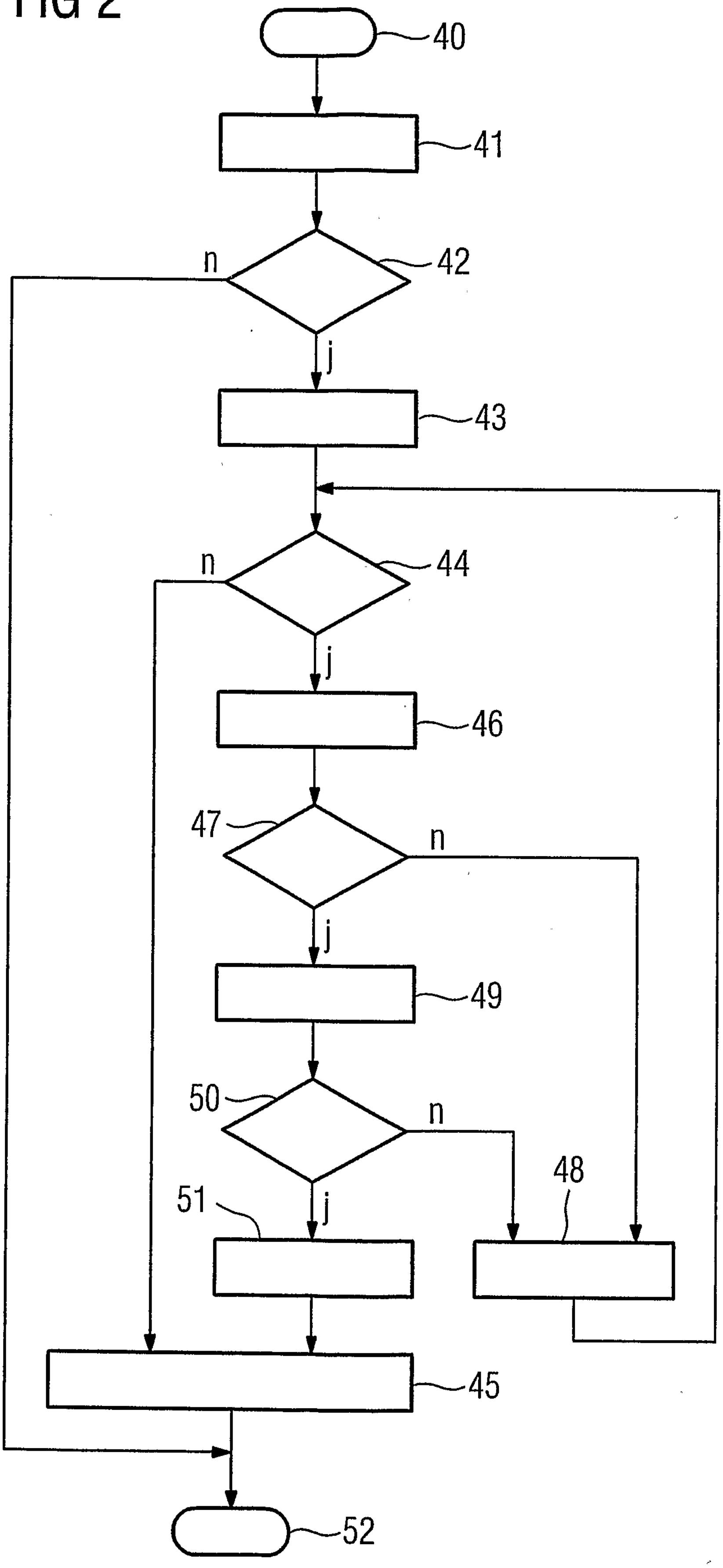

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
30
31

FIG 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/RU2006/000172

A. CLASSIFICATION OF SUBJECT MATTER
INV. G05B19/04 G05B19/05

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)
G05B

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 practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 102 45 176 A1 (ENDRESS & HAUSER PROCESS SOLUT [CH]) 1 April 2004 (2004-04-01) abstract the whole document -----	1-8
X	US 2004/193287 A1 (LEFEBVRE MARTINE [DE] ET AL LEFEBVRE MARTINE [FR] ET AL) 30 September 2004 (2004-09-30) the whole document -----	1-8

□ 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 document 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 12 January 2007	Date of mailing of the international search report 22/01/2007
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Goya, Jesus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/RU2006/000172

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 10245176 A1	01-04-2004	AU 2003273847 A1	23-04-2004
		WO 2004031874 A1	15-04-2004
		EP 1543391 A1	22-06-2005
US 2004193287 A1	30-09-2004	AU 2003301778 A1	07-06-2004
		CN 1711512 A	21-12-2005
		DE 10251503 A1	09-06-2004
		WO 2004042482 A1	21-05-2004
		EP 1558975 A1	03-08-2005