(19) DANMARK

(10) DK/EP 3454246 T3

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: *G 06 F 21/57 (2013.01)* *G 06 F 9/445 (2018.01)* *G 06 F 21/64 (2013.01)*

(45) Oversættelsen bekendtgjort den: **2020-04-27**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2020-01-29**

(86) Europæisk ansøgning nr.: **18193027.2**

(86) Europæisk indleveringsdag: **2018-09-06**

(87) Den europæiske ansøgnings publiceringsdag: **2019-03-13**

(30) Prioritet: **2017-09-08 FR 1758290**

(84) Designerede stater: **AL 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 RS SE SI SK SM TR**

(73) Patenthaver: **ALSTOM Transport Technologies, 48 rue Albert Dhalenne, 93400 Saint-Ouen, Frankrig**

(72) Opfinder: **BREGARDIS, Cedric, 19, rue professeur Paul Sisley, 69003 Lyon, Frankrig**
QUADRINI, Matthieu, Lieu-dit le Poux, 63120 Sauviat, Frankrig
FERNANDEZ-VALBON, Rafael, 2, Place Jules Ferry, 69003 Lyon, Frankrig
DEGENEVE, Xavier, 27 Rue Charles Richard, 69003 Lyon, Frankrig

(74) Fuldmægtig i Danmark: **NORDIC PATENT SERVICE A/S, Bredgade 30, 1260 København K, Danmark**

(54) Benævnelse: **FREMGANGSMÅDE TIL TRANSMISSION OG KONTROL AF GYLDIGHEDEN AF KONFIGURATIONSDATA I ET ELEKTRONISK SYSTEM, TILHØRENDE ELEKTRONISK SYSTEM OG COMPUTERPROGRAMPRODUKT**

(56) Fremdragne publikationer:
DE-A1-102009 058 754
US-A1- 2008 216 067
US-A1- 2014 032 916

DESCRIPTION

[0001] The present invention relates to a method for transmitting and checking the validity of configuration data in an electronic system, an electronic system and a computer program product associated therewith.

[0002] Methods for reconfiguring a plurality of electronic boards in a vehicle are known from US 2008/216067, US 2014/032916 and DE 10 2009 058754.

[0003] In the prior art, it is likewise known to use electronic systems for centralized storage of configuration data. The configuration data are intended for different modules or also electronic boards constituting these systems.

[0004] Among these systems, mention may be made in particular of certain items of equipment accommodated on board a railway vehicle, such as, for example, a console for communication with the driver of the railway vehicle, traction equipment, network equipment, equipment which actuates outputs or reads inputs. Mention may also be made, in particular, of certain items of equipment on the ground along tracks of a railway system, in particular for signaling, such as, for example, equipment which interfaces with objects on the track (signal lights, switches, level crossings, track circuits, beacons).

[0005] The configuration data are necessary for the operation of the corresponding electronic modules or boards, and are stored in a centralized storage module provided for this purpose.

[0006] When an electronic system with centralized storage of configuration data exhibits a high level of criticality, the configuration data are stored in the form of a secure data structure.

[0007] This structure is associated with a signature which makes it possible to check the validity of the corresponding configuration data. The checking of the validity of data comprises in particular the checking of the authenticity, the integrity and the coherence of these data.

[0008] In general, the validity of the configuration data is checked each time the corresponding electronic system boots up.

[0009] In particular, at the time of such a bootup, one of the electronic boards of the electronic system extracts all of the configuration data from the storage module and checks the validity of these data.

[0010] When the validity is checked, said electronic board transmits the configuration data corresponding to these boards to the other electronic boards.

[0011] Upon reception of the corresponding configuration data, each electronic board stores these data in its internal memory and checks their integrity as well as their coherence.

[0012] The electronic system is operational when each board has received, has checked and has

stored the corresponding configuration data.

[0013] It will then be understood that such a method of booting up an electronic system with centralized storage of configuration data is particularly slow and is unsuitable when it is necessary to perform frequent reboots of the system and/or when the system includes a large number of electronic modules or boards. Thus, for example, the duration of a bootup of an electronic system according to this method can take up to 30 minutes when the system is composed, for example, of 50 electronic boards.

[0014] The present invention relates to a method for remedying this drawback of the prior art by proposing an electronic system and a method for transmitting and checking the validity of configuration data implemented by this system, making it possible to considerably reduce the reboot time of such a system.

[0015] For this purpose the invention relates to a method for transmitting and checking the validity of configuration data according to claim 1.

[0016] According to other advantageous aspects of the invention, the method comprises one or more of the characteristics of claims 2 to 10.

[0017] The invention also relates to a computer program product comprising software instructions which, when implemented by computer equipment, implement the method as defined above.

[0018] The invention also relates to an electronic system with centralized storage of configuration data according to claim 12.

[0019] These characteristics and advantages of the invention will be apparent from a reading of the following description, given solely by way of non-limiting example and with reference to the appended drawings, in which:

- Fig. 1 shows a schematic view of an electronic system according to the invention, the system comprising, in particular, a centralized storage module;
- Fig. 2 shows a schematic view of a data structure stored in the storage module of Fig. 1; and
- Fig. 3 shows a flow diagram of a method for transmitting and checking the validity of configuration data in the electronic system of Fig. 1.

[0020] The electronic system 10 of Fig. 1 includes a plurality of electronic boards 12A to 12N implementing the operation of the system 10, and a centralized storage module 14.

[0021] The electronic system 10 can be used in particular in the railway sector and has, for example, an item of equipment fitted onboard a railway vehicle, such as a console for communication with the driver of the vehicle.

[0022] Each electronic board 12A to 12N provides a service to the electronic system 10 using

configuration data specific to this board. In other words, the configuration data define the department provided by the corresponding electronic board 12A to 12N in response to different events occurring in the system 10.

[0023] Each electronic board 12A to 12N is, for example, in the form of a programmable logic device comprising in particular an internal memory M. Such a programmable logic device is, for example, of the FPGA (field-programmable gate array) type.

[0024] The internal memory M may have the property of keeping the information stored, even when it is not supplied with electrical power.

[0025] The internal memory is designed to store a signature variable and configuration variables.

[0026] The signature variable corresponds to an elementary signature of the configuration variables.

[0027] The configuration variables correspond to data configurations retrieved by the electronic board 12A to 12N, as will be explained below.

[0028] According to one variant, at least some of the electronic boards have a more complex form, for example the form of a miniature computer comprising in particular a processor and an internal memory.

[0029] According to one variant, at least some of the electronic boards are replaceable. In this case, the electronic system 10 is said to be adaptable.

[0030] According to one variant, at least some of the electronic boards are replaceable when hot without disrupting the operation of the other boards of the system (except for the communications/service using the card being replaced. In this case, the electronic system 10 is said to be adaptable when hot or in operation.

[0031] The configuration data of all of the boards 12A to 12N are stored at least initially in the centralized storage module 14 in the form of a secure data structure 20 which is illustrated in greater detail in Fig. 2.

[0032] Thus, with reference to this Fig. 2, the data structure 20 comprises a plurality of blocks of configuration data 22A to 22N associated respectively with the electronic boards 12A to 12N.

[0033] Each of these blocks of data 22A to 22N includes configuration data specific to the electronic board 12A to 12N associated with this block.

[0034] This data structure 20 is associated with a global signature 24 which makes it possible to check the validity of the data contained in this structure.

[0035] The global signature 24 is, for example, stored in the centralized storage module 14 with the data structure 20.

[0036] The global signature 24 is, for example, determined from the data contained in the structure 20 according to methods known per se.

[0037] The configuration data are modifiable, for example, by a user in order to modify the operation of the onboard system 10. Thus, in the preceding example of the console for communication with the driver, the modification of the configuration data makes it possible, for example, to trigger new messages for the driver.

[0038] When the configuration data are modified, the global signature 24 is likewise modified.

[0039] The centralized storage module 14 is connected to one of the electronic boards 12A to 12N, for example the electronic board 12A, referred to below as the main board.

[0040] The main board 12A makes it possible to implement a method of transmitting and checking the validity of configuration data obtained from the centralized storage module 14 which will be explained below with reference to Fig. 3, which shows a flow diagram of the method steps.

[0041] In particular, the method of transmitting and checking the validity of configuration data corresponds to a bootup phase PR of the electronic system 10.

[0042] This bootup phase PR is then implemented on initial bootup of the electronic system 10 and at subsequent reboot.

[0043] During the initial step 110 of the bootup phase PR, the electronic system 10 receives an initial bootup or reboot command. It should be noted that the command received does not indicate whether or not the bootup is initial or modified by configuration data.

[0044] The electronic system 10 then activates the operation of all of the electronic boards 12A to 12N and, in particular, the operation of the main board 12A.

[0045] During the following step 120, the main board 12A extracts the data structure 20 from the storage module 14.

[0046] Then the main board 12A checks the validity of the configuration data from the data structure 20.

[0047] The checking of the validity of the data comprises in particular the checking of the authenticity, the integrity and the coherence of these data.

[0048] In order to check the validity, the main board 12A generates a global signature SG, for example, from the configuration data received, using the same methods as those used in order to determine the global signature 24 associated with the data structure 20.

[0049] Then the main board 12A compares the generated global signature SG with the signature 24 associated with the data structure 20.

[0050] When the two signatures coincide, the main board 12A moves on to the step 130. In the

opposite case, the main board 12A moves on to the step 135 during which it generates an error message intended, for example, for the user and interrupts the execution of the bootup phase PR.

[0051] During the step 130, the main board 12A generates an elementary signature SE for each of the electronic boards 12A to 12N.

[0052] Such an elementary signature SE for a given electronic board 12A to 12N is, for example, generated from configuration data specific to this electronic board 12A to 12N using, for example, methods analogous to those used in order to generate the global signature SG.

[0053] During the following step 140 the main board 12A stores the generated elementary signatures SE and the generated global signature SG in its internal memory M.

[0054] Then, during the same step 140, the main board 12A provides each electronic board 12A to 12N with the generated elementary signatures SE and the configuration data specific to this board 12A to 12N.

[0055] Then, each electronic board 12A to 12N retrieves the elementary signature which is associated with it by the main board 12A.

[0056] During the following step 145, each board 12A to 12N calculates its elementary signature SE from configuration variables stored in its internal memory M using, for example, methods analogous to those used in order to generate the global signature SG, and fixes the signature variable to be equal to the calculated value of the elementary signature.

[0057] During the following step 150, each electronic board 12A to 12N compares the retrieved elementary signature SE with the signature variable that it has in its internal memory M (it should be noted that, if no information has been stored in this memory M beforehand, the board will behave as if the signature variable is different and the data are not valid).

[0058] Then, each electronic board (12A to 12N) checks the validity of the configuration variables stored in its internal memory using the retrieved elementary signature (SE) and the signature variable.

[0059] In order to check the validity of the corresponding configuration variables, each electronic board 12A to 12N compares the retrieved signature variable with the retrieved elementary signature SE.

[0060] If the elementary signature SE coincides with the signature variable, the corresponding electronic board 12A to 12N validates the configuration variables and the board 12A to 12N moves on to the step 180. In the opposite case, the corresponding electronic board 12A to 12N moves on to the step 160.

[0061] During the step 180, the corresponding board 12A to 12N retrieves the configuration variables from its internal memory M and, for example, puts these variables in place in order to

be operational.

[0062] During the step 160, the board 12A to 12N retrieves the configuration data which are associated with it and are provided by the main board 12A, calculates the received data signature SE and checks that it coincides with the signature SE provided.

[0063] Then, the corresponding board 12A to 12N fixes the signature variable to be equal to the calculated or retrieved elementary signature SE and fixes the configuration variables to be equal to the retrieved configuration data.

[0064] At the end of this step 160, the corresponding board 12A to 12N retrieves the configuration variables from its internal memory and, for example, puts these variables in place in order to be operational.

[0065] Thus, after the steps 160 and 180, each board 12A to 12N has its configuration data and the signature SE and has a copy of the configuration data and of the signature in its memory M.

[0066] The step 190 is the final step of the bootup phase PR, at the end of which the electronic system 20 is operational.

[0067] Advantageously, following the step 180, the boards 12B to 12N check periodically that the configuration data used are indeed authorized. For this, they check that the elementary signature SE used, that is to say the signature variable, is always the same as that provided by the main board 12A.

[0068] If this is not the case, the board generates an error message intended, for example, for the user, and interrupts the execution or returns to the step 160 in order to retrieve the new configuration data (this choice depends upon the function provided, for example for a security function the product will be set into a secure state).

[0069] Advantageously, the method considerably simplifies the replacement of an electronic board 12B, ... 12N in the electronic system 10 by a new electronic board.

[0070] In this case, the method further comprises the following steps:

- replacement of an electronic board 12B, ... 12N in the electronic system 10 by a new electronic board;
- generation of an elementary signature SE for at least the new electronic board from the configuration data stored in the centralized storage module 14;
- transmission of the elementary signature SE at least to the new electronic board; and
- performance of the step 150 of checking the configuration variables for the new electronic board.

[0071] It will be understood that the invention offers a certain number of advantages.

[0072] In fact, the method of transmitting and checking the validity of configuration data

according to the invention makes it possible to perform a reboot of the electronic system particularly quickly since only the data not present will be sent.

[0073] In particular, during the reboot phase of the electronic system 10, the configuration data, when they are unchanged, are not transmitted again to the corresponding electronic boards.

[0074] The validity of these data is checked using the corresponding elementary signatures which are transmitted to the corresponding electronic boards particularly quickly.

[0075] The validity of these data is checked periodically using the corresponding elementary signatures, which makes it possible ensure that a change of configuration is properly applied (or that the appropriate actions will be carried out).

[0076] This then makes it possible to considerably reduce the execution time for carrying out the reboot phase and therefore the total reboot time of the electronic system.

PATENTKRAV

1. Fremgangsmåde til transmission og kontrol af gyldigheden af konfigurationsdata i et elektronisk system (10) med centraliseret lagring af konfigurationsdata, hvilket elektronisk system omfatter en flerhed af elektroniske kort (12A, ...,12N), der er egnede til implementering af det elektroniske systems (10) funktion ved anvendelse af konfigurationsdata, der er specifikke for hvert af disse kort (12A, ...,12N), og et modul med centraliseret lagring (14), der er egnet til centraliseret lagring af konfigurationsdata for samtlige elektroniske kort (12A, ...,12N), hvor hvert elektronisk kort (12A, ...,12N) omfatter en intern hukommelse, der er specifik til lagring af en variabel signatur og konfigurationsvariabler;

hvilken fremgangsmåde omfatter følgende trin:

- generering (130) af en elementær signatur (SE) for hvert af de elektroniske kort (12A, ...,12N) ud fra konfigurationsdata, der er lagret i det centraliserede lagringsmodul (14);
- transmission (140) til hvert elektronisk kort (12A, ...,12N) af den elementære signatur (SE), der er specifik for dette kort (12A, ...,12N);
- beregning (145) ved hjælp af hvert elektronisk kort (12A, ...,12N) af den variable signatur som en funktion af de konfigurationsvariabler, der er lagret i dette elektroniske korts (12A, ...,12N) interne hukommelse;
- kontrol (150) ved hjælp af hvert elektronisk kort (12A, ...,12N) af gyldigheden af konfigurationsvariablerne, der er lagret i dette korts (12A, ...,12N) interne hukommelse ved anvendelse af den modtagne elementære signatur (SE) og den variable signatur; og

hvor fremgangsmåden omfatter følgende trin implementeret for hvert elektronisk kort (12A, ...,12N), for hvilket i trinnet med kontrol (150) af konfigurationsvariablernes gyldighed konfigurationsvariablerne anses for ugyldige:

- hentning (160) af konfigurationsdata, der er specifikke for dette kort (12A, ...,12N) og ændring af konfigurationsvariablerne ud fra de hentede konfigurationsdata.

2. Fremgangsmåde ifølge krav 1, hvor hver elementær signatur (SE) genereres af ét enkelt af de elektroniske kort (12A, ...,12N) ved anvendelse af de konfigurationsdata, der er specifikke for de elektroniske kort (12A, ...,12N), der er lagret i det centraliserede lagringsmodul (14).

3. Fremgangsmåde ifølge krav 1 eller 2, hvor konfigurationsdata lagres i form af en sikret datastruktur (20), der er forbundet med en global signatur (24).

4. Fremgangsmåde ifølge krav 3, hvilken fremgangsmåde omfatter, før trinnet med generering (130), følgende trin:

- kontrol (120) af gyldigheden af konfigurationsdata fra datastrukturen (20) ved anvendelse af den globale signatur (24), der er forbundet med denne struktur (20);

og trinnet med generering (130) udføres, hvis gyldigheden af konfigurationsdataene er kontrolleret.

5. Fremgangsmåde ifølge krav 4, hvor efter trinnet med generering, samtlige elementære signaturer (SE) og den globale signatur (24) lagres i den interne hukommelse af ét af de elektroniske kort (12A, ...,12N), betegnet hovedkortet (12A).

6. Fremgangsmåde ifølge krav 5, hvor trinnene med kontrol (120) af gyldigheden af konfigurationsdataene og generering (130) af en elementær signatur (SE) for hvert af de elektroniske kort (12A, ...,12N) implementeres af hovedkortet (12A).

7. Fremgangsmåde ifølge et hvilket som helst af de foregående krav, hvor der i trinnet med hentning (160) af konfigurationsdata foretages en kontrol af, at de hentede konfigurationsdata svarer til den elementære signatur (SE), derefter modificeres konfigurationsvariablerne ud fra de hentede konfigurationsdata, således at de hentede konfigurationsdata lagres i kortets (12A, ... 12N) interne hukommelse.

8. Fremgangsmåde ifølge et hvilket som helst af de foregående krav, hvor fremgangsmåden omfatter, for hvert elektronisk kort (12A, ...,12N), for hvilket i trinnet med kontrol (150) af konfigurationsvariablernes gyldighed konfigurationsvariablerne anses som gyldige:

- hentning (180) ved hjælp af det elektroniske kort (12A, ..., 12N) af konfigurationsvariablerne fra kortets (12A, ... 12N) interne hukommelse.

9. Fremgangsmåde ifølge et hvilket som helst af de foregående krav, hvor trinnet med hentning (160) af konfigurationsdata endvidere omfatter:

- hentning ved hjælp af det elektroniske kort (12A, ..., 12N) svarende til konfigurationsvariablerne fra kortets (12A, ... 12N) interne hukommelse.

10. Fremgangsmåde ifølge et hvilket som helst af de foregående krav, hvor fremgangsmåden omfatter følgende trin:

- udskiftning af et elektronisk kort (12B, ... 12N) i det elektroniske system (10) med et nyt elektronisk kort;
- generering af en elementær signatur (SE) til mindst det nye elektroniske kort ud fra konfigurationsdata, der er lagret i det centraliserede lagringsmodul (14);
- transmission til mindst det nye elektroniske kort af den elementære signatur (SE); og
- udførelse af trinnet med kontrol (150) af konfigurationsvariablerne for det nye elektroniske kort.

11. Computerprogramprodukt, der omfatter des softwareinstruktioner, der, når de udføres af et edb-udstyr, udfører fremgangsmåden ifølge et hvilket som helst af de foregående krav.

12. Elektronisk system (10) med centraliseret lagring af konfigurationsdata, hvilket elektronisk system omfatter en flerhed af elektroniske kort (12A, ...,12N), der er egnede til at implementere det elektronisk systems (10) funktion ved anvendelse af konfigurationsdata, der er specifikke for hvert af kortene (12A, ...,12N), og et modul med centraliseret lagring (14), der er egnet til centraliseret lagring af konfigurationsdata for samtlige elektroniske kort (12A, ...,12N), hvor hvert elektronisk kort (12A, ...,12N) omfatter en intern hukommelse, der er specifik til lagring af en variabel signatur og konfigurationsvariablerne;
hvilket elektronisk system (20) omfatter midler til implementering af fremgangsmåden ifølge et hvilket som helst af kravene 1 til 10.

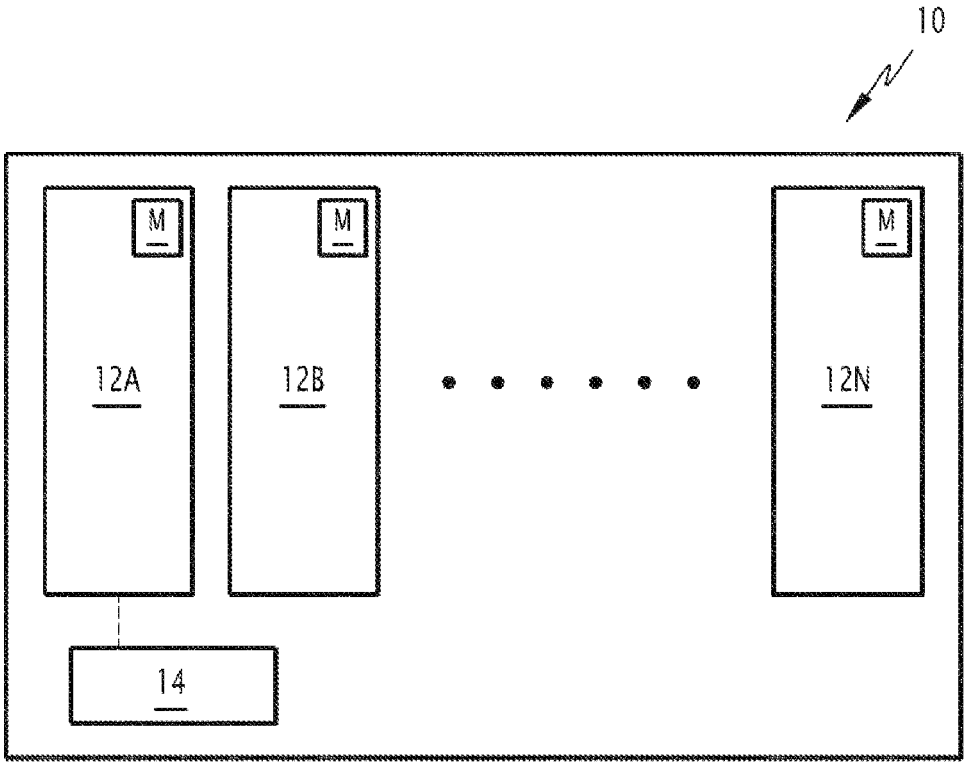

FIG.1

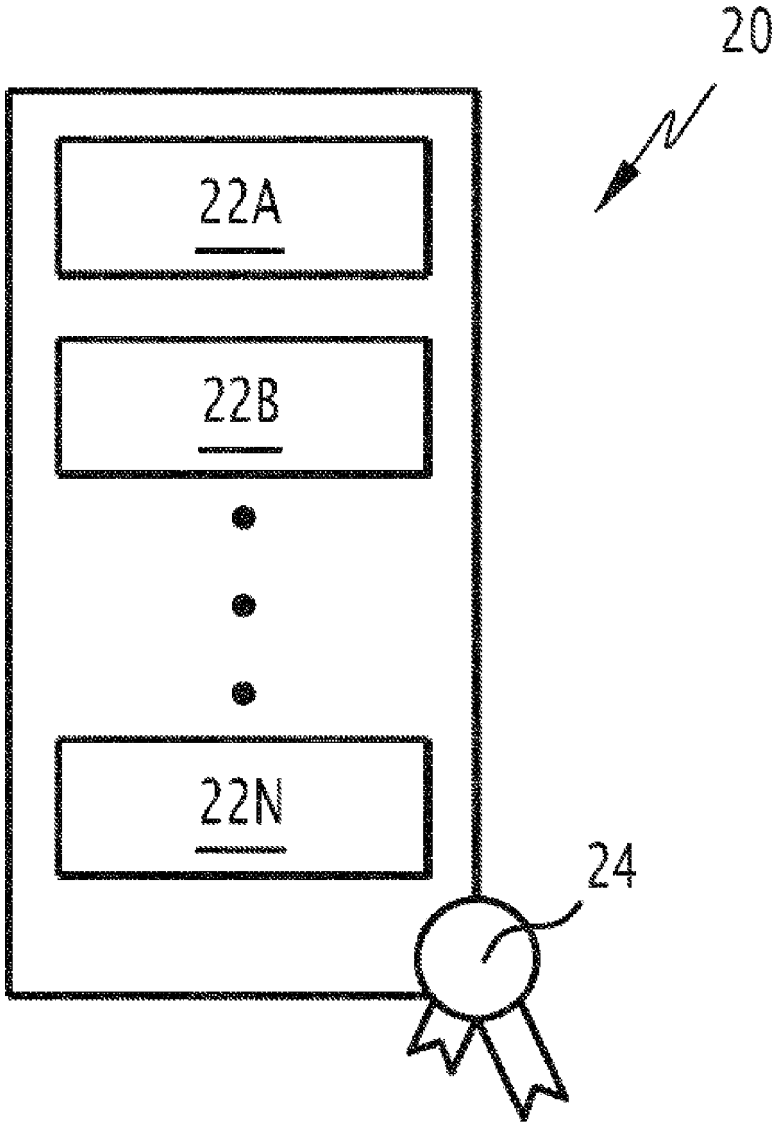

FIG.2

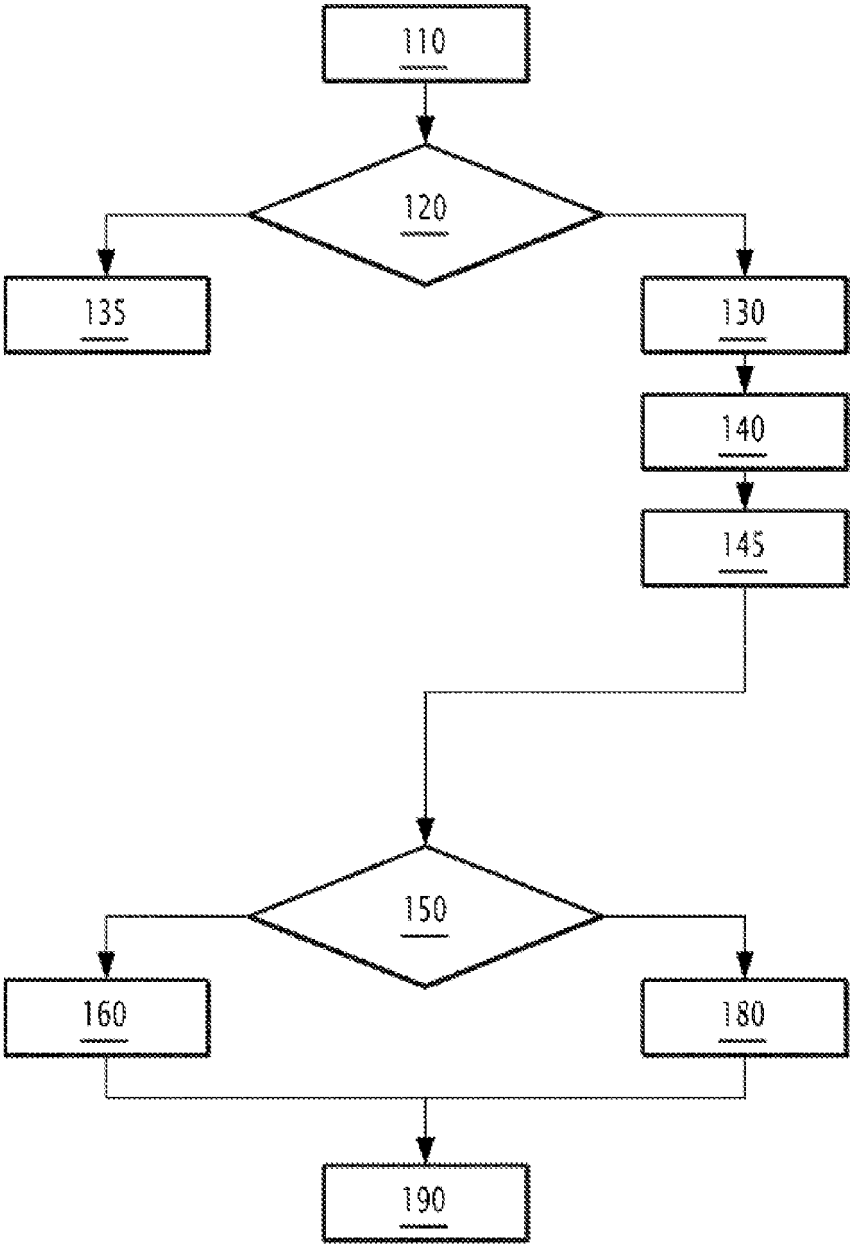

FIG.3