(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 284 816 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
16.02.2011 Bulletin 2011/07

(51) Int Cl.:
G08B 25/14 *(2006.01)* ***G06F 9/00*** *(2006.01)*

(21) Application number: **09305688.5**

(22) Date of filing: **20.07.2009**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Designated Extension States:
AL BA RS

(71) Applicant: **Afone**
49100 Angers (FR)

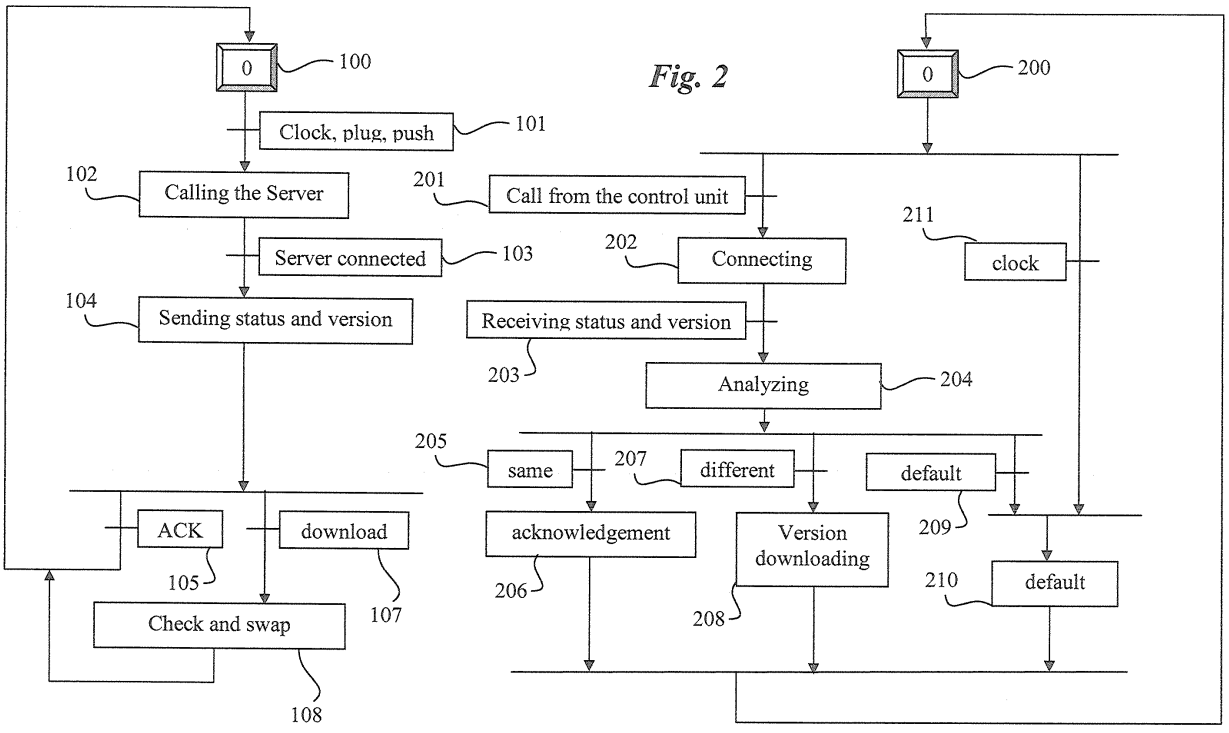
(72) Inventor: **Fournier, Philip**
49100 Angers (FR)

(74) Representative: **Thinat, Michel et al**
Cabinet Weinstein
56 A, rue du Faubourg Saint-Honoré
75008 Paris (FR)

(54) Alarm control method and system

(57) For handling alarms relating to premises, the method comprises a downloading step (208) wherein a distant server downloads into a local control unit, a configuration for handling the alarms locally to the premises. The system implementing the methods provides a ready to use alarm system innovative with respect to the complexity of the configuration process of classical systems.

Fig. 2



EP 2 284 816 A1

Description

[0001] The present invention relates generally to the field of alarm control methods and systems, and more particularly to a method and a system wherein a control unit handles alarms locally to premises.

[0002] The intervention of a professional technician is generally needed for installing a system wherein a control unit handles alarms locally to premises essentially because it is of huge complexity to configure a local control unit in view of the complex functionalities that can be assigned to sensors and devices, which are linked to the control unit and of the multiplicity of possible scenarios of alarm occurrences and of actions to be engaged.

[0003] A solution consisting of totally transferring the handling of alarms in a centralised equipment offers more resources in terms of adjustment and maintenance.

[0004] For example, US7,113,090 discloses a computer implemented method comprising the steps of compiling monitoring data, which are gathered from one or more remote sensor located at a location.

[0005] The known solutions for avoiding local installation of elaborate systems are not satisfying because they do not assure a sufficient autonomy of the system and a problem occurs in case of communication disruption or break for safeguarding a continuity of service.

[0006] The present invention provides a method for handling alarms relating to premises, comprising a downloading step wherein a server downloads into a local control unit, a configuration for handling the alarms locally to the premises.

[0007] The method of the present invention, preferably comprises a calling step wherein the local control unit calls the server before downloading.

[0008] Preferably also, the method of the present invention comprises a check step wherein the control unit proceeds to a verification of the downloaded configuration and enables the downloaded configuration if the verification is positive.

[0009] Advantageously in the method provided by the present invention, the local control unit works with a former configuration up to enabling the downloaded configuration, swaps on the downloaded configuration after enabling the downloaded configuration and keep a possibility of swapping back to the former configuration at least up to a following downloading of a further configuration.

[0010] Particularly, the server downloads the configuration from a profile, which is associated with the local control unit.

[0011] More particularly, the method of the present invention comprises a configuration updating step wherein the server updates the profile with a new configuration for the control unit and with a new reference attached to the new configuration.

[0012] According to an embodiment of the present invention, the method comprises a version sending step wherein the control unit transmits to the server a former version reference pertaining to the configuration, which is enabled in the control unit.

[0013] More precisely, the method comprises an analyzing step wherein the server compares the former version reference with the new version reference so as to trigger the downloading step when the two versions are different.

[0014] In the same or another embodiment, the server retrieves the profile from a database wherein the profile is indexed in association with the local control unit.

[0015] The invention further provides the method with a dialog step for a user to transmit by a terminal to the server dialog data relating to the configuration, which is to be downloaded.

[0016] In particular, the updating step is triggered by a transition, which is validated by dialog data received by the server.

[0017] Advantageously, the configuration comprises a program to be executed by the local control unit and/or the updating step is triggered by a transition, which is validated by the detection of a new program to be executed by the local control unit.

[0018] The present invention provides also a system for handling alarms relating to premises, comprising a local control unit arranged for downloading from a distant server, a configuration for handling the alarms locally to the premises.

[0019] Preferably, the local control unit of the system is arranged for calling the server and for accepting downloading only after having called the server.

[0020] Advantageously, the control unit comprises:

- a read only memory including a backup program; and
- two non-volatile memory zones, a first one for storing a program, which is enabled to run and a second one which is ready for downloading a new program.

[0021] Non-volatile memory zones are also supposed to handle configuration data. The same or another couple of memory zones can be dedicated to configuration data, working the same way as that for program downloading and swapping.

[0022] The present invention provides also a control unit for handling alarms comprising:

- a read only memory including a program able to run by first plug of the control unit; and
- two non-volatile memory zones, a first one for storing a configuration, which is usable and a second one which is ready for downloading a new configuration.

[0023] The system implementing the methods provides a ready to use alarm system innovative with respect to the complexity of the configuration process of classical systems.

[0024] These and other objects and advantages of the present invention will become apparent after considering the following detailed specification of preferred embodi-

ments in conjunction with the accompanying drawings wherein:

- Figure 1 is a schematic view of a security system implementing the invention;
- Figure 2 is a flowchart of a communication process between a control unit and a server according to the invention;
- Figure 3 is a flowchart of a communication process between a remote terminal and the server according to the invention.

[0025] The security system illustrated in Figure 1 comprises locally to a protected scene one or more hard-wired sensors 14 and/or wireless sensors 18 like for example door or window open/close detectors, universal perimeter protection detectors, smoke detectors, motion detectors, microphones, emergency pendant transmitters, user keys, one or more hard-wired half duplex devices 12 and/or wireless half duplex devices 16 like for example internal siren, external siren, chime, programmable (PGM) relays for remote control of appliances, one or more hard-wired full duplex devices 13 and/or wireless full duplex devices 17 like for example camera, keypads and a control unit 10 connected to a cabled local area network 11 for handling hard-wired sensors and devices 12-14 and/or to a radio local area network 15 for handling wireless sensors and devices 16-18. We note that many originally half duplex devices, are becoming full duplex in order to be "manageable". For example, a full duplex siren could be tested. The security system can be used in a mass-market context as in a professional field for protected scenes relating to an apartment, a house, a factory, a shop or any public building. The communication protocols between the control unit and the sensors and devices are preferably standardized protocols.

[0026] The control unit 10 is arranged to communicate with a remote server 20 by one or more digital communication channels. The control unit 10 is for example connected to a large area network 22 like the Internet and using IP protocol on a DSL (Digital Subscriber Loop) link, on an Ethernet type local area network, on a WIFI (802.11 or higher standard) link. An advantage of the Internet is to allow accessibility to the server 20 from anywhere in the world by using any computer 30. Preferably, the control unit 10 comprises an activated SIM (Subscriber Identity Module) card for connecting to the server 20 through a cellular telephony network 21 allowing packet oriented mobile data service like GPRS system based on FDD and TDMA technology or UMTS based on CDMA technologies. The SIM card ensures the security in identifying the device, in particular the control unit to which it is associated in a radio network which can be compared to the security of identification provided by an address MAC (Media Access Control) in a hardwired network. The cellular telephony network ensures a permanent access from the control unit 10 to the server 20 with an automatic configuration capacity of the control unit as it will be further explained later in the description. The cellular telephony network presents an additional advantage with a possibility of directly calling a mobile phone of the user when an alarm occurs, directly from the control unit and not necessarily from the server. Other radio networks can be used with the same advantages like e.g. any WIMAX (acronym for *Worldwide Interoperability for Microwave Access*) network.

[0027] The control unit 10 is arranged to allow only communications, which are initiated by the control unit. In this manner, the control unit 10 can be implemented in any kind of network without need of a firewall to block unauthorized access. The server does not need any ability for reaching the control unit because every communication of the server with the control unit is realized only after a call from the control unit to the server. Every communication implying the control unit is ciphered in a way that ensures the security of any transaction for all communication channels potentially to be used. At the beginning of any transaction, an identity check of the control unit is carried out. The checking process is based on the unique identifier of any control unit used by the system. The identifier may be, for illustrative purpose only, the ICCID (Integrated Circuit Card Identifier Digits) number of the SIM card for example.

[0028] The server 20 is linked up with a database 23 which indexes each control unit that is or can potentially be connected to the server. A profile is attached in the database to each control unit comprising a unique identifier of the control unit, a version of the software or programs implemented in the control unit and of the configuration of the control unit.

[0029] The control unit 10 and the server 20 comprise each a processor and a memory containing one or more computer programs comprising program code means for performing steps of a method according to the invention when a first part of the program is run on the control unit 10 and a second part of the program is run on the server 20.

[0030] More precisely, the memory of the control unit 10 comprises a ROM (read only memory) zone 7 wherein a backup program is engraved during the manufacture process in a factory producing the control unit 10. The memory of the control unit 10 comprises also two non volatile zones 8 and 9 wherein a first non volatile zone is ready for downloading a release program from the server 20 and a second non volatile zone for hosting an enabled program. The same process may apply for configuration data.

[0031] The backup program is a basic program which affords access to the server 20 for establishing a dialog comprising the transmission of a status from the control unit to the server and the download of the release program from the server 20 to the ready non volatile zone 8 or 9. The memory zone 7 contains also an address of a rescue server 24 able to provide the control unit with a release program and with one or more addresses of configuration servers. On initial start, that is to say on the

first start when plugging the control unit coming from the factory, the control unit boots on the backup program. In case of power failure, the control unit reboots with the last program, which has been enabled.

[0032] Dialog steps between the control unit 10 and the server 20 may be illustrated in Figure 2.

[0033] The control unit 10 is generally in an idle step 100 waiting for an event.

[0034] A transition 101 is periodically validated by a clock signal for periodically checking the good working of the control unit. The transition 101 may also be validated by a plug signal when it is started for a first time, by a push signal when the user press a dedicated button on the front panel of the control unit or by any default of the control unit 10 or any signal received from a sensor 14, 18 or a device 13, 17 which is connected to the control unit.

[0035] The transition 101 triggers a calling step 102 wherein the control unit 10 calls the server 20 through the IP network 22 or through the cellular network 21, which is steadily available if the IP network 22 is not available. The control unit 10 can call automatically the server through the Internet using an URL (Uniform Resource Locator) or through the cellular network using a telephone number stored at least in the ROM memory 7. Data enabled cellular networks like GPRS or UMTS allow communications in IP mode. The use of a POTN (plain old telephone number) is a good means of alarm transmission as a final backup of sending an alarm if wired or wireless data networks are not available. The server 20 is generally in a monitoring step 200 waiting for a request or a call.

[0036] A transition 201 is validated when the server receives a call from the control unit.

[0037] The transition 201 triggers a connecting step 202 wherein the server establishes a communication with the control unit.

[0038] A transition 103 is validated when the control unit detects that the server is connected.

[0039] The transition 103 triggers a transmission step 104 wherein the control unit sends its version and the status of the alarm control system to the server. The version of the control unit comprises the unique identifying number of the control unit, a version identifier of the enabled program, which is recorded in the non-volatile zone of the memory, and a version identifier of the configuration of the security system. The configuration of the security system comprises for example a list of sensors and devices which are connected to the control unit, how to proceed with each of the sensor or device according to the circumstances, the telephone number to be called in case of an alarm and so on. The status of the alarm control system comprises the status of the control unit and of each sensor and device, which is connected to the control unit for notifying if a default, detection or activation occurs and which event occurs or if nothing is to declare.

[0040] A transition 203 is validated when the server receives the status and version from the control unit.

[0041] The transition 203 triggers an analysing step 204 wherein the server 20 uses the unique identifying number of the control unit for retrieving its profile out of the database 23 and verifies the received status. A transition 209 is validated when a default, detection, activation or the connection of a new sensor or a new device to the control unit is notified. When the transition 209 is not validated, the server 20 compares the received version with the version, which is registered in the database 23. A transition 205 is validated when the received version is the same as the registered version. A transition 207 is validated when the received version is different from the registered version.

[0042] The transition 209 triggers a default step 210 wherein the server 20 records the status and launches the actions, which are ordered by registered rules associated with the profile of the control unit in the database 23. Step 210 is also triggered by a transition 211. The transition 211 is validated by a clock pulse signal for the case where transition 201 is not validated because of no call received from the control unit in a predetermined period after last validation of transition 201. Validation of transition 211 is indeed an alarm condition for launching actions according to the registered rules associated with the profile of the control unit in the database 23.

[0043] The transition 205 triggers an acknowledgement (ACK) step 206 wherein the server 20 sends an ACK message to the control unit 10.

[0044] A transition 105 is validated when the control unit 10 receives the ACK message and returns to step 100.

[0045] The transition 207 triggers a download step 208 wherein the server 20 sends a release program having the version, which is indicated by the database and/or an updated configuration having the version, which is indicated by the database when the versions of the program are different, and/or respectively when the versions of the configuration are different. A standard protocol like the XML (extensible Markup Language) is used for communicating the configuration features and content between the server and the control unit.

[0046] Reception of the release program or of the updated configuration by the control unit validates a transition 107, which triggers a step 108.

[0047] In step 108, the running program on the control unit 10 indicates the memory zone wherein it is recorded and the memory zone, which is free for recording the received release program. When the running program is the enabled program, which is recorded in the non volatile zone 8, it indicates that the non volatile zone 9 is ready for downloading the release program from the server 20. When the running program is recorded in the non volatile zone 9, it indicates that the non volatile zone 8 is ready for downloading the release program from the server 20. When the running program is the backup program which is recorded in the ROM 7, it indicates one or the other of the zones 8, 9 as a ready zone for recording the downloaded program.

[0048] When transition 107 is validated by the reception of the release program, the running program records the release program in the indicated ready zone 8 or 9. The running program checks the coherence of the release program by using a key which is provided by the central server 20. If the downloaded release program is correct, the running program enables the downloaded release program, indicates that the memory zone wherein the current running program is recorded becomes the memory zone ready for downloading a new release program and that the memory zone containing the just downloaded release program becomes the memory zone of the enabled program. The up to now running program swaps to the new enabled program by branching itself to the enabled program in such a way that the enabled program becomes the running program. After swapping of the running programs, the former running program is an enabled non running program, which constitutes a rescue program in case of execution failure of the more recently activated program. A back swapping is executed as if the former running program would be a release program in the ready non-volatile zone 8, 9 which is otherwise ready for downloading.

[0049] When transition 107 is validated by the reception of the updated configuration, the running program locally updates the configuration of the control unit.

[0050] After execution of one of the steps 206, 208, 210, the server 20 goes back to step 200.

[0051] The terminal 30, for instance a computer, which is connected on the Internet network 22, executes the steps now described with reference to Figure 3. It is not necessary for the control unit 10 to be connected to the network 22 because for sake of security, no appliance can access directly to the control unit 10 but via the server 20 during a connection initiated by the control unit itself. Of course, when a user modifies the configuration of his/her control unit, he/she can force a connection of the control unit by pressing a key on the control unit. He/She can also wait for the next recurrent check process, for example, when he/she is not "at home".

[0052] The terminal 30 is considered here in an initial step 300 when a browser is in an idle state. A transition 301 is validated when the terminal 30 is connected to the Internet. Computer resources for the terminal 30 provide a convivial environment for configuring and monitoring the alarm system. Any 3G or higher mobile phone 31 on UMTS, HSDPA (High Speed Downlink Packet Access) or any other data radio network can also be used on the network 22.

[0053] The transition 301 triggers a step 302 wherein a request to the service of the server 20 is initiated for example by the user of the alarm system. On the side of the Internet, the server 20 is considered to be in a waiting step 250. A transition 251 is validated when a request is received from the Internet, precisely here from the terminal 30.

[0054] The transition 301 triggers a step 252 wherein the server connecting the terminal 30, displays pages with scroll menus and/or hyperlinks to sub pages relating to the control unit 10. More particularly, the pages gives access to the profile associated with the control unit 10 after having entered a password. A transition 303, which is validated when the service is opened, triggers a dialog step 304 for configuring, monitoring and driving the profile of the control unit in the database 23.

[0055] A transition 253, which is validated by reception of dialog data in the server, triggers a configuration updating step 254 wherein the server updates a new configuration version of the profile, which is stored in the database 23.

[0056] The terminal 30 and the server 20 return respectively is initial step 300 and in initial step 250 after validation of respectively transition 305 and 255 by a disconnection.

[0057] Independently of the terminal 30, step 254 can be triggered also by a transition 257, which is validated when a new program is detected for implementation in the local control unit.

[0058] The above described method and system can be used in the following way.

[0059] The alarm system is purchased by the user in a shop or via Internet sites. The purchased alarm system comprises the control unit 10 and some sensors and devices.

[0060] It will be apparent here that the commissioning of the alarm system is very easy without the need of a professional installer.

[0061] The user hangs up himself the control unit 10 where he wants in home or business premises to be protected. When the user supplies the control unit 10 with electricity using the sector or battery cells, the automatic validation of transition 101 triggers step 102. In step 102, the backup program, which is stored in ROM 7, calls the server 20, redirected if necessary from the server 24 by using a permanent address, which is stored in ROM 7. By activation of steps 202 to 210, the server 20 automatically associates a profile with the control unit in the database 23 by using the unique identifying number, which is communicated by the control unit from the ROM 7. The server 20 verifies if the control unit 10 is OK and automatically assures that the control unit 10 is provided with the more recent version of programs.

[0062] The user connects his terminal 30 to a web portal associated with the server 20 by using an URL indicated in a light user guide, which is provided with the control unit or simply on the packing box of the control unit. By activation of dialog step 254, the server 20 displays automatically a window requiring the user to identify or to register him or her. A displayed register form comprises a window to be completed with the unique identifying number, which is printed on the control unit and a window for specifying a password, which will be used for later identification of the user. Any kind of more robust identification method can also be used. The password is memorized in the profile of the control unit. The server 20 accesses automatically to the profile of the control

unit 10 in the database 23 and displays relevant elements of the profile in the web page, which is opened on the portal for the user.

[0063] The user can immediately or later complete the installation of his or her alarm control system. The user is not stressed by a necessary immediate complete installation of the alarm control system. If the user whishes to delay the complete installation, he or she simply disconnect from the web portal. He or she will connect later by using the password, which is memorized in the profile of the control unit 10.

[0064] When the user decides to link a sensor 14, 18 or a device 12, 13, 16, 17 to the control unit, he or she presses a dedicated button on the sensor or device and the dedicated button on the control unit 10. The transition 101 validated by the push button of the control unit triggers steps 102-108 in such a way that the sensor or device is registered in the profile associated with the control unit 10 in the database 23. Here again the user can immediately or later specify the function of the linked sensor or device.

[0065] When the user decides to specify the function of the linked sensor or device, for instance because no kid is using the terminal 30 or is to be accompanied to school, the user leisurely connects to the web portal of the server 20 and identifies him or herself by using the password. The web portal displays the relevant elements of the profile comprising sensors and devices not already specified. The user can set a name to each unspecified sensor or device, for example "motion detector in sleeping room of Harry". The user can set one or more scenarios associated with the sensor or device, date and time of activation, delay for launching an alarm and so on.

[0066] The system can be droved progressively operational. Of course the system can also be droved rapidly operational in case of urgency.

[0067] Other embodiments, uses and advantages of the present invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. The specification and examples should be considered exemplary only. The intended scope of the invention is only limited by the claims appended hereto.

Claims

1. A method for handling alarms relating to premises, comprising a downloading step (208) wherein a server downloads into a local control unit, a configuration for handling the alarms locally to the premises.

2. The method according to Claim 1, comprising a calling step (102) wherein the local control unit calls the server before downloading.

3. The method according to Claim 1 or 2, comprising a check step (108) wherein the control unit proceeds to a verification of the downloaded configuration and enables the downloaded configuration if the verification is positive.

4. The method according to Claim 3, wherein the local control unit works with a former configuration up to enabling the downloaded configuration, swaps on the downloaded configuration after enabling the downloaded configuration and keep a possibility of swapping back to the former configuration at least up to a following downloading of a further configuration.

5. The method according to anyone of Claims 1 to 4, wherein the server downloads the configuration from a profile, which is associated with the local control unit.

6. The method according to Claim 5, comprising a configuration updating step (254) wherein the server updates the profile with a new configuration for the control unit and with a new reference attached to the new configuration.

7. The method according to anyone of Claims 5 or 6, comprising a version sending step (104) wherein the control unit transmits to the server a former version reference pertaining to the configuration, which is enabled in the control unit.

8. The method according to Claim 7, comprising an analyzing step (204) wherein the server compares the former version reference with the new version reference so as to trigger the downloading step (208) when the two versions are different.

9. The method according to anyone of Claims 5 to 8, wherein the server retrieves the profile from a database wherein the profile is indexed in association with the local control unit.

10. The method according to anyone of preceding Claims, comprising a dialog step (304) for a user to transmit by a terminal (30, 31) to the server dialog data relating to the configuration, which is to be downloaded.

11. The method according to Claim 6, wherein the updating step (254) is triggered by a transition (253), which is validated by dialog data received by the server.

12. The method according to anyone of preceding Claims, wherein the configuration comprises a program to be executed by the local control unit.

13. The method according to Claim 6, wherein the updating step (254) is triggered by a transition (257),

which is validated by the detection of a new program to be executed by the local control unit.

14. A system for handling alarms relating to premises, comprising a local control unit (10) arranged for downloading from a distant server (20), a configuration for handling the alarms locally to the premises.

15. The system according to Claim 13, wherein the local control unit (10) is arranged for calling the server (20) and for accepting downloading only after having called the server.

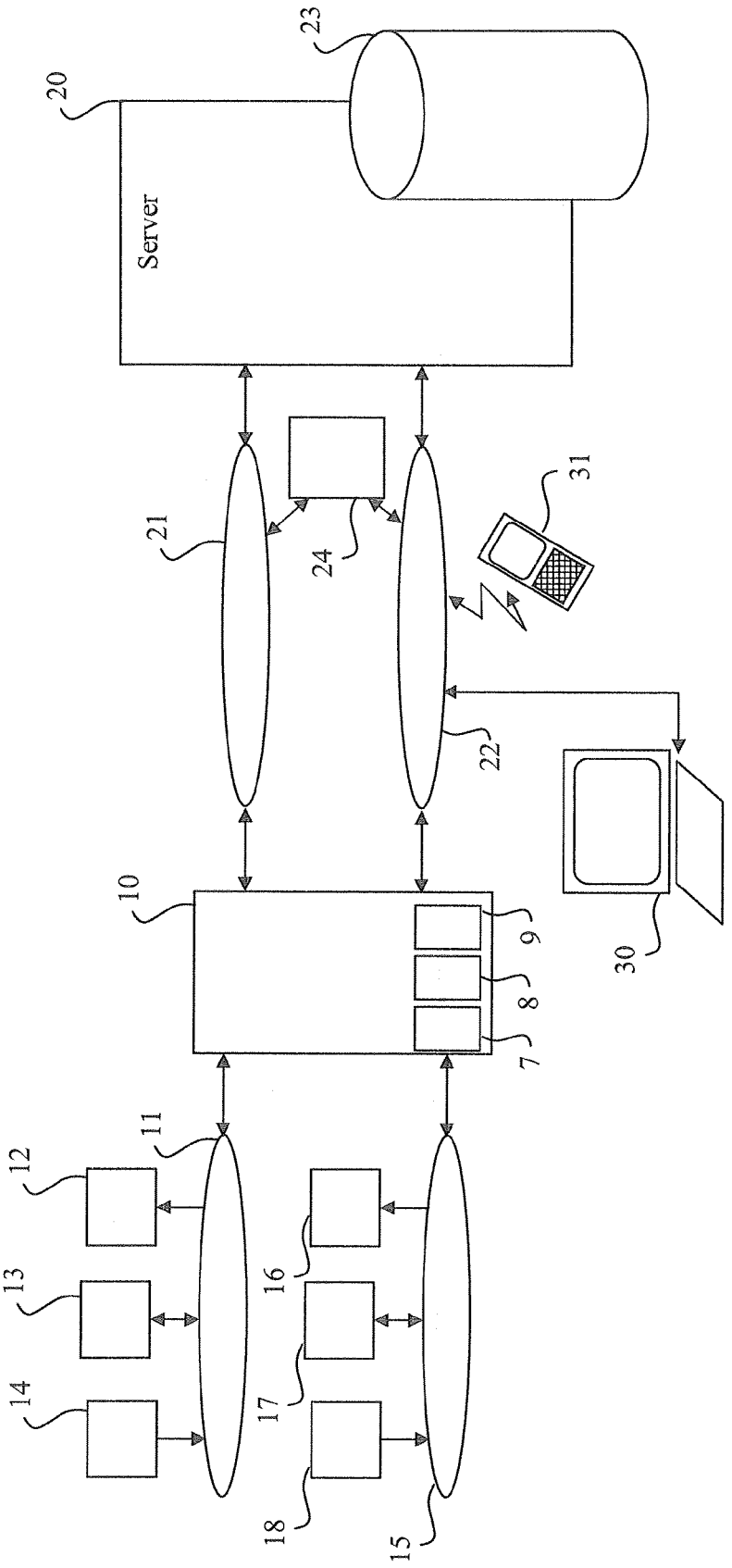
16. The system according to Claim 14 or 15, wherein the control unit (10) comprises:

- a read only memory (7) including a backup program; and
- two non-volatile memory zones (8, 9), a first one for storing a program, which is enabled to run and a second one which is ready for downloading a new program.

17. A control unit (10) for handling alarms comprising:

- a read only memory (7) including a program able to run by first plug of the control unit; and
- two non-volatile memory zones, a first one for storing a configuration, which is usable and a second one which is ready for downloading a new configuration.

Fig. 1



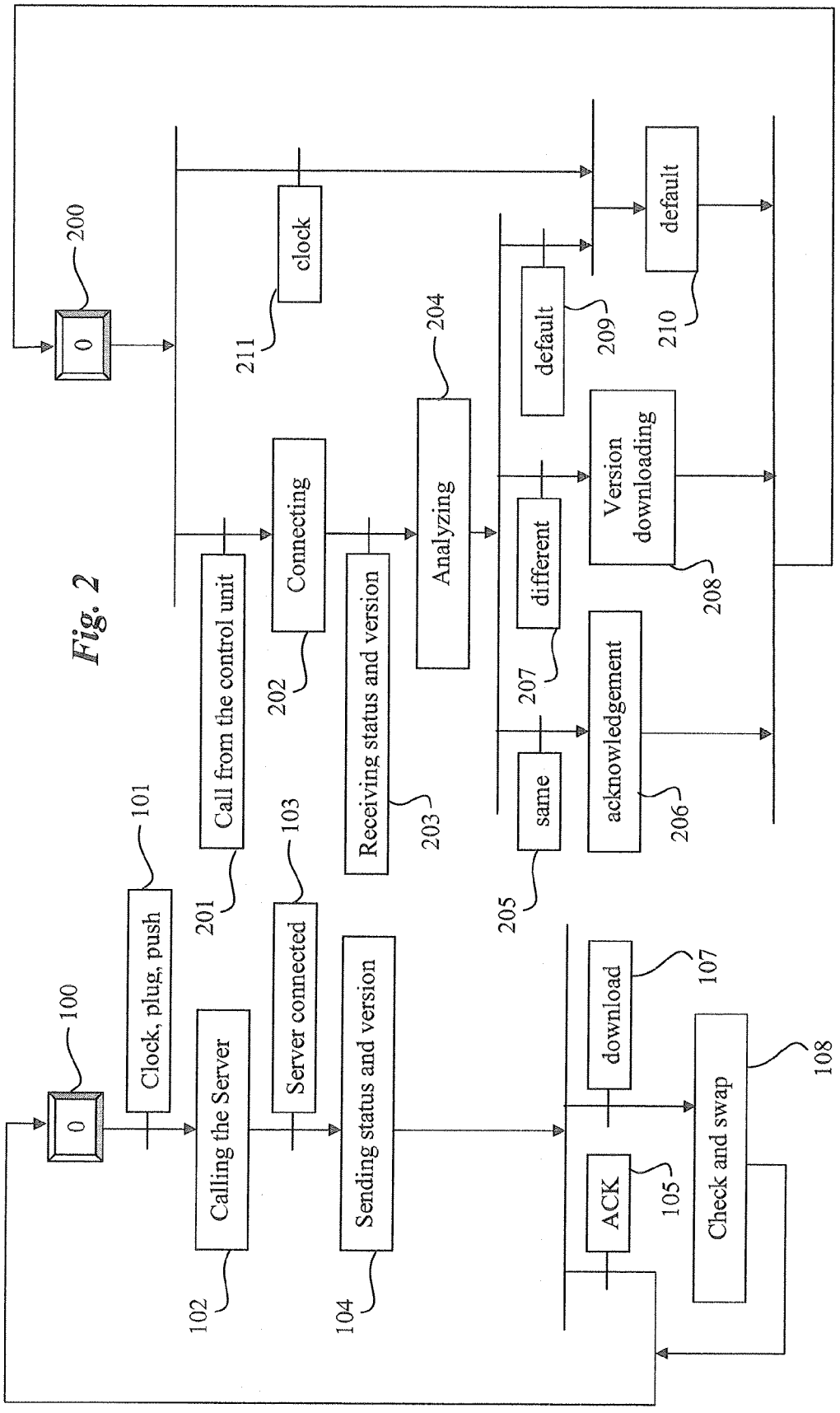

0
100
Clock, plug, push
101
Calling the Server
102
Call from the control unit
201
Connecting
202
Server connected
103
Receiving status and version
203
Sending status and version
104
Analyzing
204
same
205
different
207
default
209
clock
211
default
210
Version downloading
208
acknowledgement
206
download
107
ACK
105
Check and swap
108
0
200

Fig. 2

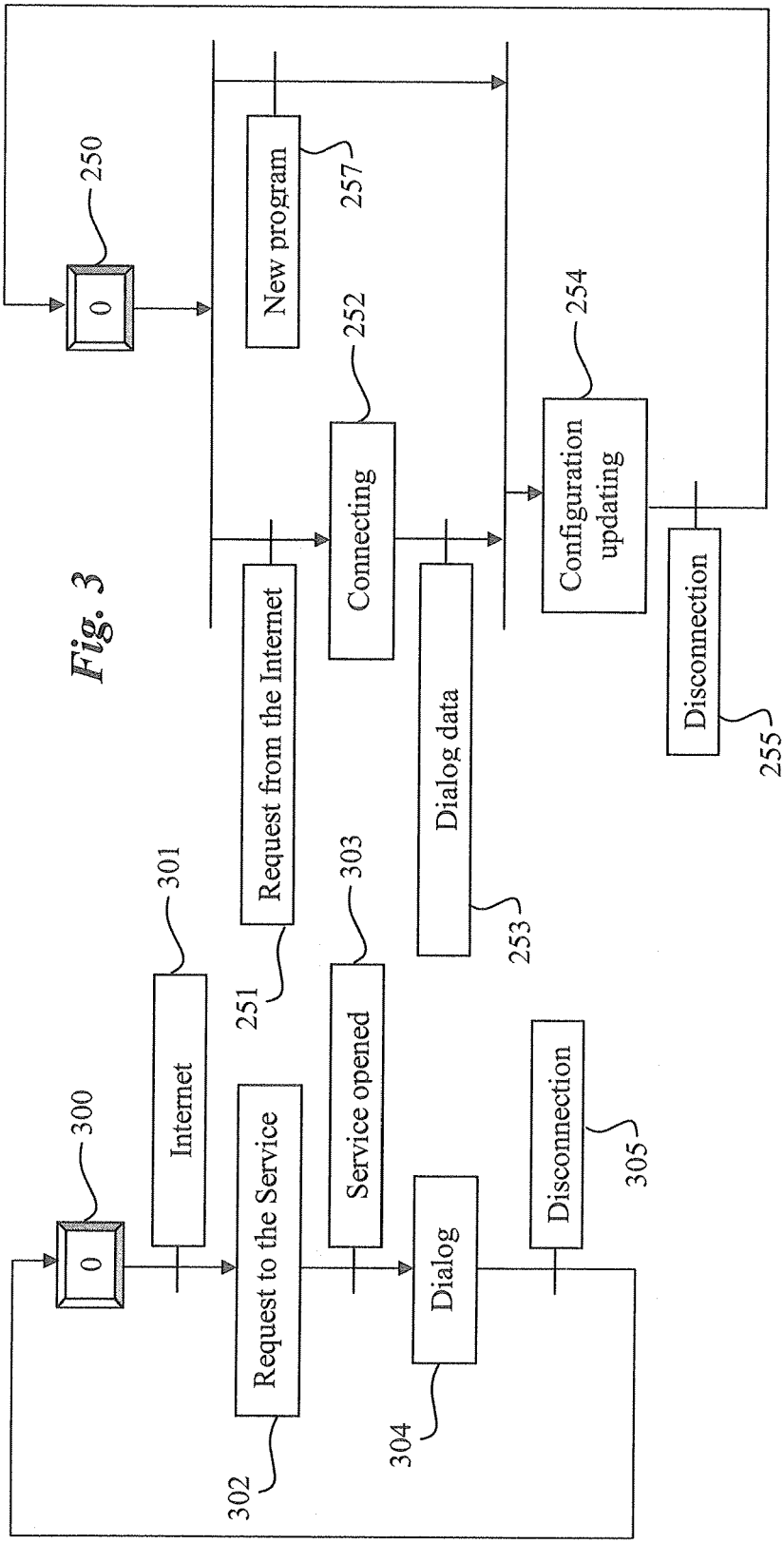

0
300
Internet
301
Request to the Service
302
Request from the Internet
251
Service opened
303
Dialog
304
Disconnection
305
Connecting
252
Dialog data
253
New program
257
0
250
Configuration updating
254
Disconnection
255

Fig. 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 09 30 5688

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y	US 2004/215750 A1 (STILP LOUIS A [US]) 28 October 2004 (2004-10-28) * abstract * * paragraphs [0015] - [0023], [0127], [0133], [0137], [0166], [0173], [0248] - [0260]; figures 1-23 * * paragraphs [0002], [00 7] - [0023]; figures 1-3 * -----	1-6, 9-15,17 7-8, 16-17	INV. G08B25/14 G06F9/00
Y	US 2009/144718 A1 (BOGGS JOSEPH [US] ET AL) 4 June 2009 (2009-06-04) * abstract * * paragraphs [0009] - [0019]; figures 1-4 * -----	7-8	
Y	JP 2001 273143 A (RICOH KK) 5 October 2001 (2001-10-05) * abstract * -----	16-17	
			TECHNICAL FIELDS SEARCHED (IPC) G08B G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	15 December 2009	Wright, Jonathan

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 09 30 5688

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

15-12-2009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004215750 A1	28-10-2004	NONE	
US 2009144718 A1	04-06-2009	NONE	
JP 2001273143 A	05-10-2001	JP 4076113 B2	16-04-2008

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 7113090 B **[0004]**