Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2648482 A1 2007/11/15

(21) 2 648 482

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/04/27
(87) Date publication PCT/PCT Publication Date: 2007/11/15
(85) Entrée phase nationale/National Entry: 2008/10/06
(86) N° demande PCT/PCT Application No.: CA 2007/000727
(87) N° publication PCT/PCT Publication No.: 2007/128102
(30) Priorités/Priorities: 2006/05/04 (US11/381,675);
2006/09/25 (CA PCT/CA2006/001578);
2007/01/11 (US60/884,536)

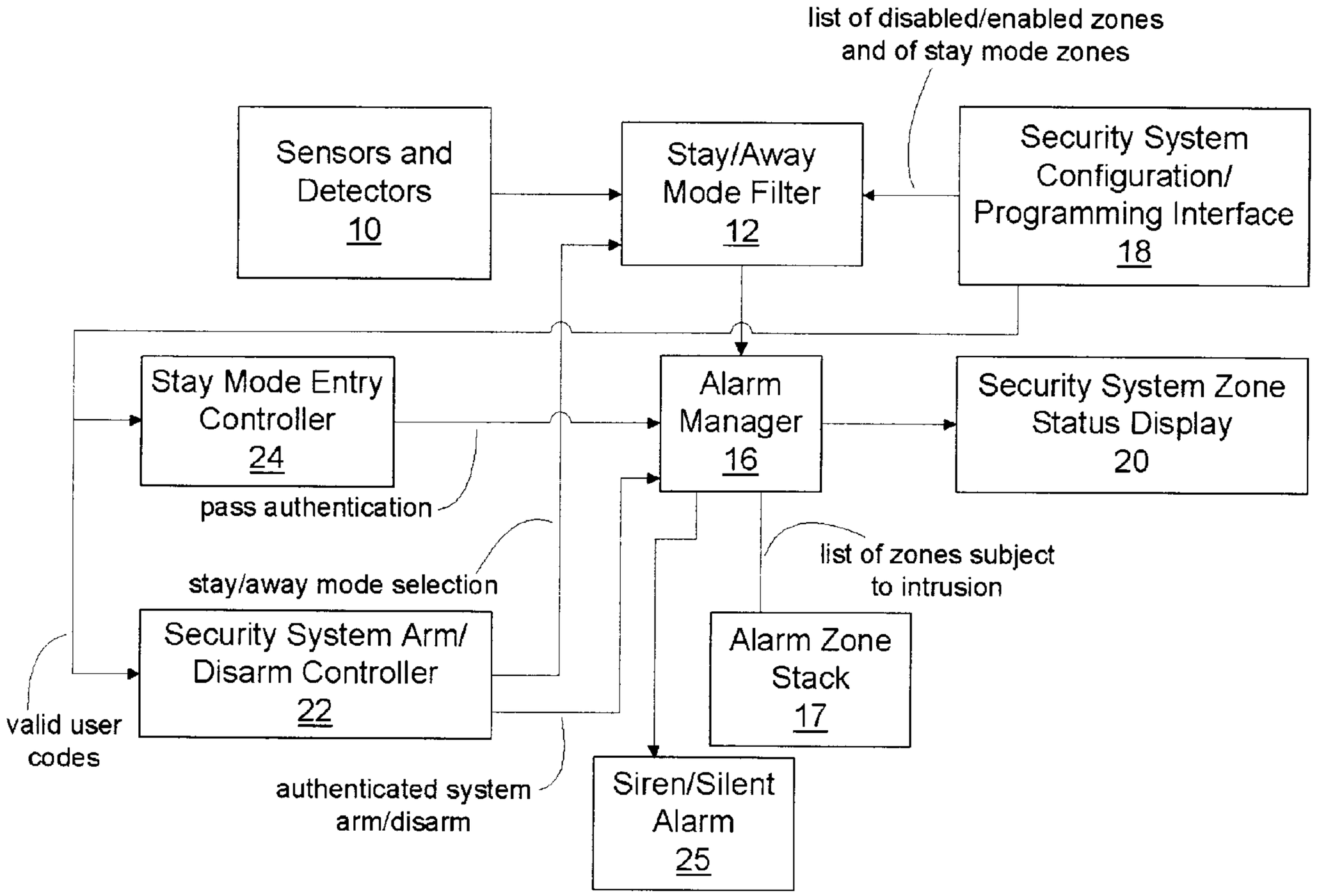
(51) Cl.Int./Int.Cl. *G08B 13/00* (2006.01)

(71) Demandeur/Applicant:
HERSHKOVITZ, SHMUEL, BS

(72) Inventeur/Inventor:
HERSHKOVITZ, SHMUEL, BS

(74) Agent: ANGLEHART, JAMES

(54) Titre : COMMANDE D'ENTREE A SYSTEME DE SECURITE
(54) Title: SECURITY SYSTEM ENTRY CONTROL



(57) Abrégé/Abstract:
A security system is operable in a stay mode in which protected premises perimeter sensors or detectors are armed wherein a delay is provided between detection of breach of the perimeter and generating an alarm. The security system is able to authenticate a user during the delay and to restore the stay mode without generating the alarm and without disarming the protected premises perimeter sensors or detectors.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2007 (15.11.2007)

PCT

(10) International Publication Number
WO 2007/128102 A1

(51) International Patent Classification:
G08B 13/00 (2006.01)

(21) International Application Number:
PCT/CA2007/000727

(22) International Filing Date: 27 April 2007 (27.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/381,675 4 May 2006 (04.05.2006) US
PCT/CA2006/001578 25 September 2006 (25.09.2006) CA
60/884,536 11 January 2007 (11.01.2007) US

(71) Applicant and
(72) Inventor: **HERSHKOVITZ, Shmuel** [CA/BS]; 53 Fortune Bay Inlet, Freeport (BS).

(74) Agent: **BERESKIN & PARR**; Suite 4000, 40th Floor, 40 King Street West, Toronto, Ontario M5H 3Y2 (CA).

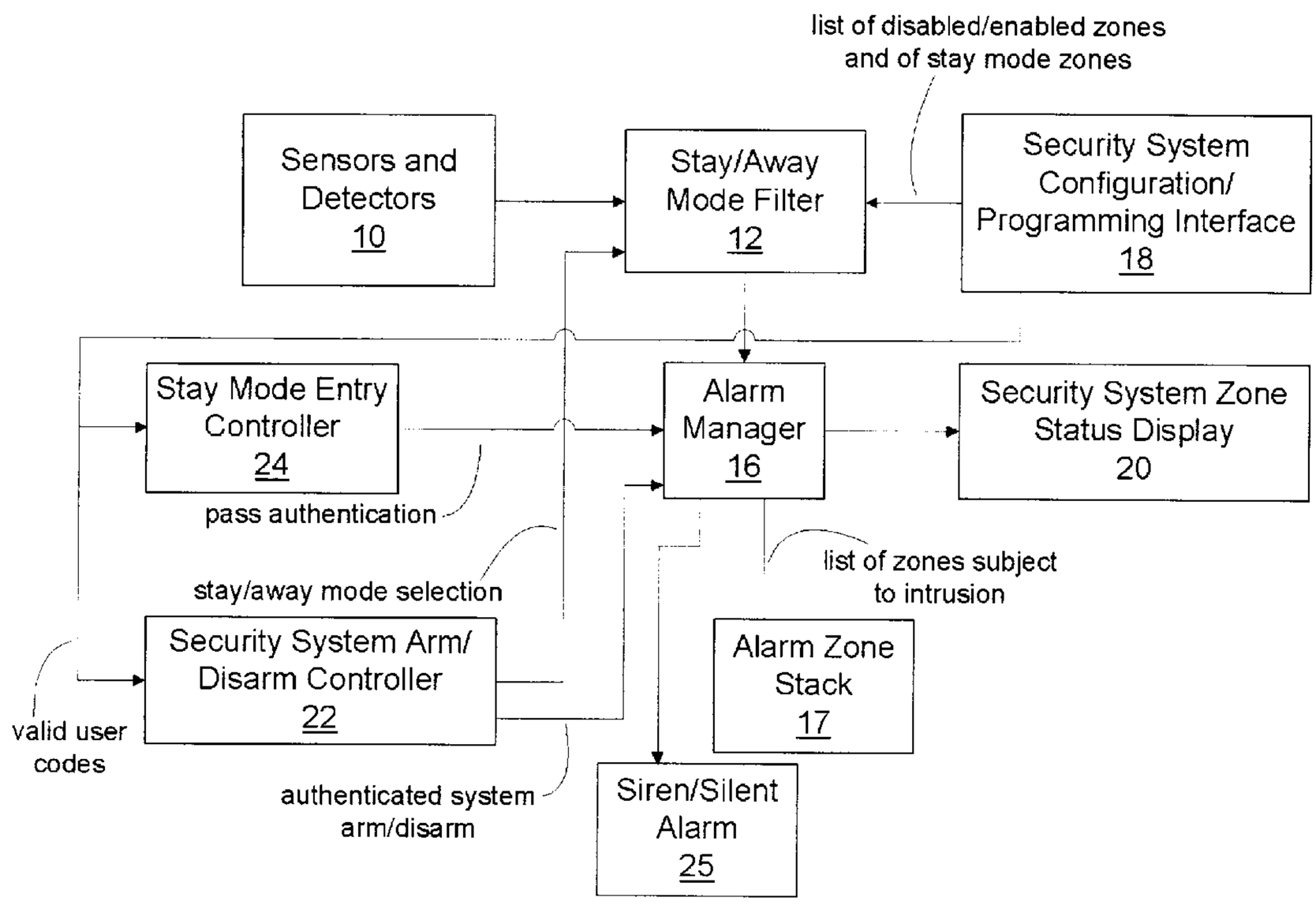
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,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

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

Published:
— *with international search report*

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

(54) Title: SECURITY SYSTEM ENTRY CONTROL



(57) Abstract: A security system is operable in a stay mode in which protected premises perimeter sensors or detectors are armed wherein a delay is provided between detection of breach of the perimeter and generating an alarm. The security system is able to authenticate a user during the delay and to restore the stay mode without generating the alarm and without disarming the protected premises perimeter sensors or detectors.

Security System Entry Control

Field of the invention

The present invention relates to intrusion security systems and more particularly to arming and disarming control of such security systems.

Background of the invention

A conventional security system integrates a number of sensors or detectors for detecting an intrusion within protected premises, such as a home or place of business, with a control system for interpreting the sensor or detectors signals for the purposes of generating an alarm. The control system for small security systems typically has a single control panel and a single keypad. The control panel is connected by wire or wirelessly to all sensors or detectors, and has control over alarm generation whether by local siren or by telecommunications, such as telephone network or cable network. The control panel is also connected to the keypad that serves as the user interface within the protected premises for arming and disarming the security system, and for programming or configuring the security system.

Most security systems today allow for the user to enter a code at the keypad to arm the security system, and either the same or a different code to disarm the security system. The keypad is safely located within the protected premises, and for those detectors that would detect an entry or exit, there is a timer used to delay the action of alarm generation from the time that a sensor or a detector generates an intrusion signal. This timer may be set to about 15 to 60 seconds, and allows for entry and exit by a user.

In many systems, the keypad can also be used for programming or setting features, such as which sensors or detectors, identified as zones within the protected premises, are to be activated or

deactivated. This is done commonly by using the keypad, and in many systems, the user enters a special security code at the keypad to enter a programming or setting mode.

Another common feature that can be programmed or set using the keypad is the stay mode. Stay mode is an armed mode where the premises are protected from intrusion while occupants remain within the premises. In this mode of operation, the detection of sensors and detectors within the protected premises is ignored, such as passive infrared motion detectors, Doppler shift microwave intrusion detectors, inside passage door sensors and floor load cell sensors. Only sensors and detectors that essentially monitor entry or egress remain activated. The stay mode is configured typically by entering the programming mode and selecting zones to be deactivated in the stay mode. The stay mode is turned on and off (namely to be in the away mode) by entering a security code and selecting the stay or away mode. The stay mode protects the perimeter of the premises and is very important in areas where there is a threat of intrusion while an occupant remains within the premises. When the occupant of the premises protected in a stay mode decides to leave, the system is disarmed and then re-armed in an away mode, in which sensors and detectors within the protected premises are active.

Such conventional security systems are vulnerable to intruders who are able to monitor the premises from outside and enter the premises at the moment when an occupant leaves or enters and other occupants remain within the premises with the security system armed in the stay mode. The timer used to allow exit or entry causes one or more zones of the security system to be by-passed during the timed period, and this may allow not only the occupant to leave or enter without generating an alarm but also the intruder. Once within the premises, the stay mode will allow the intruder to move about without generating an alarm. Because an occupant may be able to call 911 or use a panic button of the security

system to generate an alarm, such intruders are likely to use violence to subdue any occupants remaining within the premises. While an alarm may later be generated after the intruder leaves the premises, this is often a minor concern to the intruder and the alarm is simply too late. When a user enters premises protected by a conventional system, there is an entry delay, and the user punches his or her code or else an alarm will be generated when the delay expires. When the code is entered, the system is fully disarmed. At this moment, and until the system is re-armed into the stay mode all premises are unprotected. This involves a two-step process, namely the entering of a code to disarm the system, and then subsequently a code to re-arm the system. This delay to enter two subsequent codes can be sufficient time for an intruder to take advantage of the full disarming of the system. An intruder that learns occupant habits can wait till someone leave or enter the premises, and during the entry / exit operation can enter the premises via any zone.

Summary of the invention

According to a first aspect of the present invention, there is provided a security system that allows users to enter and/or exit secured premises without compromising the security of the rest of the system.

According to a second aspect of the present invention, there is provided a security system that when armed in an away mode immediately switches in a single action to an armed stay mode (without first being temporarily disarmed) when a user enters the premises and enters a code.

According to a third aspect of the present invention, there is provided a security system that includes a keypad for security code entry by users in which code entry specifies the action of the code including arm or disarm and at least one of entry and exit. For entry, authentication of the person entering is important, while for exit, authentication may be

achieved in some embodiments merely by pressing a key on a keypad without relying on the use of passcodes.

According to a fourth aspect of the present invention, there is provided a security system in which a satellite keypad is used for code entry near a point of protected premises entry or exit to enter an entry or exit code. Such a keypad can be used to authenticate an exit by merely pressing a button on the keypad because the keypad is located within the secured unarmed premises and the primary exit path associated with the keypad is not ambiguous.

According to a fifth aspect of the present invention, there is provided a security system that is to be used by at least some users at all times in the stay mode and such users only have codes to allow for entry and exit while other users have codes for arming and disarming the security system in addition to entry and exit.

According to a sixth aspect of the present invention, there is provided a security system having more than one stay mode configuration with the ability to select a desired one of the stay mode configurations. Such configurations may be organized as a function of different levels of security, and optionally with the level of security being displayed at a user interface. One example of such different configurations is a nighttime stay mode in which sleeping quarter zones are not armed, while daytime quarter zones are armed, and a daytime stay mode in which all interior zones are not armed. In general, stay mode configurations are determined by occupant usage of the premises, namely unused quarters are armed and used quarters are unarmed, while the interior-exterior perimeter remains armed. A sliding glass door leading onto a closed deck may be unarmed in a stay mode when outdoor areas are considered within protected premises. Other doors and windows may be armed.

In the case that the user interface (e.g. keypad) is located within an armed interior zone, a satellite keypad within the unarmed area

may be used to switch between stay mode configurations before an occupant enters an interior armed zone, or pass authentication may be done immediately following entry into the armed interior zone.

According to a seventh aspect of the present invention, there is provided a security system in which detector zones are classified as "with entry and/or exit delay" or as "immediate alarm", the latter class either requiring a user to provide a specific disarm authentication or immediately generating an alarm without allowing for the user to stop the alarm generation. The specific disarm authentication may optionally be available to a reduced number of users or occupants, while authentication for entry or exit via zones specifically identified for this purpose is made available for all authorized users or occupants. To avoid false alarms, it may be desirable to combine physical security, such as key locks or deadbolts, to prevent occupants or users (particularly those users or occupants not authorized to provide the specific disarm authentication) from inadvertently using doors classified as "immediate alarm".

Optionally, the security system may be programmed with different classification configurations of the zones with the ability to select a desired one of the classification configurations. The classification configuration may be combined with the stay mode configuration, in accordance with the sixth aspect of the present invention. This also allows for the option of organizing configurations according to security level.

According to an eighth aspect of the invention, a security system is operative to use a wireless transmitter to authorize an entry or exit. The transmitter may be used as a substitute for manual code entry, or as a first step in authentication, namely to enable the function of entry or exit with a delay (and thus without generating an immediate alarm), while still requiring the user to enter a code or otherwise provide authentication. In the case that the security system is configured to allow entry or exit using different paths through protected premises and the wireless

transmitter has a range to be detected when entry or exit is possible via different paths, the invention provides the ability to determine a path for entry or exit following wireless transmitter authorization by detecting a path-distinguishing zone within the security system.

According to a ninth aspect of the invention, a security system is operative to by-pass a zone and automatically re-arm the zone when it is detected that the by-pass is no longer required. For example, the by-pass of a zone representing a window sensor may be authenticated using a keypad, and the by-pass is automatically removed when the window is closed again. This makes the use of a by-pass more secure and more convenient since the removal of the by-pass does not require use of the keypad. The removal of the by-pass can be instant or after a short delay of a few seconds, the latter providing a "debounce" function.

Brief description of the drawings

The invention will be better understood by way of the following detailed description with reference to the appended drawings, which:

Figure 1 is a flow chart illustrating the sequence of operational steps of a security system in a stay mode according to one embodiment of the invention;

Figure 2 is a schematic block diagram of a security system having a entry authorization controller generating a pass signal for canceling an intrusion event;

Figure 3 is a schematic block diagram of a security system having a entry authorization controller generating a zone specific pass signal for canceling an intrusion event for a specific zone;

Figure 4 is a schematic block diagram of a security system having a entry authorization controller cooperating with an arm/disarm

authentication controller to generate a pass signal for canceling an intrusion event;

Figure 5a is a schematic representation of the content of an intrusion event stack corresponding to the embodiment of Figure 2 for two entries into the protected premises with a single authenticated pass;

Figure 5b is a schematic representation of the content of an intrusion event stack corresponding to the embodiment of Figure 3 for one authorized exit and one intrusion entry into the protected premises with a single authenticated zone specific pass;

Figure 5c is a schematic representation of the content of an intrusion event stack corresponding to the embodiment of Figure 3 for two entries into the protected premises with a single authenticated zone specific pass; and

Figure 6 is a hardware block diagram of one possible implementation of the invention.

Detailed Description of the Invention

With reference to Figure 1, the operation of a security system is schematically summarized in which steps 30 through 40 are found in conventional systems, while steps 50 and up are new. A security system is armed in the single "stay mode" at step 30, and as long as no intrusion is detected (step 32) among the stay mode active sensors and detectors no action is taken.

In accordance with one embodiment of the invention, the arming in the stay mode involves selecting one of a number of stay modes with different levels of security. These different "stay modes" may correspond to different partitions of the secured premises in addition to different levels of security. Once intrusion is detected, an exit or entry

delay countdown is started at step 33. This is followed by indicating the zone of the intrusion on the security system user interface at step 34.

Optionally according to some embodiments of the invention, zones may be classified "entry/exit delay" and "immediate". If the intrusion detected in step 32 is in a zone that is "immediate", the system may immediate jump to step 37 or it may operate with delay without offering the option of normal pass authentication. This may be done by following conventional operation requiring the user to enter a system disarm code (step 35) that in accordance with the present invention may not be available to all users or occupants, or by following the embodiment of Figure 1 with step 50, but with a special authentication. If the zone is classified as "entry/exit delay", then the process is as per Figure 1.

In the conventional mode of operation, only two options are available to the user: do nothing, and the security system will proceed to generate an alarm once the delay has lapsed (steps 36 and 37); and disarm the system before the delay lapses (steps 35 and 38). Once the system is disarmed at step 38, the user is required to rearm the system at step 39 in order to be reprotected. However, the security system applies the normal exit delay at step 40 before beginning the normal stay mode armed state at 30.

In the embodiment of Figure 1, the user has an additional option of authenticating a pass (step 50), namely to authorize the entry or exit from the secured premises, before the delay lapses. Authenticating a pass at step 50 may involve entering a special code at a keypad or any equivalent means of authenticating an occupant of the secured premises. When using pass authentication, the security system remains armed and active for all other zones. For the zone that was used for the entry or exit, the system will detect that the zone is "open", namely that intrusion is detected, and that it is later "closed", namely that the intrusion detection ceases. The system will make sure that the intrusion detection ceases at

step 51, for example the door sensor detects that the door is closed following entry or exit. A delay may be provided as a maximum time that a door may remain open before an alarm is generated. When a door is shut, the door zone may be immediately re-armed (or re-armed after a short "debounce" delay of a few seconds to make sure that the door has been properly and permanently shut) or, particularly in the case of exit, it may remain unarmed for the duration of an exit delay. Then the display of the zone on the security system interface as being subject to intrusion is reset at step 52, and the Entry/Exit Delay is reset at step 53. The security system then returns to the normal armed stay mode at step 30.

Figures 2 to 4 schematically illustrate a security system according to a first embodiment. Such schematic illustration is for the purposes of understanding the invention, without necessarily following an actual implementation that may involve dedicated logic circuitry, programmed circuitry, a programmed microcontroller, a programmed computer, or any combination thereof. In one embodiment, the security system comprises the elements illustrated in Figure 6, namely a microcontroller 60 programmed with suitable program code that when executed performs the functions illustrated in Figure 1, a power supply 61 with battery back-up and AC/DC converter, a clock signal source oscillator 62, and non-volatile memory 63. A security system keypad/display unit 64 is connected to the microcontroller 60 via a serial bus 65.

In Figures 2, 3 and 4, security sensors and detectors 10 of the secured premises are connected by secure connection (wired, optical or wireless) to an alarm manager 16 through a stay/away mode filter 12. Zone inputs can be analog signals generated by intrusion detectors connected to ADC pins of microcontroller 60, and a software module running on processor 60 can interpret the analog states and maintain a register or memory store for each zone with corresponding detector states for interpretation by filter 12. Zone inputs can also be from bus 65, or a

wireless interface module that comprises wireless hardware circuitry 66 and a corresponding wireless interface software module running on processor 60. Filter 12 is configured using a programming interface 18 to indicate to filter 12 the list of enabled and disabled zones as well as the stay mode zones. Filter 12 is essentially a software module on processor 60.

Zones can be identified typically as being immediate alarm or with a timer or countdown before generating an alarm, active or enabled, disabled or by-passed, in a follow mode where the zone is by-passed as a function of detection by another zone and otherwise active. Follow mode is used for zones next to doors, for example. In this way, the manager 16 only considers intrusion events coming from enabled armed zones in the selected mode of away or stay. When an intrusion event occurs, manager 16 causes the status display 20 to show the event. Alarm manager 16 is essentially a software module running on processor 60.

Programming interface 18 uses keypad and display 64 to first authenticate a master user and allow such master user to configure the system including defining the valid user codes. The programming interface is essentially a software module running on processor 60 operating in conjunction with keypad/display 64. When the alarm manager 16 receives an intrusion signal from a sensor or detector 10 through filter 12, it enters the event in memory 17 (provided within processor 60) that may be arranged as a stack or circular buffer, and begins a timer countdown before an alarm is generated using unit 25. The siren output is done using driver circuit 25a connected to an output pin of processor 60, while the silent alarm is done using telephone dialer circuit 25b and a modem software module running on processor 60.

In some embodiments, the entry authorization controller 24 involves the use of a wireless transmitter to authenticate a pass. The transmitter may be a portable, battery-powered transceiver carried on a

keychain or the like. It may be used as a substitute for manual code entry, or as a first step in authentication, namely to enable the function of entry or exit with a delay (and thus without generating an immediate alarm), while still requiring the user to enter a code or otherwise provide authentication. The security system includes a wireless receiver that detects the code transmitted by the user's transmitter. When using a transmitter to enable entry, the perimeter can remain armed and be operative to generate an instant alarm when the perimeter is breached. Use of the transmitter allows for entry to take place without an instant alarm. Whether further authentication using code entry is required or not can be a programming choice by the user, as a function of the level of security desired. The user transceiver can also have a display of the system state, such as solid green for disarmed, flashing green for pass authentication in stay mode, flashing red for alarm, solid red for fully armed or away mode, and solid yellow for armed in stay mode. In some embodiments, the wireless transmitter can serve a dual function, namely to activate the pass authentication and to actuate a gate or garage door opener.

In the case that the security system is configured to allow entry or exit using different paths through protected premises and the wireless transmitter has a range to be detected when entry or exit is possible via different paths, the invention provides the ability to determine a path for entry or exit following wireless transmitter authorization by detecting a path-distinguishing zone within the security system. A path is a collection of zones operating with an entry or exit delay that would involve detection as a person enters or exits the premises. By determining which path is to be used for an entry or exit, other paths can be left armed in an instant mode.

In some embodiments, the interface 18 may be used to program more than one stay mode configuration. Such configurations may

be organized as a function of different levels of security. Display 20 may display the selected level of security. One example of such different configurations is a nighttime stay mode in which sleeping quarter zones are not armed, while daytime quarter zones are armed, and a daytime stay mode in which all interior zones are not armed. In general, stay mode configurations are determined by occupant usage of the premises, namely unused quarters are armed and used quarters are unarmed, while the interior-exterior perimeter remains armed. A sliding glass door leading onto a closed deck may be unarmed in a stay mode when outdoor areas are considered within protected premises. Other doors and windows may be armed.

In the case that the user interface (e.g. keypad) 64 is located within an armed interior zone, a satellite keypad associated with controller 22 and/or controller 24 can be provided within the unarmed area for switching between stay mode configurations before an occupant enters an interior armed zone, or pass authentication may be done immediately following entry into the armed interior zone. The arm/disarm controller 22 and likewise the entry authorization controller 24 are provided by using keypad/display unit 64 in conjunction with corresponding software modules running on processor 60. Security codes established using interface 18 are stored in non-volatile memory 63.

In other embodiments, the programming interface 18 is used to classify zones as "with entry and/or exit delay" or as "immediate alarm", the latter class either requiring a user to provide a specific disarm authentication or immediately generating an alarm without allowing for the user to stop the alarm generation. In this case, the interface 18 communicates this configuration to alarm manager 16, preferably via stay mode filter 12. When the stay mode filter signals to alarm manager 16 that an armed zone has detected intrusion, the alarm manager 16 determines whether the zone is "with delay" or "immediate". If the zone is "with delay",

then pass authentication may be used as in the embodiment of Figures 2 or 3. If the zone is classified as "immediate", then the system may be configured either to generate an immediate alarm, namely manager 16 signals alarm 25 immediately, or else, a delay is implemented with alarm generation being avoided either by system disarm or by special pass authentication. The specific disarm authentication is preferably available to a reduced number of users or occupants, while authentication for entry or exit via zones specifically identified for this purpose is made available for all authorized users or occupants.

It will be appreciated that the programming interface 18 can be used in some embodiments to define in each stay mode configuration which zones may be used by which users for entry and/or exit.

Separate lists may handle entry and exit, since it may be acceptable for a user to authenticate an exit through a door, while the same door would not be secure for entry. For example, it may be acceptable to authenticate a user from within the premises to exit through a door leading into a back alley, while no user should be allowed to enter through such back alley due to a higher risk of an intruder entering with the user by force.

Likewise, some users may be authorized to enter or to exit via certain zones, while others are not. Pass authentication can identify individual users or a level of user (group of users) so that more precise management of entry and exit of users can be provided. Logging of user entry and exit can be done efficiently when authentication is unique to each user. In the case that some users, such as employees or children, are not authorized to arm or disarm the system, but instead merely to use pass authorization, then greater security can be provided.

To avoid false alarms, physical security, such as key locks or deadbolts, is combined with the electronic security system to prevent occupants or users (particularly those users or occupants not authorized

to provide the specific disarm authentication) from inadvertently using doors classified as "immediate alarm".

Optionally, the security system may be programmed with different classification configurations of the zones with the ability to select a desired one of the classification configurations. The classification configuration may be combined with the stay mode configuration and communicated to alarm manager 16 via the stay mode filter 12. This also allows for the option of organizing configurations according to security level that can be displayed on display 20.

In Figure 2, an arm/disarm controller 22 is included for authenticating a user and then either arming the security system or disarming the security system by signaling the alarm manager 16 accordingly. A entry authorization controller 24 is also provided for authenticating a user and issuing a pass. The valid user codes used by the two controllers 22 and 24 may be the same or different, and may be user specific or not. The alarm manager 16 responds to the pass signal by removing or otherwise ignoring one intrusion event in memory 17. If only one event was recorded, a single pass will cause the alarm manager to continue to operate in the armed stay mode, and the display 20 will indicate no intrusion events. If two or more events were recorded, a single pass will cause the alarm manager merely to remove or ignore the first received event, and the display will show the remaining events (namely the zones where intrusion was detected). The user would need to use the entry authorization controller 24 repeatedly to generate additional pass signals to remove all events to prevent an alarm from being generated. However, in conventional configurations, two events generated during exit or entry would be an indication of foul play.

In Figure 3, the operation is similar to Figure 2 except that the controller 24 generates a pass signal that identifies the zone through which the pass is to be authorized, and manager 16 removes or ignores

the event corresponding to the identified zone only. This allows for a clear identification on display 20 of the exact zones where an unauthorized event was detected after the user authenticates the zone specific pass.

Zone identification in the pass signal can be done by using a keypad that is related to the specific entry/exit zone. A satellite keypad can be located near an entrance/exit for this purpose. Such a co-located keypad can be set to identify the local entrance/exit by default, while still be used with an additional key press for authenticating an exit or entry via a different door.

As an alternative to the embodiment of Figure 2, the stay mode controller 24 functionality, as shown in Figure 4, may be provided by cooperating with controller 22 for the purposes of authenticating the user, while for example allowing the user to press a key on a keypad to issue a pass authentication instead of a disarm or arm signal command. As an example, the user may enter the secured premises, thus creating an intrusion event. At the user interface keypad, the user enters the normal code for disarming the system. The controller 22 however sends this signal to controller 24 for processing. Controller 24 causes an indicator on the interface keypad to flash or otherwise to indicate that the system will disarm very shortly, say in 3 seconds. If the user presses a key on the keypad, possibly associated with the flashing indicator, then controller 24 issues to alarm manager 16 a pass authentication signal. If the key is not pressed within the short time period, then controller 24 issues the authenticated disarm signal. For the user, this embodiment allows for a single code to be used and for a simply key press to change the authenticated function from full disarm to pass. Use of a single code can be easier for the user, either because only one code for keypad entry needs to be memorized or because only one key or RFID device needs to be in possession of the user.

For issuing a pass for exiting the secured premises, the operation is similar. A user enters at controller 22 the normal disarm code. The controller 24 then causes display 20 to indicate that disarm has been authenticated and will take effect shortly. The user may press a key within the short time period to cause controller 24 to issue to alarm manager 16 a pass authentication instead of a disarm signal. In absence of the user entry within the short period, the controller 24 sends the disarm signal.

As an alternative embodiment to the embodiment of Figure 3, the key to be pressed can indicate the zone for which the pass is to be issued, and thus will trigger the pass and specify the zone at the same time. Of course, it is likewise possible to require an entry to request a pass instead of a system disarm and a separate entry to request that the pass applies to a specified zone.

It will be appreciated that the use of RFID transponders, smart cards, Dallas® keys, magnetic stripe cards, key lock switches, biometric scanners, or the like may be used in place of a keypad or in conjunction with a keypad for authenticating users or occupants. In the above embodiments, pass authentication is done using a controller 24 within the secured premises. However, it will be appreciated that when a user is authenticated outside secured premises as part of access control, such authentication can be either used in combination with inside authentication for pass authentication purposes, or may be used as a substitute for inside secured premises pass authentication. Such security system configuration can be defined as a function of specific doors and/or as a function of specific users. In the case that different stay mode configurations are provided, access control authentication may be used for pass authentication in some stay mode configurations and not others.

As illustrated in Figure 5a, if an occupant enters protected premises and a few seconds later a thief enters through a different entrance, the events may be recorded as shown. In the embodiment of

Figure 2, the pass does not identify the event, and so it is assumed that it is the first event to be passed. The display will continue to show the outstanding "patio door" zone event after the pass is authenticated, and the alarm will be generated unless other action is taken.

As illustrated in Figure 5b, if an occupant leaves protected premises and a few seconds later a thief enters through a different entrance, the events may be recorded as shown. In the embodiment of Figure 3, the pass identifies the event, and so remaining occupants will see on the display the outstanding "patio door" zone event, and the alarm will be generated unless other action is taken.

As illustrated in Figure 5c, if a thief carefully monitors an occupant entering protected premises, perhaps with the help of a spotter in radio contact with the thief, and the thief enters through a different entrance even a few seconds before the occupant, the events may be recorded as shown. In the embodiment of Figure 3, the pass identifies the event, and so the occupants will see on the display the outstanding "patio door" zone event, and the alarm will be generated unless other action is taken.

While the invention has been described above with reference to entry and exit, it can also be applied to authorizing a window or a patio door to be opened temporarily for ventilation. In this embodiment, the security system is operative to by-pass a zone and automatically re-arm the zone when it is detected that the by-pass is no longer required. For example, the by-pass of a zone representing a window sensor may be authenticated using a keypad, and the by-pass is automatically removed when the window is closed again. This makes the use of a by-pass more secure and more convenient since the removal of the by-pass does not require use of the keypad. The removal of the by-pass can be instant or after a short delay of a few seconds, the latter providing a "debounce" function.

Claims

1. A security system operable in a mode in which at least protected premises perimeter sensors or detectors are in an armed state, the security system comprising an entry authorization controller adapted to authenticate a user and, in response to authenticating said user, to prevent generating said alarm as said user activates said protected premises perimeter sensors or detectors and to otherwise maintain said armed state.

2. The security system as defined in claim 1, wherein said mode is a stay mode wherein sensors or detectors within said protected premises remain in an unarmed state.

3. The security system as defined in claim 1 or 2, wherein a delay is provided between detection of breach of said perimeter and generating an alarm, said entry authorization controller being adapted to restore said armed state during said delay in response to said authenticating said user.

4. The security system as defined in claim 2, wherein said entry authorization controller is further adapted to authenticate a user about to exit said perimeter and restore said stay mode following detection of breach of said perimeter by said exit causing a zone to be open without generating said alarm and without disarming said protected premises perimeter sensors or detectors.

5. The security system as defined in claim 4, wherein said stay mode is restored immediately following a brief debounce delay after detection of closing of said zone.

6. The security system as defined in any one of claims 1 to 5, wherein said entry authorization controller authenticates said user by detecting a code entered at a keypad located within said protected premises.

7. The security system as defined in claim 6, wherein said security system is adapted to use said keypad for arming and disarming said security system.

8. The security system as defined in claim 7, wherein said security system is further adapted to use said keypad for programming said security system.

9. The security system as defined in any one of claims 6 to 8, wherein said code is accepted to authenticate said user and to signal to said entry authorization controller to prevent generating said alarm.

10. The security system as defined in claim 9, wherein said code identifies a point of entry through said perimeter, said security system being adapted to generate said alarm if a different point of entry is also detected.

11. The security system as defined in any one of claims 1 to 5, further comprising a portable wireless transmitter and a wireless receiver, the wireless receiver being adapted to receive a code from said transmitter, said entry authorization controller receiving said code and using said code to authenticate said user.

12. The security system as defined in claim 11, wherein said entry authorization controller further authenticates said user following entry into said premises by detecting a code entered at a keypad located within said protected premises.

13. The security system as defined in claim 11 or 12, wherein said user's activation of said protected premises perimeter sensors or detectors causes a zone of said security system to be open, and said armed state is restored immediately following a brief debounce delay after detection of closing of said zone.

14. The security system as defined in claim 2, wherein said armed protected premises perimeter sensors or detectors include sensors or detectors associated with at least one zone within said protected premises perimeter, said stay mode being associated with a partition of said protected premises.

15. The security system as defined in claim 14, wherein more than one stay mode configuration is defined and said entry authorization controller is adapted to allow one of said stay mode configurations to be user selected.

16. The security system as defined in claim 15, wherein said stay mode configurations represent different levels of security.

17. The security system as defined in claim 16, further comprising a display of said selected level of security.

18. The security system as defined in any one of claims 1 to 13, wherein said security system is adapted to operate selectively in said stay mode or in an away mode, said security system operating in said away mode with both said protected premises perimeter sensors or detectors and interior sensors or detectors armed wherein an away mode entry delay is provided between detection of breach of said perimeter or intruder detection within said protected premises and generating an alarm, and said entry authorization controller is further adapted to authenticate said user during said away mode entry delay and place said security system in said stay mode without generating said alarm and without disarming said protected premises perimeter sensors or detectors.

19. The security system as defined in one of claims 1 to 13, wherein said entry authorization controller is adapted to define which ones of said protected premises perimeter sensors or detectors may be involved in entry or exit with said entry authorization controller restoring said stay

mode without generating said alarm and without disarming said protected premises perimeter sensors or detectors.

20. The security system as defined in claim 19, wherein said system is adapted to generate an immediate alarm when others of said protected premises perimeter sensors or detectors are involved in entry or exit.

21. The security system as defined in claim 19, wherein said system is adapted to generate an alarm when others of said protected premises perimeter sensors or detectors are involved in entry or exit in absence of authentication of said user different from said stay mode controller authentication.

22. The security system as defined in any one of claims 1 to 13, wherein said stay mode controller is adapted to have a configuration according to which said stay mode controller authenticates said user as a function of any two of: zone corresponding to said protected premises perimeter sensors or detectors; exit, entry or both; and individual user or one of a plurality of user groups.

23. The security system as defined in claim 22, wherein more than one configuration is defined and said entry authorization controller is adapted to allow one of said configurations to be user selected.

24. The security system as defined in claim 23, wherein said configurations represent different levels of security.

25. The security system as defined in claim 22, wherein said stay mode controller is adapted to authenticate said user as a function of: zone corresponding to said protected premises perimeter sensors or detectors; exit, entry or both; and individual user or one of a plurality of user groups.

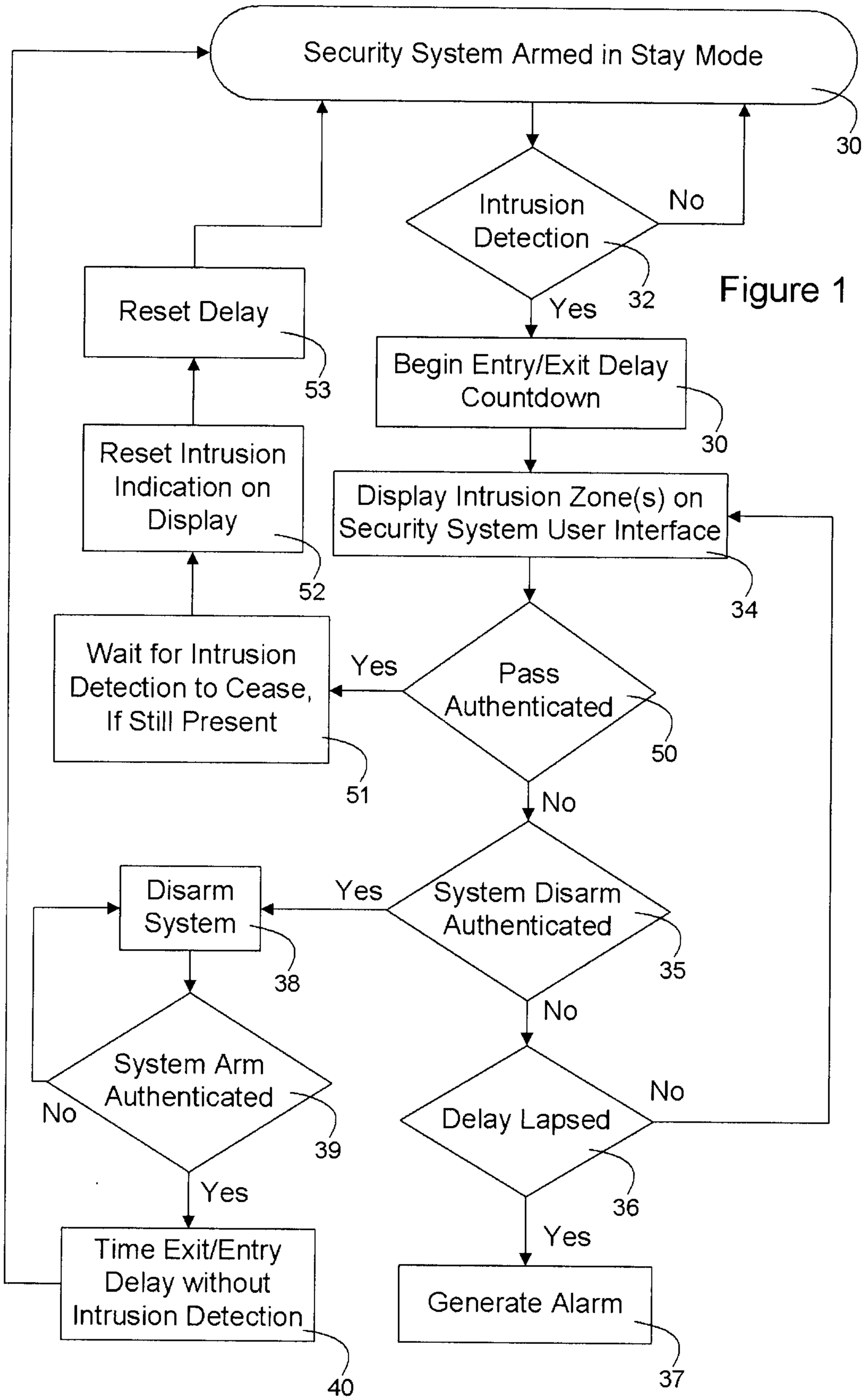

Security System Armed in Stay Mode
30
Intrusion Detection
No
32
Yes
Reset Delay
53
Begin Entry/Exit Delay Countdown
30
Reset Intrusion Indication on Display
52
Display Intrusion Zone(s) on Security System User Interface
34
Wait for Intrusion Detection to Cease, If Still Present
51
Yes
Pass Authenticated
50
No
Disarm System
38
Yes
System Disarm Authenticated
35
No
System Arm Authenticated
No
39
Yes
Delay Lapsed
No
36
Yes
Time Exit/Entry Delay without Intrusion Detection
40
Generate Alarm
37

Figure 1

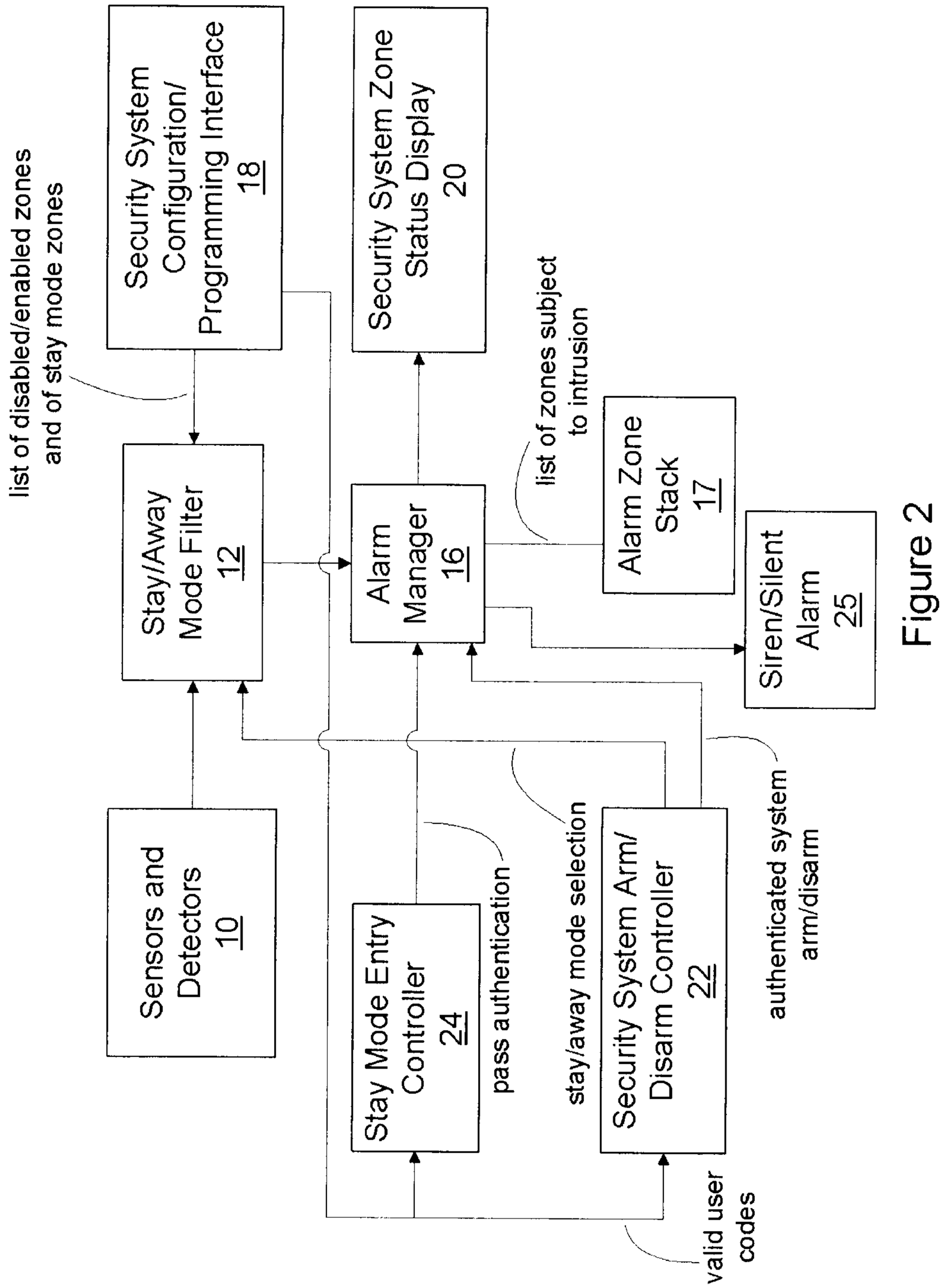

Security System Configuration/ Programming Interface 18
Security System Zone Status Display 20
list of disabled/enabled zones and of stay mode zones
Stay/Away Mode Filter 12
Alarm Manager 16
list of zones subject to intrusion
Alarm Zone Stack 17
Siren/Silent Alarm 25
Sensors and Detectors 10
Stay Mode Entry Controller 24
pass authentication
stay/away mode selection
Security System Arm/ Disarm Controller 22
authenticated system arm/disarm
valid user codes

Figure 2

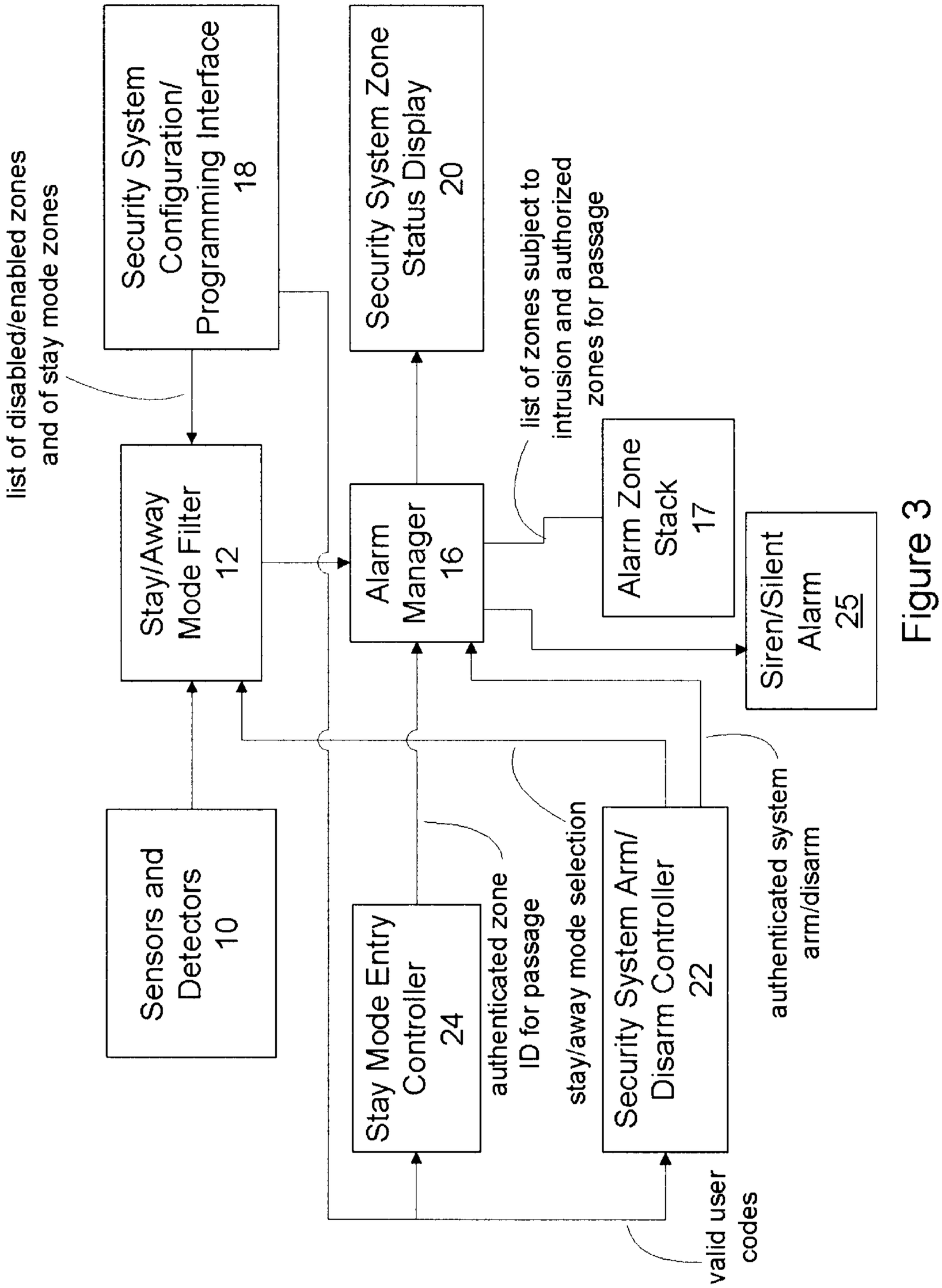

Security System Configuration/ Programming Interface 18
Security System Zone Status Display 20
list of disabled/enabled zones and of stay mode zones
Stay/Away Mode Filter 12
Alarm Manager 16
list of zones subject to intrusion and authorized zones for passage
Alarm Zone Stack 17
Siren/Silent Alarm 25
Sensors and Detectors 10
Stay Mode Entry Controller 24
authenticated zone ID for passage
stay/away mode selection
Security System Arm/ Disarm Controller 22
authenticated system arm/disarm
valid user codes

Figure 3

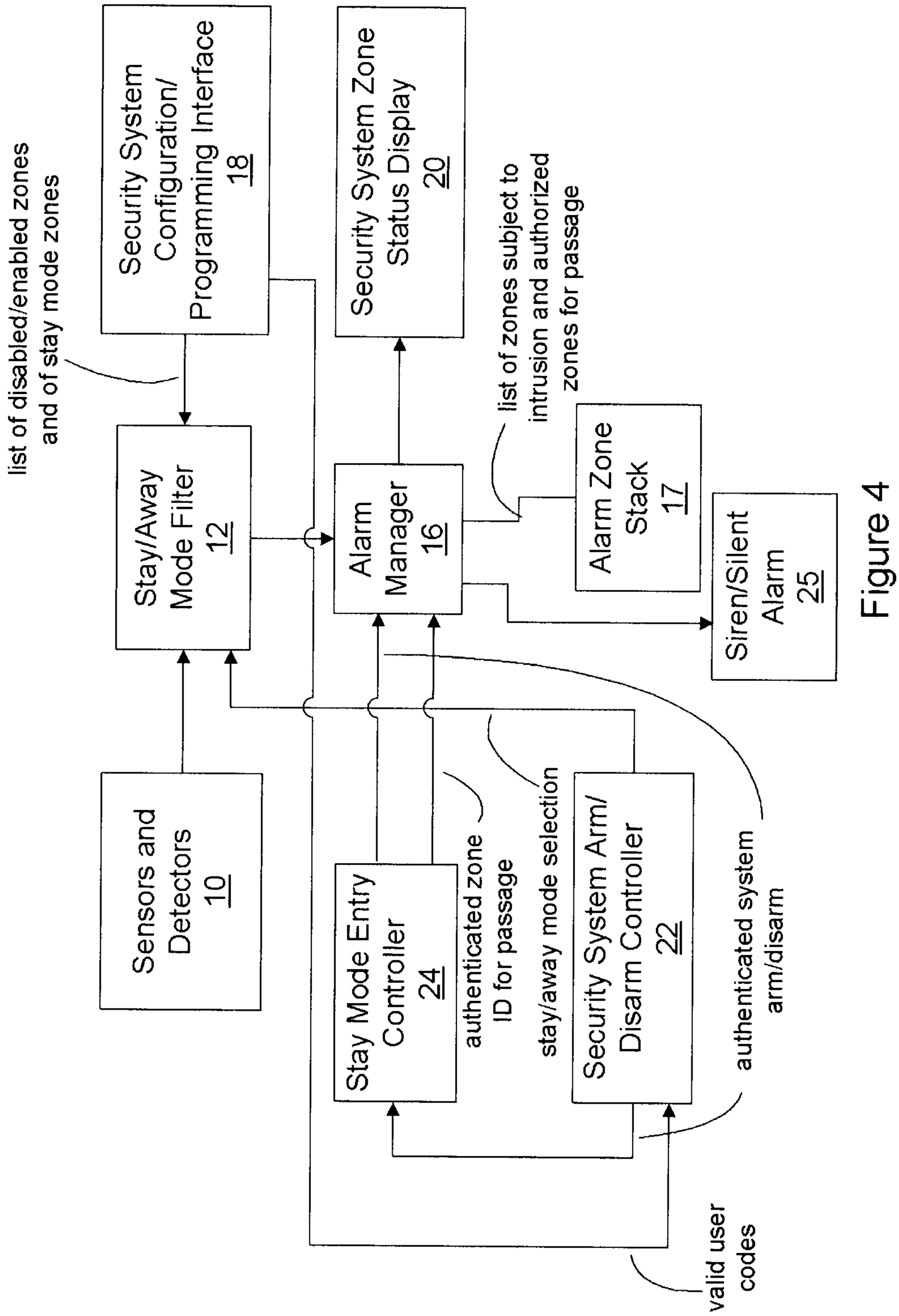

Security System Configuration/ Programming Interface 18
Security System Zone Status Display 20
list of disabled/enabled zones and of stay mode zones
Stay/Away Mode Filter 12
Alarm Manager 16
list of zones subject to intrusion and authorized zones for passage
Alarm Zone Stack 17
Siren/Silent Alarm 25
Sensors and Detectors 10
Stay Mode Entry Controller 24
authenticated zone ID for passage
stay/away mode selection
Security System Arm/ Disarm Controller 22
authenticated system arm/disarm
valid user codes

Figure 4

Alarm Zone Stack

Intrusion	Pass
22:24:09 Front Door Open	....
22:24:14 Patio Door Open	....
22:24:15 Front Door Closed	....
22:24:19 Patio Door Closed	....
....	22:24:32

Figure 5A

Alarm Zone Stack

Intrusion	Pass
....	07:14:19 Front Door
07:14:28 Front Door Open	....
07:14:32 Front Door Closed	....
07:14:37 Patio Door Open	....
07:14:40 Patio Door Closed	....

Figure 5B

Alarm Zone Stack

Intrusion	Pass
22:24:11 Patio Door Open	....
22:24:13 Front Door Open	....
22:24:18 Front Door Closed	....
22:24:19 Patio Door Closed	....
....	22:24:32 Front Door

Figure 5C

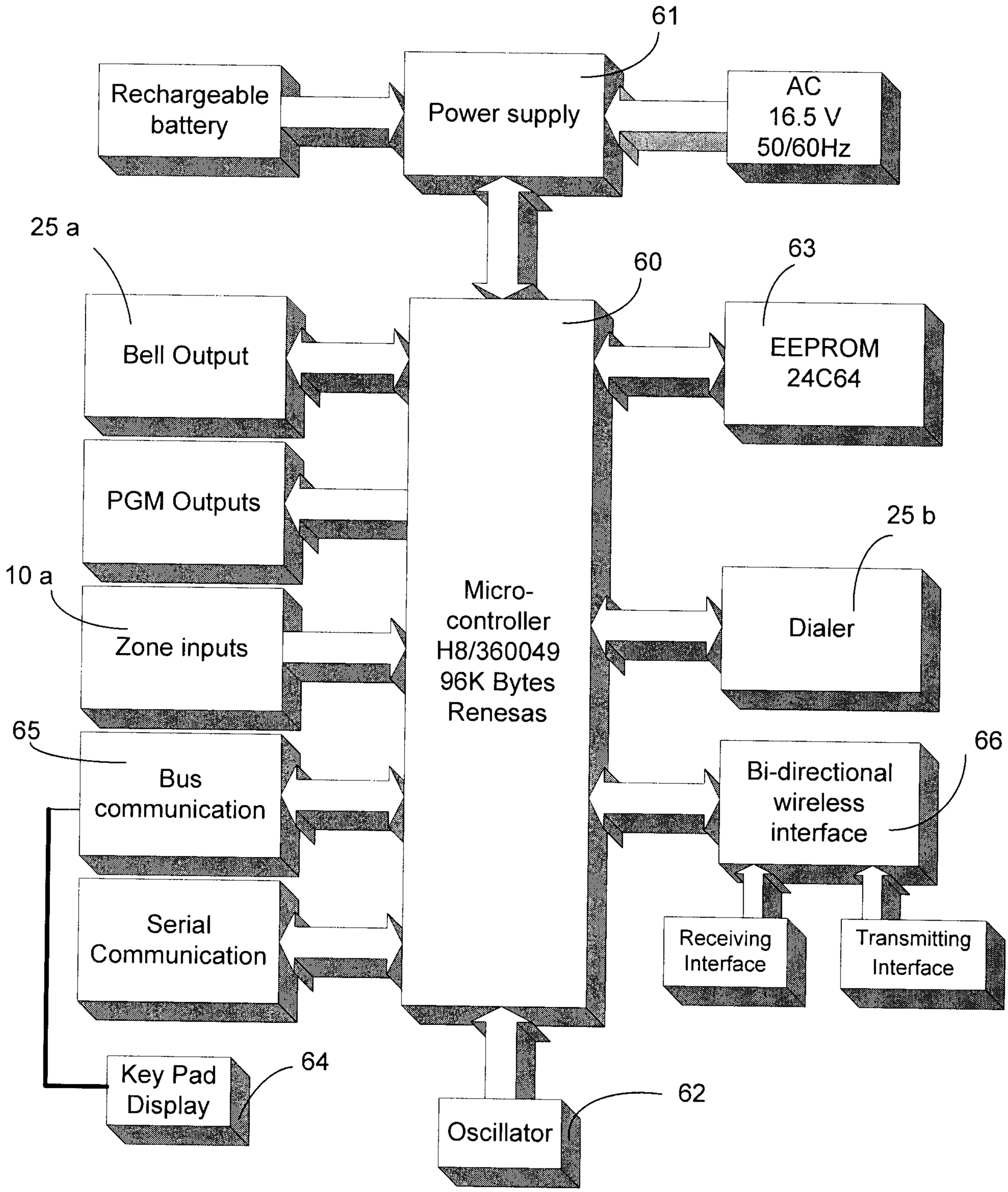
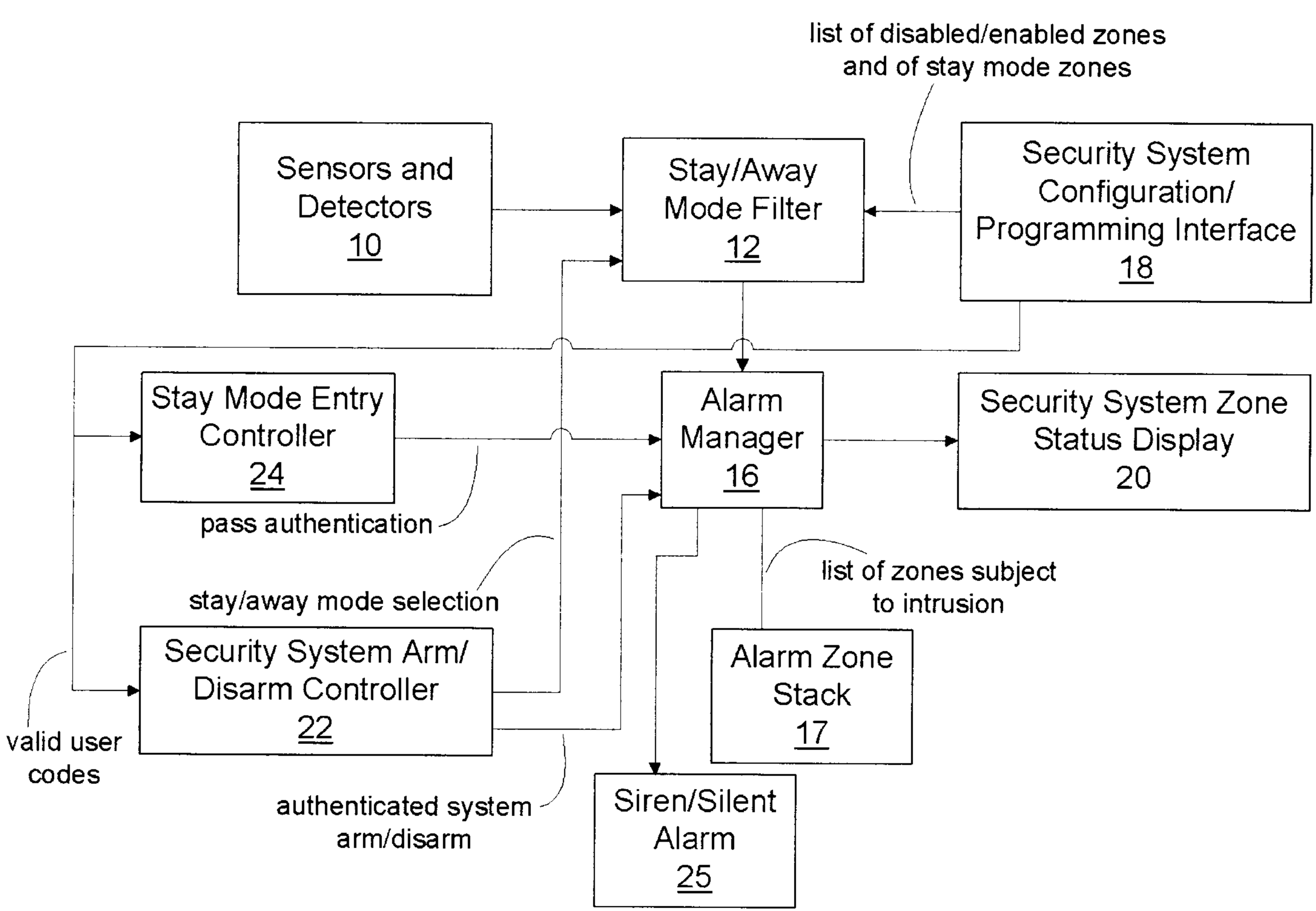

61
Rechargeable battery
Power supply
AC 16.5 V 50/60Hz
25 a
60
63
Bell Output
EEPROM 24C64
PGM Outputs
25 b
10 a
Zone inputs
Micro-controller H8/360049 96K Bytes Renesas
Dialer
65
66
Bus communication
Bi-directional wireless interface
Serial Communication
Receiving Interface
Transmitting Interface
64
Key Pad Display
62
Oscillator

Figure 6


list of disabled/enabled zones
and of stay mode zones
Sensors and Detectors 10
Stay/Away Mode Filter 12
Security System Configuration/ Programming Interface 18
Stay Mode Entry Controller 24
Alarm Manager 16
Security System Zone Status Display 20
pass authentication
stay/away mode selection
list of zones subject to intrusion
Security System Arm/ Disarm Controller 22
Alarm Zone Stack 17
valid user codes
authenticated system arm/disarm
Siren/Silent Alarm 25