



(11)

EP 2 355 066 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
10.08.2011 Bulletin 2011/32

(51) Int Cl.:
G08C 17/02 (2006.01)

(21) Application number: **11000429.8**

(22) Date of filing: **20.01.2011**

(84) Designated Contracting States:
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
 Designated Extension States:
BA ME

(72) Inventor: **Nielsen, Martin Sandal**
6830 Nørre Nebel (DK)

(74) Representative: **Olesen, Kaj et al**
Patentgruppen A/S
Arosgaarden
Aaboulevarden 31
8000 Aarhus C (DK)

(30) Priority: **28.01.2010 DK 201000067**

(71) Applicant: **VKR Holding A/S**
2970 Hørsholm (DK)

(54) **Method of operating a controller, and a master unit configured as an access device**

(57) The invention relates to a method of operating a controller configured to control an independent control system (3). The independent control system (3) comprises at least two units wherein at least one of said units is designed to operate as a master unit (26, 30, 34, 62, 72) and wherein at least one of said units is designed to operate as a slave unit (2, 4, 6, 8, 60, 70), wherein at least one of said at least one master unit (26, 30, 34, 62, 72) further is configured as an access device, which can communicate with one or more external control units (64, 74, ECD, ECD1, ECD2, ECD3, ECDn), which are external to said first independent control system 3.

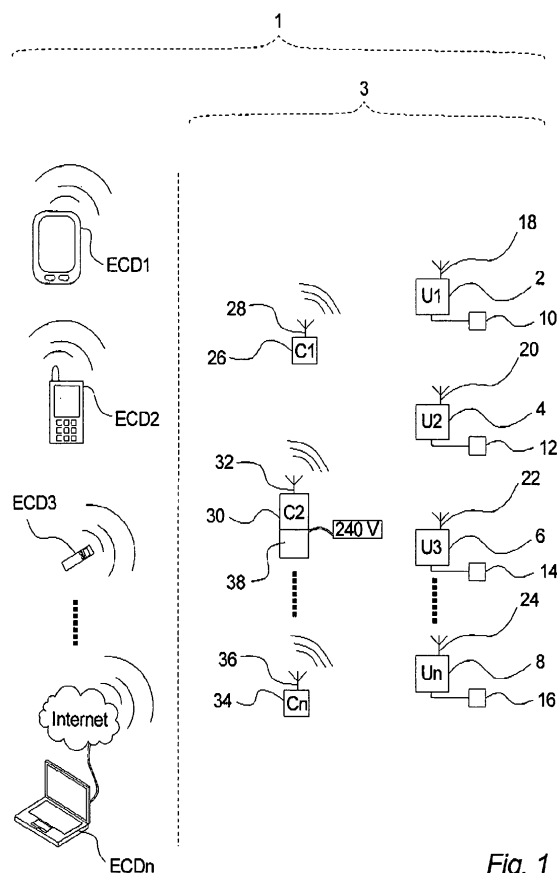


Fig. 1

Description**Background of the invention**

5 **[0001]** The invention relates to a method for controlling a control system according to claim 1.

Description of the Related Art

10 **[0002]** In the recent years the development of new communication means have been widely increased, both to ease communication, to increase the speed of communication, to save space on the radio frequency networks, to consume less power during communication and the like. Examples of such developed communication means could be e.g. Blue-tooth, wibree, zigbee, LAN, WLAN, common cell phone networks and the like. These communication methods have been and will most likely in the future be integrated in a plurality of different devices such as cell phones, PDAs, laptops and the like, to obtain the advantages mentioned above and to facilitate communication between the plurality of different
15 devices. Even though such devices normally facilitate communication with devices facilitating the same communication means, they normally do not facilitate communication with other communication means e.g. smaller independent control systems using other communication methods. Due to the fact that these devices to a great extent are common household items it would be advantageous if these devices facilitate communication with other communication means and control systems which are already implemented.

20 **[0003]** The international patent application WO 03/028300 A1 relates to a remote control system using a mobile communication terminal. A user of the mobile communication terminal executes a program in the mobile communication terminal to communicate wirelessly with a controller. The mobile communication terminal hereby can transmit commands, e.g. state information of a controlled apparatus to remotely controlled apparatuses. A security code is added to the transmitted signal, and when the controller receives a contact request from the mobile communication terminal, the
25 contact request is authenticated by the controller. The communication between the mobile communication terminal and the controller could be performed by a short message service (SMS), WAP or the like. A control command from the mobile communication terminal is analyzed by the controller and then transmitted, and the transmitted control command is processed in the controlled apparatus.

30 **[0004]** A problem with this approach is that no authentication of the controller is performed by the controlled apparatus when it receives a signal, which makes the communication less safe. Further, the controlled apparatus is controlled dependently of the controller.

35 **[0005]** It is therefore an object of the invention to facilitate safe control of independent control systems without the disadvantages mentioned above.

Summary of the invention

40 **[0006]** The invention relates to a method of operating a controller configured to control an independent control system comprising at least two units wherein at least one of said units is designed to operate as a master unit and wherein at least one of said units is designed to operate as a slave unit, where said at least one master unit and said at least one slave unit comprise one and the same code key, said code key being unique to said independent control system, and where said at least one slave unit comprises an address being unique to said at least one slave unit and being registered by said at least one master unit, wherein at least one of said at least one master unit further is configured as an access device, which can communicate with one or more external control units, which are external to said independent control system,
45

- whereby said at least one slave unit is independently operateable by means of said at least one master unit and/or a master unit configured as an access device,
- whereby said at least one slave unit is dependently operateable by at least one external control device where said
50 at least one external control device is operating said at least one slave unit via said at least one master unit configured as an access device,
- whereby an operation of said at least one slave unit comprises:

55 receiving from at least one external control device a control signal by said at least one master unit configured as an access device where said control signal at least comprises a control command relating to at least one of said at least one slave unit and identification of said at least one external control device,

- whereby, when said at least one master unit configured as an access device receives said control signal from said at least one external control device, said at least one master unit configured as an access device processes said received control signal from said at least one external control device to perform authentication of said at least one external control device and to identify said at least one slave unit in order to retrieve said address being unique to said at least one slave unit, and
- whereby said at least one master unit configured as an access device transmits coded control signals to said at least one slave unit on the basis of said control commands of said control signals from said at least one external control device, when said at least one external control device is authenticated by said at least one master unit configured as an access device.

[0007] The independent control system is a safe control system, among other things due to that master units and slave units of the independent control system comprise the one and same code key, and that slave units comprise an address being unique to the slave units. Furthermore, since slave units of the independent control system are identified by the master unit configured as an access device, so that the master unit knows the address unique to each slave unit, it can be achieved that the unique address of the slave unit is kept internal in the independent control system, and is not known outside the independent control system. Therefore it is possible for master units configured as an access devices in a safe way to control the access to the slave units from the external control devices. This is advantageous, since the safety of the independent control system is not jeopardised by the use of an external control device.

[0008] By utilizing external control devices as explained above, it is likewise possible to add control devices to the independent control system, different from the master units of the independent control unit, whereby a more dynamic and user friendly operation of the control system can be achieved without jeopardising the safety of the control system.

[0009] It is understood that control commands may comprise a control command to request that a slave unit initiates an action, e.g. to open and close a window, operate a shutter, a blind or the like, it may comprise a status request to receive a status update from a slave unit and/or a master unit, for example to access data from sensors such as rain sensors, position sensors, temperature sensors, anemometers or the like.

[0010] For the purpose of this application the term "identification" is understood that identification of said at least one external control device may take place by an address and/or credentials, but identification may also be performed based on type of external device or the communication link or protocol used with the external device or parameters of the protocol used or combinations hereof. The identification may likewise comprise that the external control unit transmits an identification code, e.g. an identification code unique to the external control device, to the master unit configured as an access device. Furthermore, an identification code may in an aspect of the invention be added to the external control device by means of a pairing process between the external control device and a master unit configured as an access device. The pairing process may comprise a gathering of information from the external control device by means of a near field network such as blue tooth, zigbee or the like, and may comprise that the master unit configured as an access device transmits a code to the external control unit which is stored in the external control unit. This code should then be transmitted by the external control device (e.g. by incorporating the code in the control signal) and may be utilized for identification and/or authentication of the external control device.

[0011] For the purpose of this application, the term "authentication" shall be understood as that a master unit configured as an access device processes the received identification information and/or other data received from the external control device, to determine if the external control device is registered as an external control device allowed to transmit control commands to a slave unit of the independent control system and/or request slave unit status and/or master unit status. The authentication preferably at least comprises processing of the transmitted identification of the external control device.

[0012] Likewise, for the purpose of this application, the term "independent control system" shall be understood as that the control system can operate completely independent of control devices external to the independent control system (e.g. the external control devices) by means of only at least one master unit and at least one slave unit.

[0013] Furthermore, for the purpose of this application, the term "dependently operateable" shall be understood as that the at least one external control device can only access slave units of the independent control system via a master unit configured as an access device.

[0014] Still further, it is understood that the external control device(s) preferably comprise identification means for identifying the at least one external control device(s).

[0015] Preferably, an authentication request signal to said at least one master unit configured as an access device is generated by said at least one slave unit in response to said coded control signals, whereby said at least one master unit configured as an access device generates and transmits a response signal to said authentication request from said at least one slave unit, and whereby said at least one slave unit processes said coded control signals if said response signal from said at least one master unit configured as an access device is verified by said at least one slave unit.

[0016] Hereby, improved safety of the control system is achieved.

[0017] Advantageously, said authentication request signal to said at least one master unit from said at least one slave

unit is generated at least partly by means of said code key.

[0018] Hereby an enhanced, safe communication between the master units and the slave units is achieved.

[0019] According to a further advantageous embodiment of the invention, when said at least one master unit configured as an access device receives said control signals from said at least one external control device, the at least one master unit configured as an access device transmit at least one acknowledgement signal to said at least one external control device.

[0020] Hereby a safe and reliable method for operating a control system is achieved. Furthermore, it may also facilitate a more enhanced, user friendly control system if the user of the external control device is informed about that the external control device has received the acknowledgement signal from the master unit configured as an access device. The acknowledgement signal may comprise an acknowledge regarding that the command signal is received and/or that the command signal (and/or control command of the command signal) is or is not authenticated, but the acknowledgement signal may also comprise other information relevant for the user/operator of the external control unit.

[0021] Advantageously, the communication in said independent control system may operate by means of communication means of a different type than at least one type of communication means of said at least one external control device utilized for communication between said master unit configured as an access device and said at least one external control device.

[0022] For the purpose of this application the term "communication means", which may also be referred to as communication methods, shall be understood means facilitating communication on the basis of a communication protocol and/or message format allowing systems to communicate over a transmission medium. Such communication means may e.g. be e.g. Bluetooth, wibree, 3G, Turbo-3G, zigbee, LAN, WLAN, wireless USB®, SMS, instant messenger, common fixed-line phone network, cell phone networks, WAP or any other suitable means. Hereby external control devices may access the independent control system in a very advantageous way, since external control devices may operate with different communication means than the independent control system

[0023] In a preferred embodiment of the invention, said master unit configured as an access device may facilitate communication between units of the independent control system, and at least one of a plurality of different communication means.

[0024] This facilitates that the master unit configured as an access device, and hereby the independent control system, may support one or more different external control devices operating with different communication means. The master unit configured as an access device thereby facilitates translation between the communication means utilized internal in the independent control system, and the external control unit, thereby enhancing the user friendliness of the control system.

[0025] According to a further advantageous embodiment of the invention, communication to said at least one slave unit distinguish between critical and non-critical coded control signals from said at least one master unit and/or master unit configured as an access device.

[0026] Hereby it is achieved that the at least one slave unit may change operation form / execute a command directly, without communication with the at least one master unit, thereby minimising communication in the independent control system.

[0027] A non-critical control signal is preferably a signal which does not compromise the safety of the independent control system. Such a non-critical control signal may e.g. be a signal for operating a roof window high above ground, operating a shutter, a blind, light means or the like.

[0028] A critical control signal is preferably a signal which may, at least under certain circumstances, compromise the safety of the independent control system. Such a critical control signal may e.g. be a signal for operating a window, a gate or door, an alarm, a window or the like.

[0029] Advantageously, a non-critical control signal is processed by said at least one slave unit without authentication of said at least one master unit.

[0030] Hereby communication in the independent control system is minimized without compromising with the security of the control system.

[0031] In a preferred embodiment of the invention, said processing comprises an evaluation of the control signal received from an external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) to determine if the control command of the control signal should be accepted.

[0032] This is advantageous in that even though an external control device is authenticated by the master unit configured as an access device, there may be several situations where the control possibilities of an authenticated external control device should be reduced e.g. for safety reasons and/or to enhance management of the control system.

[0033] For the purpose of this application, the evaluation of the control signal shall be understood as that the control unit configured as an access device processes data such as e.g. data received from the external control device (e.g. ID, control command, communication means utilized by the external control device for transmitting the signal etc.), data regarding relevant slave unit(s) (e.g. to a slave unit to which a control command is intended), different safety measures such as access security parameters (explained in more details later on) of slave units, hierarchy levels of external control

devices (explained in more details below) and/or the like, to determine if the control command should be allowed. It is understood that the external control device may (beyond transmitting control commands and identification) also transmit other data relevant to the evaluation of the control signal and/or external control device. Such data may e.g. be user specific data (especially if more users with different access allowances may operate the same external control device e.g. by utilizing different user identification or user profiles), data regarding the geographical location of the external control command at the time of transmitting the command signal, time of transmittance of the command signal and any other data which may be relevant to the authentication of the control signal and/or external control device.

[0034] Advantageously, communication to at least one of said at least one slave units of the independent control system is associated with at least one access security parameter.

[0035] For the purpose of this application, the term "access security parameter" shall be understood a parameter or a group of parameters which is/are associated to a slave unit of the independent control system and which defines security demands which has to be complied with to allow operation/access to the slave unit. The access security parameter may e.g. be a security flag in a slave unit, and/or a security flag in another master unit. However, the access security parameter is preferably a security flag stored in a master unit configured as an access device, for example in an access security parameter table.

[0036] In an aspect of the invention, the access security parameter may change safety level over time, and in such a case, the master unit configured as an access device is updated over time, at least if the status of the access security parameter in stored in the master unit configured as an access device.

[0037] By introducing an access security parameter assigned to a slave unit, and utilizing the access control parameter in the above.mentioned evaluation, it is possible in an advantageous way to decide in which situations an authenticated external control device should be prevented or allowed to access functions of a slave unit to uphold sufficient security.

[0038] In an advantageous embodiment of the invention, the said at least one access security parameter is selected from a group of access security parameters comprising at least two access security parameters.

[0039] This facilitates easy management and association of an access security parameter to a slave unit. The access control parameter group may define an access security parameter hierarchy so that by choosing an access control parameter, the safety level of the slave unit required to allow access to/operation of the slave unit may easily be defined. Furthermore, it may ease the division of a group of slave units in the independent control system into a group of slave units with different safety levels.

[0040] In a further advantageous embodiment of the invention, the said at least one access security parameter is dependent of a time parameter.

[0041] This may be advantageous in that it is hereby possible to enable the independent control system to allow or refuse a control command based on the time of the day. Preferably, the slave unit and/or master unit configured as an access device at least in this embodiment comprises a clock/time function to be able to register the time of receiving a control signal. Likewise or instead, the external control device may transmit the time of transmittance of the control signal, as a part of the control signal.

[0042] It is understood that the dependence of a time parameter may also comprise that the time parameter may define one or more time limits used for defining different security levels for the same slave unit. Likewise, it is understood that the dependence of a time parameter may comprise that the type of access security parameter is change over time, e.g. by choosing between different access security parameters in the said group of access security parameters.

[0043] Advantageously, said at least one access security parameter is associated with demands to the geographical location of one or more of said external control devices.

[0044] For safety reasons, it is advantageous to only allow access to a slave unit from an external control device if an external control device transmitting the control signal is within a certain geographical distance from the independent control system, for example in the case of performing safety critical operation such as opening a window, a door, a gate or the like. The independent control system may therefore for example ensure that safety critical control commands and/or control demands which is dedicated to a slave unit assigned a certain access security parameter has to be transmitted by means of a near field network allowing only close range communication. The near field network facilitates communication between the master unit configured as an access device and the external control unit only within a limited range, and may be e.g. Bluetooth, Zigbee or the like. Thereby, an automatic safety control is established in that at least critical functions of the independent control system in at least some situations are not available/allowed by utilizing certain communication means such as GPRS, WLAN, 3 G or the like, which facilitates communication over a longer range. the independent control system, and the external control unit, or the like.

[0045] In a advantageous embodiment of the invention, at least one of said at least one external control device is assigned at least one hierarchy level selected from a plurality of hierarchy levels.

[0046] In this way, advantageous evaluation of external control devices and/or control command of the received control signal may be achieved. Furthermore, it may facilitate a further safety enhancement in that it is possible to set up which slave units of the independent control unit the individual external control device and/or individual user (e.g. implemented by means of a user ID transmitted with the control signal) of the external control unit may access and/or control, and in

which way.

[0047] In an aspect of the invention, the evaluation comprises processing of said hierarchy level assigned to an external control device and said access security parameter assigned to a slave unit to determine if a control signal should be accepted or denied.

[0048] In a further advantageous embodiment of the invention, said control signals from the at least one external control device is evaluated by said at least one master unit configured as an access device on the basis said at least one hierarchy level assigned to said at least one external control device.

[0049] Hereby, an advantageous aspect of the invention is achieved, since it hereby is possible to assign an external control, device a different safety level. This e.g. facilitates that different users and/or external control devices may gain various access to different functions of the independent control system. Furthermore, safety of the control system may be enhanced.

[0050] Furthermore, the said control signals from said at least one external control device may advantageously be evaluated on the basis of geographical placement of said at least one external control device, user information of the user operating said at least one external control device, time and/or date, distance between the said at least one master unit configured as an access device and said at least one external control device, and/or the utilized type of communication means.

[0051] By performing the evaluation based on one or more of these parameters a more safe and dynamic system may be achieved.

[0052] For example, if the external control device utilizes a near field network, and the user of the external control unit is accepted to perform the transmitted control command within the independent control system, the control command may be accepted. The external control device may in this example for example be a laptop communicating wirelessly with the master unit configured as an access device by means of e.g. Bluetooth. The user may as one example be a parent logged onto a user interface (for example a user interface as explained later on) for control of the independent control system, and when the master unit configured as an access device recognizes the logged in parent and that a near field network is utilized, a safety critical control command may be accepted even though it is transmitted from an external control unit and not a master unit of the independent control system.

[0053] According to a further advantageous embodiment of the invention, said master unit configured as an access device imposes a safety limit to a control command of the said received control signal.

[0054] This may increase control possibilities of the independent control system without jeopardizing safety. The safety limit may facilitate that in some safety critical situations, a control command is limited. For example an external control device transmitting a control signal to open a window to e.g. 80% of its total opening range may be imposed said safety limit so that the window is only allowed to open to e.g. 5% or 10% of its total opening range. Thereby, the window is opened, and unauthorised persons are not able to enter through the window. The safety limit is preferably imposed during the above mentioned evaluation, but it may also be imposed before or after the evaluation.

[0055] In a further advantageous embodiment of the invention, an user interface is communicated to said at least one external control device, and said user interface is operated by a user to access functions of the independent control system.

[0056] Hereby it is achieved that already existing external control devices may operate slave units of the independent control system by means of the user interface added to/implemented in the external control device. This is especially advantageous since a plurality of different control devices hereby may be configured to access and control units of the independent control system. The user interface may for example be implemented in a platform-independent object-oriented programming language such as e.g. a JAVA. This may e.g. facilitate cross-platform (also known as multi platform) implementation of the user interface. Another example may be that the user interface may be implemented in a web browser, e.g. in a way so that the user may accesses a homepage and enter a user login (e.g. also utilizing a digital signature) to gain access to control of the control system. Thereby, it may be possible in an advantageous way to utilize PC's, laptops, handheld wireless devices such as mobile phones, PDAs, GPS, MP3 players or the like for accessing functions of the independent control system.

[0057] Preferably, the at least one external control device accesses aliases to the at least one slave unit of the independent control system.

[0058] Hereby, it is possible to maintain the safety of the independent control system, since the addresses, key codes and the like of the independent control system are not known to the external control devices.

[0059] Advantageously, said at least one external control device is updated with the status of said at least one slave unit of the independent control system continuously, periodically, as a response to a slave status request signal from an external control device which could be generated automatically or manually by a user of said external control device or any combination thereof.

[0060] Hereby it is possible for a user of an external control device to retrieve status of the slave units of the slave units of the independent control system. This facilitates that the user may be updated with the status of the units of the control system, e.g. to see which windows that are open or closed, if it rains at the building which comprises the independent control system (if one of the slave unit is a rain sensor), the temperature (if one of the slave unit is a temperature

sensor), to see status of shutters and/or blinds, or the like.

[0061] Advantageously, the before mentioned at least one hierarchy level may be selected based on the type of the communication link used.

[0062] Hereby it is possible to maintain the security, because external devices using a secure type of communication like for example wired or near field communication may access high security features like opening windows, while less secure types of communication like for example WLAN may be restricted to access features/functions without risk to security, for example dimming light.

[0063] The invention may furthermore relate to a unit being a master unit configured as an access device, said master unit configured as an access device being a part of an independent control system comprising at least one slave unit,

- wherein said master unit configured as an access device and said at least one slave unit are configured to comprise one and the same code key, said code key being unique to said independent control system,
- wherein said at least one slave unit comprise an address being unique to said at least one slave unit and being registered by said at least one master unit,
- wherein said master unit configured as an access device is configured for receiving and processing a control signal received from at least one control device external to said independent control system, said control signal at least comprising a control command relating to a slave unit of said independent control system and identification of the least external control device transmitting the control signal, and
- wherein said processing comprises an authentication of the external control device and identification of the at least one slave unit to which said control command is related, in order to retrieve said address being unique to said at least one slave unit.

[0064] Such a unit being a master unit configured as an access device is advantageous in that it facilitates safe communication between external control devices and units of the independent control system.

[0065] In an advantageous aspect of the invention, the above mentioned unit being a master unit configured as an access device is configured to operate according to any of the claims 1-21.

[0066] Advantageously, the above mentioned unit being a master unit configured as an access device may be configured to be retrofitted into an existing independent control system to allow access to said at least one slave unit by means of said at least one external control device.

[0067] By retrofitting a unit into an existing independent control system, the existing independent control system is capable of being updated with newer and more modern management facilities.

[0068] The invention may also relate to use of the method according any of claims 1-15 as well as according to other aspects described in this document in a building automation system such as a home automation system.

[0069] Furthermore, the invention may relate to use of the method according any of claims 1-15 as well as according to other aspects described in this document for operating at least one window, blind, shutter, door, gate, awning, curtain or light source of a building and/or the premises of a building.

The figures

[0070] The invention will be explained in further detail below with reference to the figures of which

fig. 1 shows a general overview of a system according to an embodiment of the invention,

fig. 2 shows a possible communication scenario according to an embodiment of the invention,

fig. 3 shows a flowchart according to an embodiment of the invention,

fig. 4 shows a an embodiment of an access security parameter group according to an embodiment of the invention,

fig. 5 shows a hierarchy table for handling a hierarchy of an external control device according to an embodiment of the invention,

fig. 6 shows updating of external control devices with the status of one or more slave units, and

fig. 7 illustrates one example of a method of operating a controller configured to control an independent control system,

according to the invention.

Detailed description

[0071] Fig. 1 shows a general overview of a control system 1 according to an embodiment of the invention. The system 1 comprises an independent control system 3, and at least one external control device ECD1-ECDn.

[0072] The independent control system 3 comprises a plurality of units 2, 4, 6, (U1-Un) comprising or linked to for example drive units for various devices 10,12,14,16. These devices may for example be activators of various types and used in a wide variety of applications. The units 2, 4, 6, 8 may also or instead comprise or be linked to assorted apparatuses, sensor devices, indicating devices, controllers etc. that may need to receive information, control signals etc. at certain points of time. Examples of the devices 10, 12, 14, 16 may be means such as actuators, motors or the like for controlling windows, blind, shutters, doors, gates, awnings, curtains, light sources of a building, it may be rain sensors, anemometers, temperature sensors or the like.

[0073] Preferably, the independent control system is a building automation system such as a home automation system.

A building automation system/home automation system may also be known as domotics.

[0074] A common feature of the units 2, 4, 6, 8 is that it is necessary or advantageous to be able to transmit some sort of information signal to the units, e.g. a control command, a status request or the like. Furthermore, it may be necessary or preferred to be able to receive information or signals from the units, e.g. confirmation signals, acknowledgement signals, measurement signals, status signals etc.

[0075] In the embodiment shown in fig. 1, all units 2, 4, 6, 8 are equipped with receiving means for radio frequency signals, e.g. including antenna means 18, 20, 22, 24. Each unit comprises e.g. one or more motor drive units or control units and is connected to a driven or controlled member 10,12,14,16. It will be understood that the means driven by, controlled by etc. the unit may be integrated with the unit. It will further be understood that a system may comprise one or more units 2, 4, 6, 8 as illustrated and that, when more than one unit is involved, these may be similar or dissimilar and may control one or more similar or different devices 10, 12, 14, 16. The units 2, 4, 6, 8 may also be referred to as controllable units or slave units in the following.

[0076] The independent control system 3 in fig. 1 further comprises a remote control unit (C1) 26 designed for transmission of signals by means of radio frequency transmission means, e.g. including antenna means 28. This control unit 26 may be used for transmitting control signals or other types of signals to one or more of the units UI - Un in the independent control system 1, e.g. by request from a user accessing buttons, touch screens or the like of the remote control unit (C1) 26.

[0077] As illustrated, the independent system 3 may likewise comprise at least one additional control unit (C2, Cn) 30, 34 similar to the first remote control, e.g. designed for transmission of signals by means of radio frequency transmission means, e.g. including antenna means 32, 36 or dissimilar to the first remote control, e.g. designed for transmission by other means such as wired means, infra red transmission means etc (not illustrated in fig. 1).

[0078] It is of course understood that the slave units 2, 4, 6, 8 may instead of comprising receiving means for radio frequency signals be connected to other units of the system by means of one or more wires such as electrical wire, a bus system, optical wires or other any other wired communication means. Likewise, combinations receiving means for radio frequency signals and wires as mentioned above may be advantageous. Furthermore, infrared receiving means may in some aspects of the invention also be relevant.

[0079] The remote controls C1 - Cn will also be referred to as controllers or master units in the following.

[0080] The master units 26, 30, 34 (C1-Cn) and slave units may be continuously powered, e.g. by 230 Volt, powered by batteries, solar power, kinetic energy, a combination of different power supply technologies known to a person skilled in the art or any other suitable means.

[0081] An external control device ECD1-ECDn may e.g. be remote controls different from the remote controls of the independent system, common devices such as PDAs, cell phones, laptops, stationary PCs, pocket PCs, plug-in devices for PCs or laptops, or the like. An external control device ECD1-ECDn may access a slave unit U1-Un of the independent control system via at least one master unit 26, 30, 34 of the independent control system 3 which further is configured as an access device. In figure 1, the master unit 30 (C2) is further configured as an access device, and comprises an access control part 38 which facilitates communication and preferably also translation between the at least one external control device ECD1-ECDn and the independent control system 3. The slave units U1-Un may hereby be dependently operated by the at least one external control device ECD1-ECDn by means of the master unit configured as an access device. The slave units of the independent control system are furthermore independently operable by the master units C1-Cn of the independent system 3, and the master units C1-Cn can hereby access and control the slave units U1-Un independently of the external slave units ECD1-ECDn.

[0082] It is noted that master units configured as access devices besides facilitating communication and translation between the independent control system 3 and external control devices ECD1-ECDn may comprise all the functions of a master unit 26, 30, 34 as mentioned above.

[0083] In the following, a master unit configured as an access device may also be referred to as only access master unit.

[0084] In an embodiment of the invention, a plurality of master units C1-Cn are configured as access devices, and a plurality of external control devices ECD1-ECDn can access the independent control system 3 by means of any of these access master units. The access master unit(s) may be hierarchically divided, e.g. by numbers, addresses, codes or the like, to facilitate that only one master units configured as an access device is accessed at a time by external control devices ECD1-ECDn, to minimize redundancy, and the like.

[0085] Likewise, different external control devices ECD1-ECDn may be assigned different access master units, access master unit(s) may communicate internally to control the communication with external control devices ECD1-ECDn or the like.

[0086] If the independent control system 3 comprises more than one access master unit, an external control device ECD1-ECDn may be assigned to an access master unit randomly, or the external control device may be assigned to a preselected access master unit.

[0087] In an embodiment of the invention, a user interface may be applied to an existing user interface of an external control device(s) ECD1-ECDn. This additional user interface preferably comprises all means necessary for the user of the control device to gain access to the independent control system 3 and its functions. The additional user interface preferably utilise one or more already existing communication means of the external control device ECD1-ECDn, and may hereby communicate with at least one master unit configured as an access device 30 (C2) of the independent control system 3.

[0088] The external control devices ECD1-ECDn may communicate by means of communication means different from the communication means of the independent control system 3, and an access master unit of the independent system 3 may therefore comprise means for translating communication between the independent control system 3 and the at least one external control device (ECD1-ECDn).

[0089] Communication means utilized by the at least one external control device ECD1-ECDn, and supported by the access master unit may be both wired and wireless communication methods. Examples of such communication means could be e.g. Bluetooth, wibree, 3G, Turbo-3G, zigbee, LAN, WLAN, wireless USB®, SMS, instant messenger, common fixed-line phone network, cell phone networks, WAP or any other suitable means. For example, an access master unit may communicate with units of the independent control system 3 and facilitate communication by means of a plurality of different communication methods known to a person skilled in the art, and can hereby be an interface for communication between a plurality of different types of external control devices ECD1-ECDn, and the independent control system 3.

[0090] According to the invention, an external control device ECD1-ECDn transmits a control signal to the access master unit 30 of the independent control system 3. Such a control signal at least comprises a control command relating to at least one slave unit U1-Un of the independent control system 3, and identification of the external control device ECD1-ECDn transmitting the control signal(s). The identification of the external control device ECD1-ECDn transmitting the control signal(s) may also be referred to in the following as identification means.

[0091] The at least one master unit C1-Cn and the at least one slave unit U1-Un of the independent control system 3 comprise one and the same code key which is unique to the independent control system 3. Each of the slave units U1-Un of the independent control system 3 further comprise an address being unique to the individual slave unit U1-Un, and this unique addresses of the slave units U1-Un are registered by the at least one master unit C1-Cn. The external control device ECD1-ECDn do not know the code key which is unique to the independent control system 3, the unique addresses of the at least one slave unit U1-Un of the independent control system 3 and/or the general identification and communication form of the independent control system 3. Instead, the external control device(s) ECD1-ECDn preferably knows, accesses and/or utilizes aliases to the slave units U1-Un, master unit(s) C1-Cn and/or master unit(s) configured as access devices of the independent control system 3. These aliases are different to the internal identification of the slave units U1-Un, master unit(s) and master unit(s) configured as access devices of the independent control system 3. Examples of such aliases may be names given to the slave units U1-Un, e.g. "Living room awning 1", "Kitchen shutter A", "Office roof window 3", "Blind 22". Likewise, the aliases may be numbers (e.g. in the form of binary, hexadecimal and/or decimal numbers), it may be codes comprising any suitable symbols and/or formats or it may be any other suitable type of alias capable of acting as an alias for a slave unit. The communication between access master units and the external control device ECD1-ECDn, regarding the slave unit U1-Un of the independent control system 3, comprises these aliases or codes for these aliases, and do not comprise the code key unique to the independent control system 3 and the unique addresses of the at least one slave unit U1-Un. The aliases are registered by the access master unit (s), and the slave unit(s) to which a control command is dedicated is thereby identifiable due to that the access master unit both knows the aliases utilized by the external control device(s) and the internal identification of the slave units of the independent control system 3. By utilizing aliases for identifying the slave and/or master units of the independent control system 3, the safety of the control of the independent system 3 is not compromised when introducing external control devices to the independent control system 3.

[0092] Beyond translation between different communication means such as communication protocols, the access master unit may also comprise translation of control commands. For example, a control command comprising an "open"

control command to open a window may be translated to a command to a slave unit facilitating opening of a window anywhere in an interval between 0 and 100%, in an interval in steps between 0 and 255 (one byte) or the like. In such a case, an "open" command may for example be translated to a command to open the window to e.g. 100%, of its opening range.

[0093] In an embodiment of the invention which is not illustrated in any figure, the access master unit may impose a safety limit to control commands received from external control units. An external control unit may for example only be able to open windows, doors and gates to a predefined limit so that none unauthorized persons may enter the building. As an example, an "open" command to a window (e.g. a window near ground) transmitted from an external control device ECD1-ECDn far away from the independent control system 3 may be translated by the access master unit so that the specific window is only opened to maximum 5% or 10%. If the same command is transmitted from the external control device, but near the independent control system, the "open" command may on the other hand be translated by the master unit configured as an access device so that the specific window is allowed to be opened to its maximum limit. The safety limit may also be imposed based on the identification of the independent control unit and/or the user of the control unit.

[0094] Fig. 2 illustrates a system according an embodiment of the invention. The system 1 in this particular embodiment comprises one external control device 64, a master unit configured as an access device 62 and a slave unit 60, where the master unit configured as an access device 62 and the slave unit 60 are comprised in the independent control system 3. It is noted that a plurality of master units, master units configured as access devices, slave units and external control devices could be comprised in the control system 1.

[0095] The external control device 64, external to the independent control system 3, transmits a control signal 40 to the master unit configured as an access device 62. The control signal 40 at least comprises a control command relating to at least one slave unit 60 of the independent system 3, and identification of the external control device 64. In this case, the control command is dedicated the slave unit 60, but it could also be dedicated a group of slave units, all slave units or the like. The identification of the external control device 64 may be an ID of the external control device 64, a code key or the like. Furthermore, the identification of the external control device 64 may be unique to the external control device 64, it may be generated by the master unit configured as an access device 62 and given to the external control device 64 during a synchronization process/ pairing process with the master unit configured as an access device 62, or the like.

[0096] As mentioned above, the identification by the external control device 64 of the slave units to which the control commands are dedicated preferably comprises aliases of slave units.

[0097] The master unit configured as an access device 62 evaluates the control signal 40 from the external control unit 64, to perform authentication of the control signal 40 from the external control device 64, by authenticating the identification of the external control device 64. If the performed authentication of the identification of the at least one external control device 64 is verified, the control signal 40 from the external control device 64 is accepted.

[0098] In an embodiment of the invention which is not illustrated in fig. 2, the master unit configured as an access device 62 transmits an authentication request signal to the external control device 64, and the external control device 64 transmits a response signal to the master unit configured as an access device 62. If this response signal is verified by the master unit 62, the control signal 40 from the external control device 64 is accepted.

[0099] In another embodiment of the invention which is not illustrated in fig. 2 the external control device 64 transmits a preamble signal before the control signal 40. This preamble signal wakes up the master unit configured as an access device 62, and or slave units, e.g. low power units supplied with power from batteries, solar cells or the like, relevant to the following control signal 40. The preamble signal from the external control device 64 may comprise identification of the external control device 64 together with the preamble. Likewise the master unit configured as an access device 62 may facilitate the generation and transmittance of a preamble signal to the slave units, when it receives the control signal 40 from the external control device 64, to wake up the slave units relevant to the control signal 40.

[0100] Preferably, when the master unit configured as an access device 62 receives a control signal 40 from the external control device 64, the master unit configured as an access device 62 transmits an acknowledgement signal 42 to the external control device 64. This acknowledgement signal 42 may comprise information regarding if the control signal 40 from the external control device 64 is authenticated or not, if the if the control signal 40 from the external control device 64 is authenticated but do not have access to the control command relating to a slave unit 60 of the independent system 3 that the control signal 40 comprises, or the like.

[0101] If the control signal 40 from the external control unit 64 is accepted, the control command relating to the slave unit 60 of the independent system 3 is evaluated and a control command 44 corresponding to the control command of the control signal 40 from the external control unit 64 is forwarded to the slave unit 60 of the independent control system 3. When the slave unit 60 receives the control command 44, it generates and transmits an authentication request signal 46 to the master unit configured as an access device 62. The master unit configured as an access device 62 receives the authentication request signal 46 from the slave unit 60 and generates and transmits an authentication response signal 48 thereto. The authentication response signal 48 is received by the slave unit 60, and if the response signal 48

is verified by the slave unit 60, the control command 44 is processed. The authentication response signal 48 may comprise a code, an ID or the like which the slave unit 60 is able to verify.

[0102] In a preferred embodiment of the invention, at least parts of the authentication request signal 46 and the authentication response signal 48 are generated by means of the unique code key of the master unit configured as an access device 62 and the slave unit 60.

[0103] In an embodiment of the invention, the master unit configured as an access device 62 transmits a command status request signal 50 to the slave unit 60 after a predetermined time interval from transmittance of the control command 44. The slave unit 60 then transmits a command status signal 52, containing information regarding the status of the command 44, as respond to the command status request signal 50. This command status signal 52 is translated and forwarded by the master unit configured as an access device 60, by means of a command status signal 54 from the master unit 62 to the external control device 64.

[0104] In a further embodiment of the invention which is not illustrated in fig. 2, the external control device 64 may transmit a command status request signal to the master unit configured as an access device 60, e.g. after a predetermined time interval from the transmittance of the control signal 40. The master unit configured as an access device 60 then transmit the command status request signal from the external control device 64 to the slave unit 60, which responds to this signal, and the master unit configured as an access device 60 translates and forwards this respond signal to the external control device 64. By means of the above mentioned command status signals it is possible for a user operating the external control device to receive information regarding the present status of slave unit.

[0105] In an embodiment of the invention, a slave unit of the independent control system 3 can distinguish between critical and non-critical control commands of the command signal 44 from the master unit configured as an access device 62. A critical control command may be commands which may be critical to the safety such as opening a window, unlocking a door, opening a garage door or the like. A non-critical control command may be the controlling of shutters, blinds, light or the like. If a critical control command are received by the slave unit 60, the slave unit requests for authentication of the master unit (not illustrated in figure 2) or master units configured as an access device 62. If instead a non-critical control command is received, the at least one slave unit may in an embodiment of the invention be processed by the slave unit without authentication request of the master unit or master unit configured as an access device.

[0106] Fig. 3 illustrates an embodiment of a flowchart according to the invention wherein an access master unit beyond authenticating an external control device also evaluates a control command received from the external control device. In this embodiment, the access master unit of the independent control system 3 tests if a control signal is received from an external control device ECD. If a control signal is received, the access master unit in step S31 processes the received command signal to authenticate the external control unit which has transmitted the control signal. If the external control device is not authenticated, the control command is denied in step S32. However, if the access master unit authenticates the external control device, the master unit configured as an access device in step S33 initiates an evaluation of the control command of the received command signal. If the control command is not accepted by means of the evaluation, the control command is denied in step S34 even though the external control device is authenticated. However, if the control command is accepted by means of the evaluation, the control command is executed in step S35.

[0107] The evaluation of the control signal may in an embodiment of the invention comprise processing of a plurality of access security parameters ASP. Such access security parameters are associated with a slave unit, so that the slave unit defines a security level necessary to allow control of the slave unit.

[0108] Fig 4 illustrates an example of a group of access security parameters ASP defining an access security parameter hierarchy. A slave unit is associated with an access security parameter ASP defining a level of security needed to access/control the slave unit. The access security parameter(s) may be stored in the slave unit, for example in the form of a safety flag. Likewise, access security parameters of associated with slave units may be stored in the master unit configured as an access device preferably in the form of a table such as the access security parameter table 90 of fig. 4. In fig. 4, a first and fourth slave unit, Slave 1 and Slave 4 of the independent control system 3, is associated with ASP 1, a second slave unit Slave 2 is associated with ASP 3, a third slave unit Slave 3 is associated with ASP 2, a fifth slave unit Slave 5 is associated with ASP n and so on.

[0109] Access security parameter ASP 1 is an access security parameter demanding a high security level. For example that a slave unit associated with access security parameter ASP 1 can only be controlled by a master unit of the independent control unit, and every attempt to control the slave unit by means of an external control device is denied even though the external control device is authenticated by a master unit configured as an access device.

[0110] Access security parameter ASP 2 may be an access security parameter demanding a lower level of security than ASP1. For example, control of a slave unit of the independent control system 3 by an external control device ECD is accepted, but only in the case that the external control device which has transmitted the control signal is located near the individual control system 3. This may for example be achieved by demanding that the command signal has to have been transmitted to the master unit configured as an access device by means of communication means with a limited range, such as e.g. Bluetooth or zigbee, or by evaluating position data received from the external control unit ECD.

[0111] Access security parameter ASP 3 may be an access control level where the access security parameter is

dependent of a time parameter. Thereby a slave unit associated with access security parameter ASP 3 may only allow operation of the slave unit by an external control device during daytime.

[0112] Access security parameter ASP 4 may be an access control level allowing any authenticated external control device to operate the slave unit associated with a the access security parameter ASP n.

[0113] Access security parameter ASP n may be an access control level allowing any authenticated external control device to operate the slave unit associated with a the access security parameter ASP n.

[0114] In an embodiment of the invention, one or more access control parameters assigned to a slave unit may be altered dynamically over time. Furthermore; a slave unit may in an embodiment of the invention be assigned more than one access security parameter ASP.

[0115] Likewise, an access security parameter may in an embodiment of the invention change safety level over time, and in such a case, the master unit configured as an access device is preferably updated over time, at least if the status of the access security parameter is stored in the access master unit.

[0116] Furthermore, a hierarchy between external control devices ECD1-ECDn is present. Such hierarchy could e.g. be determined on the basis of the identification data of the individual external control device ECD1-ECDn, the present geographical placement of the external control device ECD1-ECDn, the type or types of communication means used by the external control device ECD1-ECDn, time and/or date or the like. Likewise, a master unit C1-Cn of the independent system 3 may be assigned a higher rank than the external control devices U1-Un so that users directly controlling the independent control system by means of a master unit C1-Cn may overrule commands transmitted by external control devices (ECD1-ECDn).

[0117] Fig. 5 illustrates an embodiment of the invention where a master unit configured as an access device (not illustrated in fig. 5) of the independent control system 3 comprises hierarchy management means for handling a hierarchy of an external control device ECD. Such hierarchy management means may e.g. be a hierarchy table 56 facilitating control of hierarchy settings relating to one or more external control devices ECD1-ECDn. An external control device ECD1-ECDn may thereby be assigned at least one of a plurality of hierarchy levels HILEV1- HILEVn by means of such hierarchy management means. The hierarchy management means may, as illustrated in fig. 5 where the hierarchy management means comprises a hierarchy table, further comprise a list of command types CMDTYP1- CMDTYPn of the independent control system 3. These command types CMDTYP1- CMDTYPn are the command types that are possible for a master unit(s) configured as access device(s) to transmit to the slave units of the independent control system 3. The hierarchy levels HILEV1 - HILEVn each define a list of command types CMDTYP1- CMDTYPn of the independent control system 3, that an external control device ECD can access in the independent control system 3 (not illustrated in fig. 5). As illustrated in fig. 5, the hierarchy level HILEV 1 gives access to all command types CMDTYP1- CMDTYPn of the independent control system 3, the hierarchy level HILEV2 gives access to the command types CMDTYP1, CMDTYP2 and CMDTYP3, the hierarchy level HILEV3 gives access to the command types CMDTYP2 and CMDTYP4 and so on. On the basis of the identification of the external control device(s) ECD, an access master unit hereby may control which command types CMDTYP1- CMDTYPn the external control device(s) is/are allowed to access, based on the hierarchy level HILEV1 - HILEVn assigned to an external access devices ECD. Alternatively, an external control device ECD1-ECDn transmits its assigned hierarchy level, together with an identification of the external control device and the control command. Furthermore, an external control device ECD1-ECDn may individually control which control commands it is able to transmit on the basis of a hierarchy table comprised in an external control device ECD.

[0118] In an embodiment of the invention, at least one of the HILEV1 - HILEVn only allow the external control system to access status data of slave units of the independent control system 3. Such status data may be room temperatures, rain sensor status, status of awnings, shutters, windows and the like.

[0119] The assignment of a hierarchy level HILEV1 - HILEVn to an external control device EDC may in an embodiment of the invention be determined by fixed hierarchy level assignments or dynamically shifting hierarchy level assignments, determined on the basis of e.g. geographical placement of an external control device ECD, user information of the user operating the at least one external control device ECD, time and/or date or the like.

[0120] By dynamically shifting hierarchy level assignments to external control devices ECD is understood that a hierarchy level assigned to an external control device may change over time. Examples of such dynamic shifting between hierarchy assignments could be that an external control device ECD changes hierarchy level when it is positioned with a certain distance from a master unit configured as an access device of the independent control system to which it is assigned. Another example of dynamic shifting between hierarchy assignments may be when a user of an external control device ECD is changing, e.g. by accessing the external control device ECD with a pin code, finger print, voice recognition or the like.

[0121] If dynamic shifting between hierarchy assignments is at least partly based on the geographical position of the at least one external control device ECD and/or the distance between the at least one master unit configured as an access device, it is preferred that the external control device ECD comprises positioning determination means such as e.g. GPS or the like. As an alternative the position of the at least one external control device ECD may be defined by the user, a telecommunication network, by evaluation of the communication means utilized for communication with an

access master unit or the like.

[0122] Fig. 6 illustrates an embodiment of the invention, where the external control device 74 is updated with the status of one or more slave units 70 of the independent control system 3 without transmitting control signals comprising control commands. The update may be performed continuously, periodically, by a user of an external control device 74 or the like. The external control device 74 transmits a slave status request signal 76 to a master unit configured as an access device 72. The external control device may transmit the slave status request signal 76 periodically, continuously, in response to user request or the like. The master unit configured as an access device 72 receives the slave status request signal 76, and transmits a status request signal 78 to one or more slave units 70 of the independent control system 3. In this embodiment the slave unit or slave units 70 transmits a status signal 80 in response to the status request signal 78, but the one or more slave units 70 may also request authentication of the master unit configured as an access device 72 as described earlier, before the transmission of the status signal 80. The master unit configured as an access device 72 then translates and transmits the received status of the slave unit or slave units 72, to the external control device 74.

[0123] In another embodiment which is not illustrated in fig. 6, access master unit 72 periodically transmits status request signals 78 to one or more slave units 70 of the independent control system 3, to get updated with the status of the one or more slave units 70. The status request signals 78 in this embodiment may be transmitted without receiving slave status request from external control devices 74. The master unit configured as an access device 72 is hereby continually updated with the status of the slave units 70 of the independent control system 3. In this embodiment, the master unit configured as an access device 72 may comprise means for storing data relating to the status of slave units of the independent control system 3. The slave status signals 82 from the master unit configured as an access device 72 is then transmitted continuously, periodically, as a response to a slave status request signal from an external control device 74 which may be generated automatically or by a user of the external control device 74 or any combination thereof to an external control device 74 which can hereby be updated with the status of one or more slave units 70 of the independent control system 3. In an embodiment of the invention, the external control device 74 and/or a master unit configured as an access device may be updated with the status of the slave units of the independent control system every time a slave unit changes value/status.

[0124] Furthermore, master units configured as access devices may continuously monitor status from other masters within the independent control system 3 to establish an up to date system status table of the system.

[0125] Fig. 7 illustrates an example of a preferred method of operating a controller configured to control the independent control system 3. According to this method, the master unit configured as an access device 72 registers the address being unique to the slave unit 70, e.g. by receiving the address from the slave unit 70. Furthermore, the master unit configured as an access device 72 and the slave unit comprise one and the same code key being unique to the independent control system 3. Likewise, the master unit configured, as an access device 72 may register other parameters such as hierarchy levels, access security parameters and/or the like. Furthermore, the slave unit 70 may receive and transmit other information from the master unit 72, e.g. to authenticate the said code key, to register information of the master unit 72, or the like.

[0126] Then, when the master unit configured as an access device 72 receives a control signal 40 from an external control device 74, the master unit configured as an access device 72 processes the received control signal 40 to establish an identification of the external control device 74 and to authenticate the external control device 74 which has transmitted the control signal 40. If the external control device 74 which has transmitted the control signal 40 is authenticated, the master unit configured as an access device 72 retrieves the address which is unique to the slave unit(s) 70 which is/are intended to be controlled by means of the control command of the control signal 40. This retrieving of the unique address of the slave unit(s) 70 may e.g. be performed by processing information of the control signal which may comprise information regarding to which slave unit(s) the control command of the control signal 40 is intended. The control signal 40 may for example (as mentioned earlier) comprise an alias for the slave unit(s) 70, to avoid that the unique address of the slave unit is transmitted between the external control device 74 and the master unit configured as an access device 72. Another way of retrieving the unique address may be that an external control device 74 may be allowed to operate only one slave unit 70, and identification and authentication of the external control device 74 may hereby facilitate automatic identification of the unique address of the slave unit to which the control command is intended without processing further information of the control signal 40. When the slave unit 70 is identified, the master unit configured as an access device 72 generates/establishes and transmits/communicates coded command(s) to the slave unit 70, based on the received control command(s) of the control signal 40 received from the external control device 74.

[0127] Furthermore, as illustrated in fig. 7 and as explained earlier, the master unit configured as an access device 72 may in an embodiment of the invention establish and communicate a feedback signal to the external control device, e.g. to inform the user of the external control device of the status of the control command of the control signal, transmitted to the independent control system 3.

[0128] It should be understood that the invention is not limited to the particular examples above, but may be designed and altered in a multitude of varieties within the scope of the invention as specified in the claims. Furthermore, it is understood that references in the description and claims should not be interpreted as limiting to the protection of the

present invention.

List:

5	[0129]	
	1	: Control system
	3	: Independent control system
10	2 (U1), 4 (U2), 6 (U3), 8 (Un) 60, 70:	: Slave unit
	10,12,14,16	: Driven or controlled members
15	18,20,22,24	: Antenna means for slave units
	26 (C1), 30 (C2), 34 (Cn), 62, 72	: Master units
	28, 32, 36	: Antenna means for master units
20	38	: Access control part
	40	: Control signal from external control device
25	42	: Acknowledgement signal from master unit configured as an access device to external control device
	44	: Control command to slave unit
30	46	: Authentication request signal
	48	: Authentication response signal
35	50	: Command status request signal from mas- ter unit to slave unit
	52	: Command status signal from slave unit to master unit
40	54	: Command status signal from master unit configured as an access device to external control device
45	56	: Hierarchy table
	64, 74, ECD, ECD1, ECD2, ECD3, ECDn	: External control devices
	76	: Slave status request signal
50	78	: status request signal from master unit to slave unit
	80	: status from slave unit to master unit
55	82	: Slave status signal from master unit con- figured as an access device to external con- trol device.

90 : Access security parameter table.

HILEV 1, HILEV 2, HILEV 3, HILEV 4, HILEV 5, HILEV n : Hierarchy levels

5 CMDTYP1, CMDTYP2, CMDTYP3, CMDTYP4, CMDTYP5, CMDTYPn : Command types.

Claims

- 10 **1.** Method of operating a controller configured to control an independent control system (3) comprising at least two units wherein at least one of said units is designed to operate as a master unit (26, 30, 34, 62, 72) and wherein at least one of said units is designed to operate as a slave unit (2, 4, 6, 8, 60, 70), where said at least one master unit (26, 30, 34, 62, 72) and said at least one slave unit (2, 4, 6, 8, 60, 70) comprise one and the same code key, said code key being unique to said independent control system (3), and where said at least one slave unit (2, 4, 6, 8, 60, 70) comprises an address being unique to said at least one slave unit (2, 4, 6, 8, 60, 70) and being registered by said at least one master unit (26, 30, 34, 62, 72), wherein at least one of said at least one master unit (26, 30, 34, 62, 72) further is configured as an access device, which can communicate with one or more external control units (64, 74, ECD, ECD1, ECD2, ECD3, ECDn), which are external to said independent control system (3),
- 15
- 20 - whereby said at least one slave unit (2, 4, 6, 8, 60, 70) is independently operateable by means of said at least one master unit and/or a master unit configured as an access device,
 - whereby said at least one slave unit (2, 4, 6, 8, 60, 70) is dependently operateable by at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) where said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) is operating said at least one slave unit (2, 4, 6, 8, 60, 70) via said at least one master unit configured as an access device,
- 25 - whereby an operation of said at least one slave unit (2, 4, 6, 8, 60, 70) comprises:
- receiving from at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) a control signal (40) by said at least one master unit configured as an access device where said control signal at least comprises a control command relating to at least one of said at least one slave units (2, 4, 6, 8, 60, 70) and identification of said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn),
- 30
- whereby, when said at least one master unit configured as an access device receives said control signal from said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn), said at least one master unit configured as an access device processes said received control signal from said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) to perform authentication of said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) and to identify said at least one slave unit (2, 4, 6, 8, 60, 70) in order to retrieve said address being unique to said at least one slave unit (2, 4, 6, 8, 60, 70), and
- 35 - whereby said at least one master unit configured as an access device transmits coded control signals (44) to said at least one slave unit (2, 4, 6, 8, 60, 70) on the basis of said control commands of said control signal from said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn), when said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) is authenticated by said at least one master unit configured as an access device.
- 40
- 45 **2.** Method according to claim 1, whereby an authentication request signal (46) to said at least one master unit configured as an access device is generated by said at least one slave unit (2, 4, 6, 8, 60, 70) in response to said coded control signals (44),
- whereby said at least one master unit configured as an access device generates and transmits a response signal (48) to said authentication request (46) from said at least one slave unit (2, 4, 6, 8, 60, 70), and
- 50 - whereby said at least one slave unit (2, 4, 6, 8, 60, 70) processes said coded control signals (44) if said response signal from said at least one master unit configured as an access device is verified by said at least one slave unit (2, 4, 6, 8, 60, 70).
- 55 **3.** Method according to any of the preceding claims, whereby communication in said independent control system (3) operates by means of communication means of a different type than at least one type of communication means of said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) utilized for communication between said master unit configured as an access device and said at least one external control device.

4. Method according to any of the preceding claims whereby communication to said at least one slave unit (2,4,6, 8, 60, 70) distinguish between critical and non-critical coded control signals from said at least one master unit (26, 30, 34, 62, 72) and/or master unit configured as an access device.
- 5 5. Method according to any of the preceding claims, wherein said processing comprises an evaluation of the control signal received from said external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) to determine if the control command of the control signal should be accepted.
- 10 6. Method according to any of the preceding claims, whereby communication to at least one of said at least one slave unit (2, 4, 6, 8, 60, 70) of the independent control system (3) is associated with at least one access security parameter (ASP).
- 15 7. Method according to claim 6, whereby said at least one access security parameter (ASP) is selected from a group of access security parameters (ASP1-ASPn) comprising at least two access security parameters.
- 20 8. Method according to claim 6 or 7, whereby said at least one access security parameter is dependent of a time parameter.
- 25 9. Method according to claim 6, 7 or 8, whereby said at least one access security parameter (ASP) is associated with demands to the geographical location of one or more of said external control devices (64, 74, ECD, ECD1, ECD2, ECD3, ECDn).
- 30 10. Method according to any of claim 5-9, whereby at least one of said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) is assigned at least one hierarchy level (HILEV 1, HILEV 2, HILEV 3, HILEV 4, HILEV 5, HILEV n) selected from a plurality of hierarchy levels.
- 35 11. Method according to claim 10, whereby said control signals from the at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) is evaluated by said at least one master unit configured as an access device on the basis of said at least one hierarchy level assigned to said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn).
- 40 12. Method according to any of claims 5-11, whereby said control signals from said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) are evaluated on the basis of geographical placement of said at least one external control device (64,74, ECD, ECD1, ECD2, ECD3, ECDn), user information of the user operating said at least one external control device (64, ECD, ECD1, ECD2, ECD3, ECDn), time and/or date, distance between the said at least one master unit configured as an access device and said at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn), and/or the utilized type of communication means.
- 45 13. Method according to any of the preceding claims, whereby said master unit configured as an access device imposes a safety limit to a control command of the said received control signal.
- 50 14. Method according to any of the preceding claims, whereby the at least one external control device (64, 74, ECD, ECD1, ECD2, ECD3, ECDn) accesses aliases to the at least one slave unit (2, 4, 6, 8, 60, 70) of the independent control system (3).
- 55 15. Method according to any of claims 10-12, whereby at least one hierarchy level (HILEV 1, HILEV 2, HILEV 3, HILEV 4, HILEV 5, HILEV n) is selected based on the type of the communication link used.

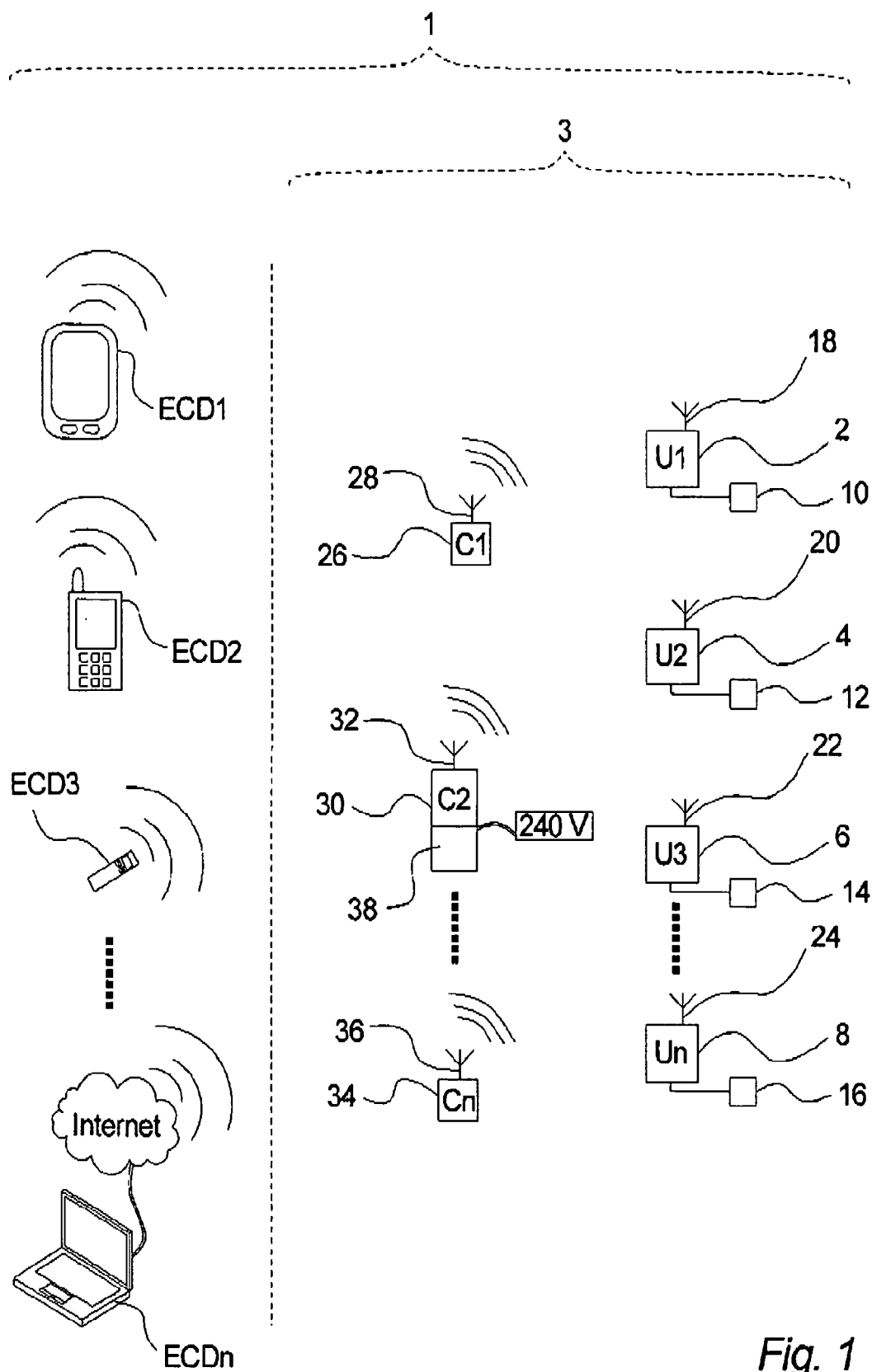


Fig. 1

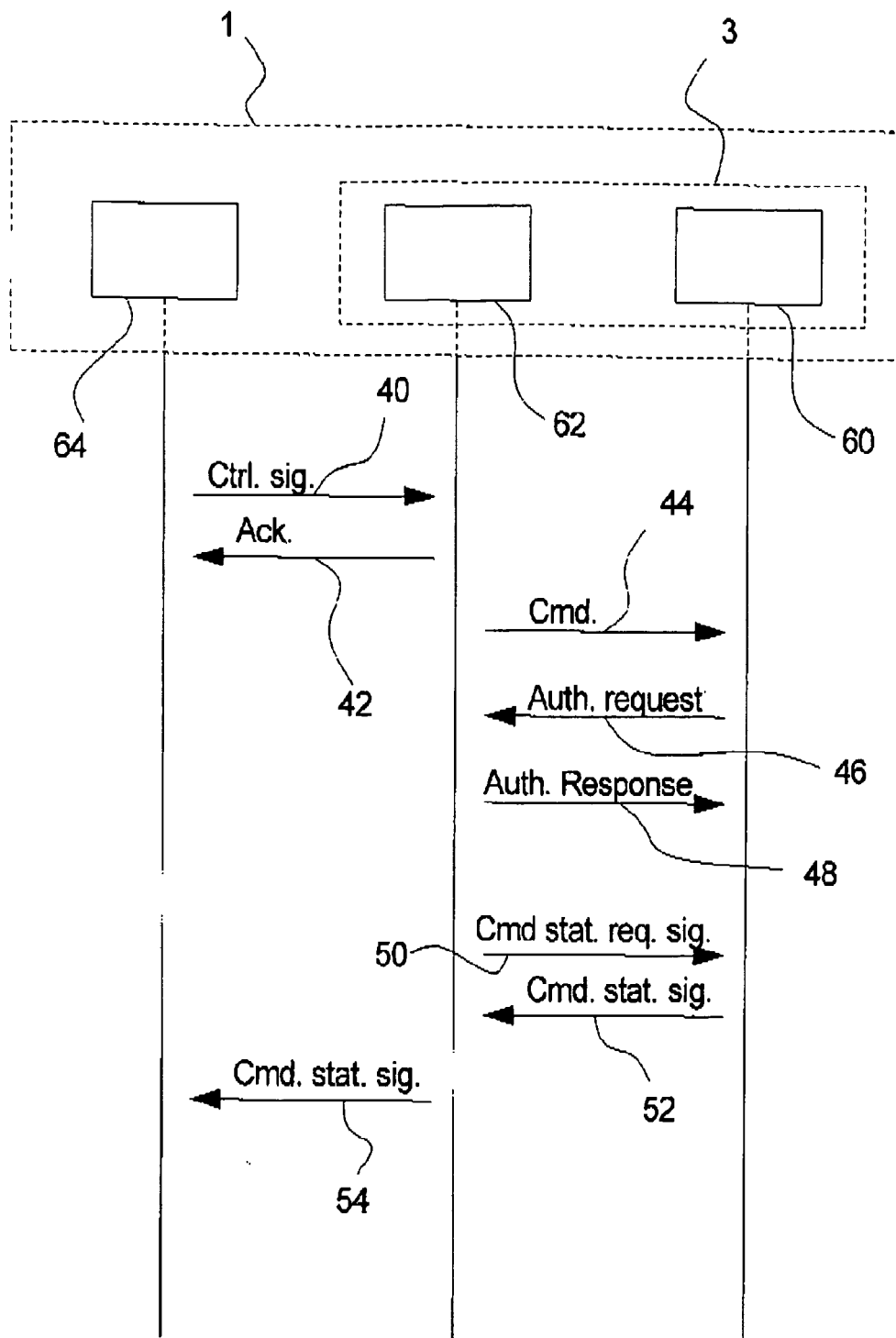


Fig. 2

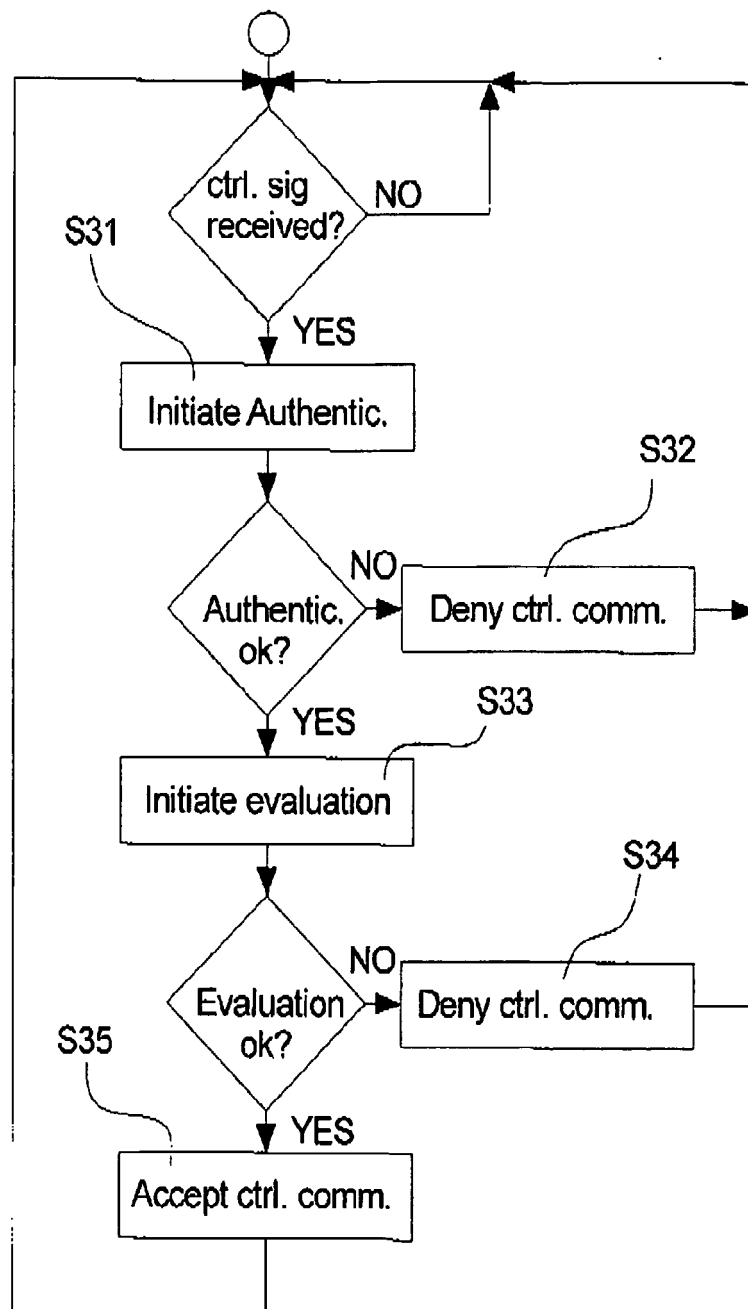
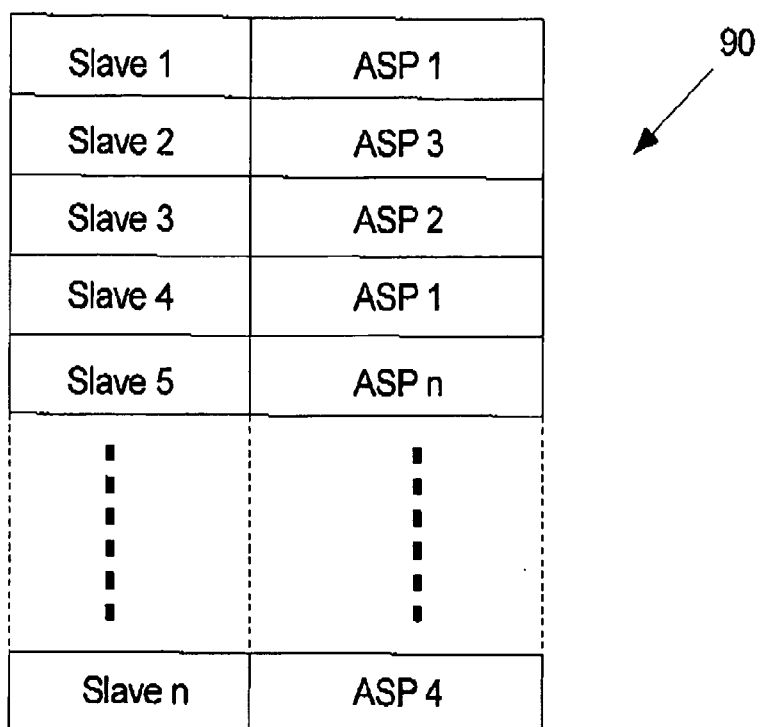


Fig. 3

Slave 1	ASP 1
Slave 2	ASP 3
Slave 3	ASP 2
Slave 4	ASP 1
Slave 5	ASP n
⋮	⋮
Slave n	ASP 4

*Fig. 4*

	HILEV1	HILEV2	HILEV3	...	HILEVn
CMDTYP1	X	X			
CMDTYP2	X	X	X		
CMDTYP3	X	X			X
CMDTYP4	X		X		
CMDTYP5	X				
...	...	...	...		...
CMDTYPn	X				

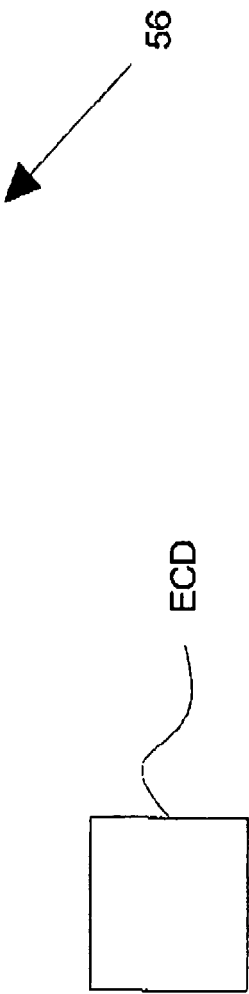


Fig. 5

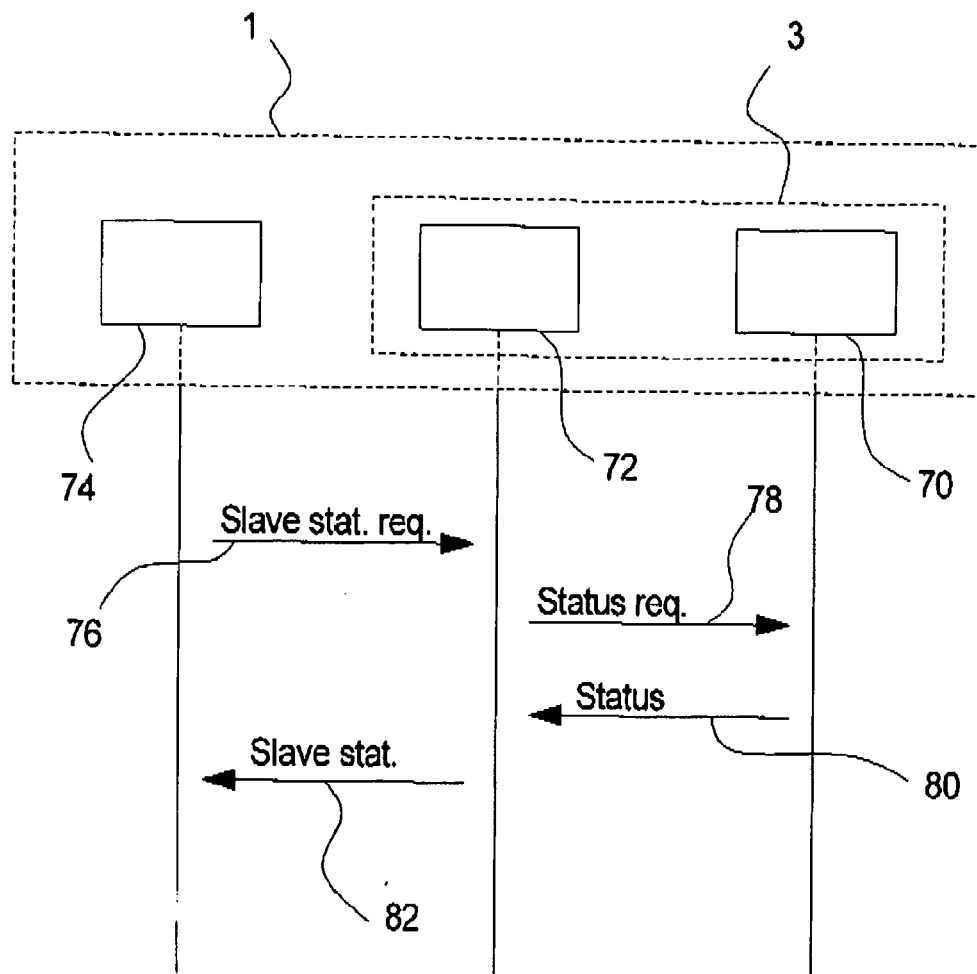


Fig. 6

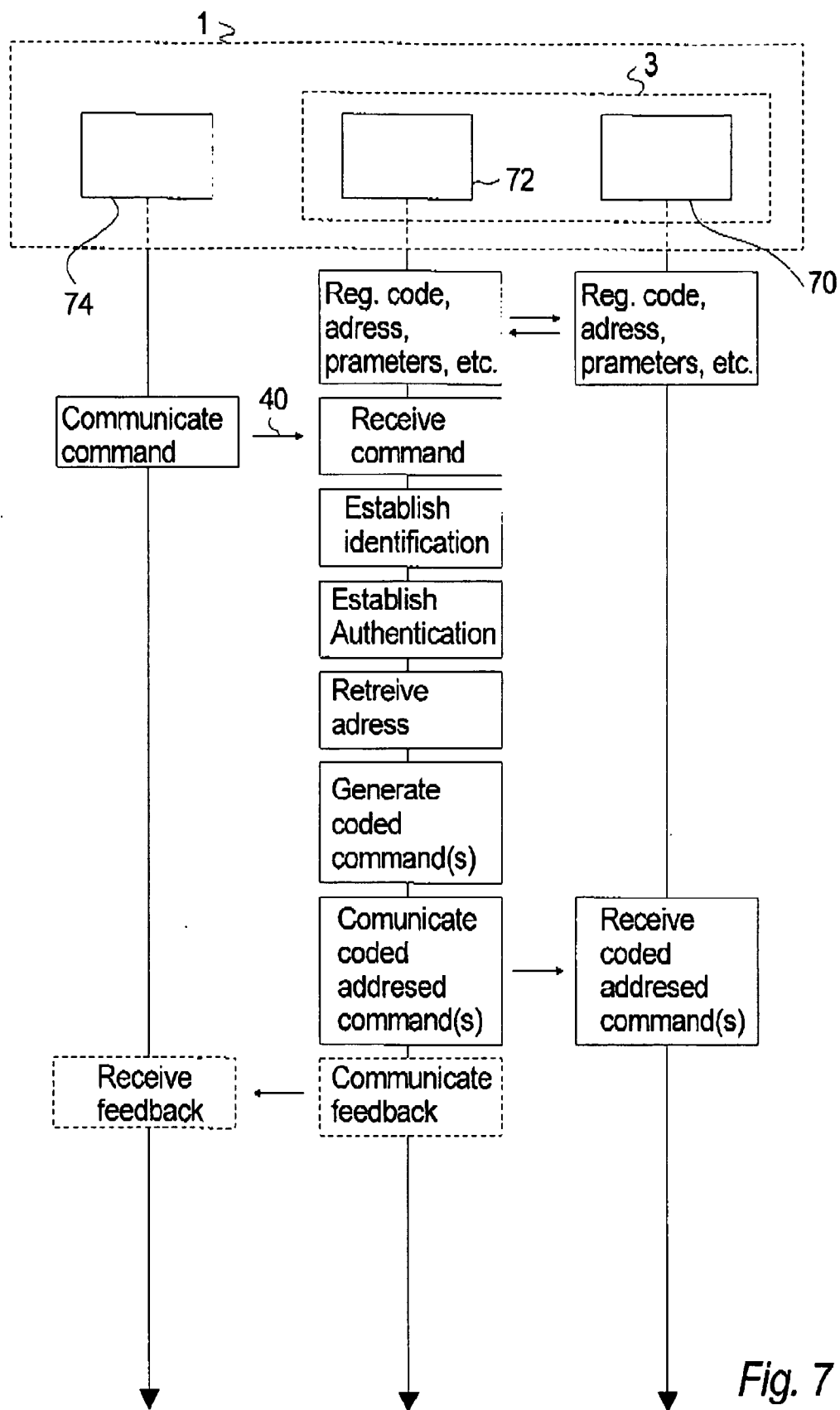


Fig. 7

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

- WO 03028300 A1 [0003]