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

(11) EP 3 285 238 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.02.2018 Bulletin 2018/08

(51) Int Cl.:
G08B 13/196 *(2006.01)*

(21) Application number: **17186497.8**

(22) Date of filing: **16.08.2017**

(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
Designated Validation States:
MA MD

(30) Priority: **16.08.2016 US 201615237873**

(71) Applicant: **iControl Networks, Inc.**
Philadelphia, PA 19103 (US)

(72) Inventors:
- **Sundermeyer, Ken**
  Philadelphia, PA 19103 (US)
- **Fulker, Jim**
  Philadelphia, PA 19103 (US)
- **Davidson, Matt**
  Philadelphia, PA 19103 (US)
- **Dawes, Paul**
  Philadelphia, PA 19103 (US)

(74) Representative: **V.O.**
P.O. Box 87930
Carnegieplein 5
2508 DH Den Haag (NL)

(54) AUTOMATION SYSTEM USER INTERFACE

(57) Systems and methods include an automation network comprising a gateway located at/in a premises. The gateway is coupled to a remote network and is configured to control components at the premises including premises devices and a security system comprising security system components. The components include at least one camera. A sensor user interface (SUI) is coupled to the gateway and presented to a user via remote client devices. The SUI includes a display elements for managing and receiving data of the premises components agnostically across the remote client devices. The display elements include a timeline user interface comprising event data of the components positioned at a time corresponding to events.

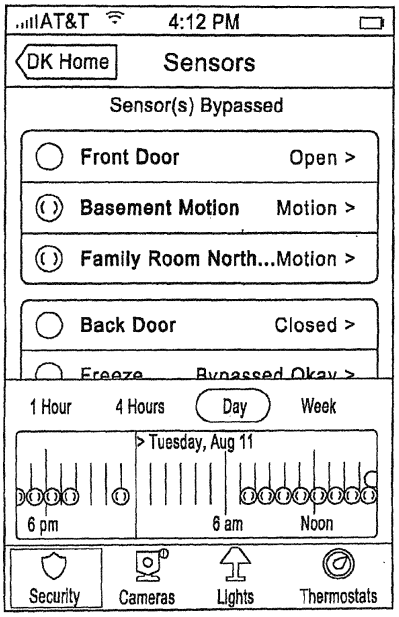


FIG. 15

EP 3 285 238 A2

Description

RELATED APPLICATIONS

[0001] This application claims the benefit of United States (US) Patent Application Number 62/205,872, filed August 17, 2015.

[0002] This application claims the benefit of US Patent Application Number 62/205,922, filed August 17, 2015.

[0003] This application is a continuation in part application of US Patent Application Number 12/189,780, filed August 11, 2008.

[0004] This application is a continuation in part application of US Patent Application Number 13/531,757, filed June 25, 2012.

[0005] This application is a continuation in part application of US Patent Application Number 12/197,958, filed August 25, 2008.

[0006] This application is a continuation in part application of US Patent Application Number 13/334,998, filed December 22, 2011.

[0007] This application is a continuation in part application of US Patent Application Number 12/539,537, filed August 11, 2009.

[0008] This application is a continuation in part application of US Patent Application Number 14/645,808, filed March 12, 2015.

[0009] This application is a continuation in part application of US Patent Application Number 13/104,932, filed May 10, 2011.

[0010] This application is a continuation in part application of US Patent Application Number 13/104,936, filed May 10, 2011.

[0011] This application is a continuation in part application of US Patent Application Number 13/929,568, filed June 27, 2013.

[0012] This application is a continuation in part application of US Patent Application Number 14/704,045, filed May 5, 2015.

[0013] This application is a continuation in part application of US Patent Application Number 14/704,098, filed May 5, 2015.

[0014] This application is a continuation in part application of US Patent Application Number 14/704,127, filed May 5, 2015.

[0015] This application is a continuation in part application of US Patent Application Number 14/628,651, filed February 23, 2015.

[0016] This application is a continuation in part application of US Patent Application Number 13/718,851, filed December 18, 2012.

[0017] This application is a continuation in part application of US Patent Application Number 12/972,740, filed December 20, 2010.

[0018] This application is a continuation in part application of US Patent Application Number 13/954,553, filed July 30, 2013.

[0019] This application is a continuation in part application of US Patent Application Number 14/943,162, filed November 17, 2015.

[0020] This application is a continuation in part application of US Patent Application Number 15/177,915, filed June 9, 2016.

[0021] This application is a continuation in part application of US Patent Application Number 15/177,448, filed June 9, 2016.

[0022] This application is a continuation in part application of US Patent Application Number 15/196,281, filed June 29, 2016.

[0023] This application is a continuation in part application of US Patent Application Number 15/198,531, filed June 30, 2016.

[0024] This application is a continuation in part application of US Patent Application Number 15/204,662, filed July 7, 2016.

TECHNICAL FIELD

[0025] The embodiments described herein relate generally to a method and apparatus for improving the capabilities of home automation systems in premises applications.

BACKGROUND

[0026] The field of home and small business security is dominated by technology suppliers who build comprehensive 'closed' security systems, where the individual components (sensors, security panels, keypads) operate solely within the confines of a single vendor solution. For example, a wireless motion sensor from vendor A cannot be used with a security panel from vendor B. Each vendor typically has developed sophisticated proprietary wireless technologies to enable the installation and management of wireless sensors, with little or no ability for the wireless devices to operate separate from the vendor's homogeneous system. Furthermore, these traditional systems are extremely limited in their ability to interface either to a local or wide area standards-based network (such as an IP network); most installed systems support only a lowbandwidth, intermittent connection utilizing phone lines or cellular (RF) backup systems. Wireless security technology from providers such as GE Security, Honeywell, and DSC/Tyco are well known in the art, and are examples of this proprietary approach to security systems for home and business.

[0027] Furthermore, with the proliferation of the internet, ethernet and WiFi local area networks (LANs) and advanced wide area networks (WANs) that offer high bandwidth, low latency connections (broadband), as well as more advanced wireless WAN data networks (e.g. GPRS or CDMA 1xRTT) there increasingly exists the networking capability to extend these traditional security systems to offer enhanced functionality. In addition, the proliferation of broadband access has driven a corresponding increase in home and small business networking technologies and devices. It is desirable to extend traditional security systems to encompass enhanced functionality such as the ability to control and manage security systems from the world wide web, cellular telephones, or advanced function internet-based devices. Other desired functionality includes an open systems approach to interface home security systems to home and small business networks.

[0028] Due to the proprietary approach described above, the traditional vendors are the only ones capable of taking advantage of these new network functions. To date, even though the vast majority of home and business customers have broadband network access in their premises, most security systems do not offer the advanced capabilities associated with high speed, low-latency LANs and WANs. This is primarily because the proprietary vendors have not been able to deliver such technology efficiently or effectively. Solution providers attempting to address this need are becoming known in the art, including three categories of vendors: traditional proprietary hardware providers such as Honeywell and GE Security; third party hard-wired module providers such as Alarm.com, NextAlarm, and uControl; and new proprietary systems providers such as InGrid.

[0029] A disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the continued proprietary approach of these vendors. As they develop technology in this area it once again operates only with the hardware from that specific vendor, ignoring the need for a heterogeneous, cross-vendor solution. Yet another disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the lack of experience and capability of these companies in creating open internet and web based solutions, and consumer friendly interfaces.

[0030] A disadvantage of the prior art technologies of the third party hard-wired module providers arises due to the installation and operational complexities and functional limitations associated with hardwiring a new component into existing security systems. Moreover, a disadvantage of the prior art technologies of the new proprietary systems providers arises due to the need to discard all prior technologies, and implement an entirely new form of security system to access the new functionalities associated with broadband and wireless data networks. There remains, therefore, a need for systems, devices, and methods that easily interface to and control the existing proprietary security technologies utilizing a variety of wireless technologies.

INCORPORATION BY REFERENCE

[0031] Each patent, patent application, and/or publication mentioned in this specification is herein incorporated by reference in its entirety to the same extent as if each individual patent, patent application, and/or publication was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

[0032]

Figure 1 is a block diagram of the integrated security system, under an embodiment.
Figure 2 is a block diagram of components of the integrated security system, under an embodiment.
Figure 3 is a block diagram of the gateway software or applications, under an embodiment.
Figure 4 is a block diagram of the gateway components, under an embodiment.
Figure 5 (collectively Figures 5A and 5B) shows the orb icon and corresponding text summary display elements,

under an embodiment.

Figure 6 is a table of security state and the corresponding sensor status displayed on the SUI, under an embodiment.

Figure 7 is a table of system state and the corresponding warning text displayed as system warnings on the SUI, under an embodiment.

Figure 8 is a table of sensor state/sort order and the corresponding sensor name and status text of the SUI, under an embodiment.

Figure 9 shows icons of the interesting sensors, under an embodiment.

Figure 10 shows the quiet sensor icon, under an embodiment.

Figure 11 is an example Home Management Mode (HMM) screen presented via the web portal SUI, under an embodiment.

Figure 12 is an example Home Management Mode (HMM) screen presented via the mobile portal SUI, under an embodiment.

Figure 13 is a block diagram of an iPhone® client device SUI, under an embodiment.

Figure 14 is a first example iPhone® client device SUI, under an embodiment.

Figure 15 is a second example iPhone® client device SUI, under an embodiment.

Figure 16 is a block diagram of a mobile portal client device SUI, under an embodiment.

Figure 17 is an example summary page or screen presented via the mobile portal SUI, under an embodiment.

Figure 18 is an example security panel page or screen presented via the mobile portal SUI, under an embodiment.

Figure 19 is an example sensor status page or screen presented via the mobile portal SUI, under an embodiment.

Figure 20 is an example interface page or screen presented via the web portal SUI, under an embodiment.

Figure 21 is an example summary page or screen presented via the touchscreen SUI, under an embodiment.

Figure 22 is an example sensor status page or screen presented via the touchscreen SUI, under an embodiment.

Figure 23 is an example Home View display, under an embodiment.

Figure 24 shows a table of sensor icons displayed on the Home View floor plan, under an embodiment.

Figure 25 shows example device icons of Home View, under an embodiment.

Figure 26 shows a Home View display that includes indicators for multiple floors, under an embodiment.

Figure 27 shows the system states along with the corresponding Home View display and system or orb icon, under an embodiment.

Figure 28 shows a Home View floor display (disarmed) that includes a warning indicator, under an embodiment.

Figure 29 shows an example of the Home View using the iPhone security tab, under an embodiment.

Figure 30 shows an example screen for site Settings, under an embodiment.

Figure 31 shows an example screen for Security Tab Options, under an embodiment.

Figure 32 shows an example "Add Floor" screen for use in selecting a floor plan, under an embodiment.

Figure 33 shows an "Edit Home View" screen of the editor, under an embodiment.

Figure 34 shows an example of dragging a device icon during which a name of the device ("Front Door") is displayed, under an embodiment.

Figure 35 is an example of a U-shaped floor plan customized by changing interior tiles to define walls, under an embodiment.

Figure 36 shows an example in which the zoom level is increased and dragging has been used to focus on a sensor location, under an embodiment.

Figure 37 is an example "Add Floor" page, under an embodiment.

Figure 38 is an example Edit Home View screen showing the floor thumbnails for use in selecting a floor, under an embodiment.

Figure 39 shows the Edit Home View screen with a delete floor selector, under an embodiment.

Figure 40 is an example Edit Home View screen displaying options to "Save" and "Don't Save" changes following selection of the Done button, under an embodiment.

Figure 41 is an example of the floor grid data, under an embodiment.

Figure 42 is an example sensor hash table for a single-floor site, under an embodiment.

Figure 43 shows an example hash table mapping, under an embodiment.

Figure 44 shows the twelve shapes of a tile set, under an embodiment.

Figure 45 shows the tile shapes and corresponding fill options for rendered tiles, under an embodiment.

Figure 46 is an example tile rendering for a room of a premise, under an embodiment.

Figure 47 is an example popup display in response to hovering near/adjacent a sensor icon (e.g., "Garage" sensor), under an embodiment.

Figure 48 shows a Home View display that includes a floor plan display 4800 of a selected floor along with indicators 4801/4802 for multiple floors, under an embodiment.

Figure 49 shows an example of the Home View user interface displayed via a mobile device (e.g., iPhone), under an embodiment.

Home View is configured via site settings as described in detail herein. Each application retains or remembers the user's preferred mode across sessions.

Figure 50 shows an example of a Settings page of Home View, under an embodiment.

Figure 51 shows an example "Home View Setup" editor page 5100 for use in selecting a floor plan, under an embodiment.

Figure 52 shows a "Home View Setup" editor screen 5200 with a selected floor plan 5201, under an embodiment.

Figure 59 shows a Home View Setup page 5900 with options displayed, under an embodiment.

Figure 53 shows an example editor screen 5300 for which a label 5301 with a name of the device ("Front Door") is displayed, under an embodiment.

Figure 54 shows a Home View Setup page 5400 with a selected floor plan 5201 that has been edited to add numerous interior walls 5401, under an embodiment.

Figure 55 shows a Home View Setup page with a label editing prompt 5501, under an embodiment.

Figure 56 shows a Home View Setup page 5600 in a zoomed editing mode to zoom on one room 5601 in a building, under an embodiment.

Figure 57 shows a Home View Setup page for adding at least one floor to a floor plan, under an embodiment.

Figure 58 shows a Home View Setup page 5800 with editing for multiple floors, under an embodiment.

Figure 60 shows a Home View Setup page 6000 with editor exit option prompts 6001 displayed, under an embodiment.

Figure 61 is an example floor plan, under an embodiment.

Figure 62 is an example Home View one-story floor plan, under an embodiment.

Figure 63 is an example Home View floor plan that includes two devices, under an embodiment.

Figure 64 is an example Home View floor plan that includes two labels, under an embodiment.

Figure 65 is a block diagram of IP device integration with a premise network, under an embodiment.

Figure 66 is a block diagram of IP device integration with a premise network, under an alternative embodiment.

Figure 67 is a block diagram of a touchscreen, under an embodiment.

Figure 68 is an example screenshot of a networked security touchscreen, under an embodiment.

Figure 69 is a block diagram of network or premise device integration with a premise network, under an embodiment.

Figure 70 is a block diagram of network or premise device integration with a premise network, under an alternative embodiment.

Figure 71 is a flow diagram for a method of forming a security network including integrated security system components, under an embodiment.

Figure 72 is a flow diagram for a method of forming a security network including integrated security system components and network devices, under an embodiment.

Figure 73 is a flow diagram for installation of an IP device into a private network environment, under an embodiment.

Figure 74 is a block diagram showing communications among IP devices of the private network environment, under an embodiment.

Figure 75 is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment.

Figure 76 is a block diagram of an integrated security system wirelessly interfacing to proprietary security systems, under an embodiment.

Figure 77 is a flow diagram for wirelessly 'learning' the gateway into an existing security system and discovering extant sensors, under an embodiment.

Figure 78 is a block diagram of a security system in which the legacy panel is replaced with a wireless security panel wirelessly coupled to a gateway, under an embodiment.

Figure 79 is a block diagram of a security system in which the legacy panel is replaced with a wireless security panel wirelessly coupled to a gateway, and a touchscreen, under an alternative embodiment.

Figure 80 is a block diagram of a security system in which the legacy panel is replaced with a wireless security panel connected to a gateway via an Ethernet coupling, under another alternative embodiment.

Figure 81 is a flow diagram for automatic takeover of a security system, under an embodiment.

Figure 82 is a flow diagram for automatic takeover of a security system, under an alternative embodiment.

Figure 83 is an example status interface of Home View 3D, under an embodiment.

Figure 84 is an example user interface of Home View 3D, under an embodiment.

Figure 85 is an example user interface showing "enable" control of Home View 3D, under an embodiment.

Figure 86 is an example user interface showing "disable" control of Home View 3D, under an embodiment.

Figure 87 is an example editor interface with indicators of Home View 3D being enabled, under an embodiment.

Figure 88 is an example user interface showing five floors, under an embodiment.

Figure 89 is an example interface of Home View 3D showing variables, under an embodiment.

Figure 90 shows example renderings for square, wide, and tall canvases, 2D single floor, and 2D multi floor, under

an embodiment.

Figure 91 is an example user interface showing a "heat map" of Home View 3D, under an embodiment.

Figure 92 is an example user interface for configuring a "heat map" of Home View 3D, under an embodiment.

Figure 93 is another example user interface for configuring a "heat map" of Home View 3D, under an embodiment.

Figure 94A is a flow diagram showing an example flow for accessing camera data via a smart phone, under an embodiment.

Figure 94B is a flow diagram showing an example flow for accessing camera data via a tablet device, under an embodiment.

Figure 95 is an example of a live view including the UI, under an embodiment.

Figure 96 is an example of a live view with the UI hidden, under an embodiment.

Figure 97 is an example of a live view with an event notification ("Motion detected") displayed during live viewing, and with the UI displayed, under an embodiment.

Figure 98 is an example of a live view with an event notification ("Motion detected") displayed during live viewing, and with the UI hidden, under an embodiment.

Figure 99 is an example of a UI including a live camera view and the Timeline, under an embodiment.

Figure 100 is an example of a UI including the live camera view and Timeline, and a message regarding data, under an embodiment.

Figure 101 is an example of a UI including the Timeline offset from the live viewing position, under an embodiment.

Figure 102 is an example of a UI as a clip or picture is loaded, under an embodiment.

Figure 103 is an example of a UI displaying a loaded picture, under an embodiment.

Figure 104 is an example of a UI displaying a loaded video clip, under an embodiment.

Figure 105 is an example of a UI displaying a paused video clip, under an embodiment.

Figure 106 is an example of a UI display having completed play of a video clip, under an embodiment.

Figure 107 is an example of a UI having no top bar and on which the zoom map is positioned in a top region of the display, under an embodiment.

Figure 108 is an example of a UI having a relatively minimal top bar, with a zoom map is positioned on the display just below the top bar, under an embodiment.

Figure 109 is an example of a UI having a relatively large top bar, with a zoom map is positioned on the display just below the top bar, under an embodiment.

Figure 110 is an example of a UI including the Timeline with CVR data, under an embodiment.

Figure 111 is an example of a UI including the Timeline with magnification, under an embodiment.

Figure 112 is an example of a UI configured to include thumbnail images in the Timeline, under an embodiment.

DETAILED DESCRIPTION

[0033] Systems and methods include an automation network comprising a gateway located at/in a premises. The gateway is coupled to a remote network and is configured to control components at the premises including premises devices and a security system comprising security system components. The components include at least one camera. A sensor user interface (SUI) is coupled to the gateway and presented to a user via remote client devices. The SUI includes a display elements for managing and receiving data of the premises components agnostically across the remote client devices. The display elements include a timeline user interface comprising event data of the components positioned at a time corresponding to events.

[0034] An integrated security system is described that integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network (broadband, cellular/GSM, POTS access) that enables users to remotely stay connected to their premises. The integrated security system, while delivering remote premise monitoring and control functionality to conventional monitored premise protection, complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices (cameras, lamp modules, thermostats, etc.) can be added, enabling users to remotely see live video and/or pictures and control home devices via their personal web portal or webpage, mobile phone, and/or other remote client device. Users can also receive notifications via email or text message when happenings occur, or do not occur, in their home.

[0035] Although the detailed description herein contains many specifics for the purposes of illustration, anyone of ordinary skill in the art will appreciate that many variations and alterations to the following details are within the scope of the embodiments described herein. Thus, the following illustrative embodiments are set forth without any loss of generality to, and without imposing limitations upon, the claimed invention.

[0036] In accordance with the embodiments described herein, a wireless system (e.g., radio frequency (RF)) is provided that enables a security provider or consumer to extend the capabilities of an existing RF-capable security system or a

non-RF-capable security system that has been upgraded to support RF capabilities. The system includes an RF-capable Gateway device (physically located within RF range of the RF-capable security system) and associated software operating on the Gateway device. The system also includes a web server, application server, and remote database providing a persistent store for information related to the system.

[0037] The security systems of an embodiment, referred to herein as the iControl security system or integrated security system, extend the value of traditional home security by adding broadband access and the advantages of remote home monitoring and home control through the formation of a security network including components of the integrated security system integrated with a conventional premise security system and a premise local area network (LAN). With the integrated security system, conventional home security sensors, cameras, touchscreen keypads, lighting controls, and/or Internet Protocol (IP) devices in the home (or business) become connected devices that are accessible anywhere in the world from a web browser, mobile phone or through content-enabled touchscreens. The integrated security system experience allows security operators to both extend the value proposition of their monitored security systems and reach new consumers that include broadband users interested in staying connected to their family, home and property when they are away from home.

[0038] The integrated security system of an embodiment includes security servers (also referred to herein as iConnect servers or security network servers) and an iHub gateway (also referred to herein as the gateway, the iHub, or the iHub client) that couples or integrates into a home network (e.g., LAN) and communicates directly with the home security panel, in both wired and wireless installations. The security system of an embodiment automatically discovers the security system components (e.g., sensors, etc.) belonging to the security system and connected to a control panel of the security system and provides consumers with full two-way access via web and mobile portals. The gateway supports various wireless protocols and can interconnect with a wide range of control panels offered by security system providers. Service providers and users can then extend the system's capabilities with the additional IP cameras, lighting modules or security devices such as interactive touchscreen keypads. The integrated security system adds an enhanced value to these security systems by enabling consumers to stay connected through email and SMS alerts, photo push, event-based video capture and rule-based monitoring and notifications. This solution extends the reach of home security to households with broadband access.

[0039] The integrated security system builds upon the foundation afforded by traditional security systems by layering broadband and mobile access, IP cameras, interactive touchscreens, and an open approach to home automation on top of traditional security system configurations. The integrated security system is easily installed and managed by the security operator, and simplifies the traditional security installation process, as described below.

[0040] The integrated security system provides an open systems solution to the home security market. As such, the foundation of the integrated security system customer premises equipment (CPE) approach has been to abstract devices, and allows applications to manipulate and manage multiple devices from any vendor. The integrated security system DeviceConnect technology that enables this capability supports protocols, devices, and panels from GE Security and Honeywell, as well as consumer devices using Z-Wave, IP cameras (e.g., Ethernet, wifi, and Homeplug), and IP touchscreens. The DeviceConnect is a device abstraction layer that enables any device or protocol layer to interoperate with integrated security system components. This architecture enables the addition of new devices supporting any of these interfaces, as well as add entirely new protocols.

[0041] The benefit of DeviceConnect is that it provides supplier flexibility. The same consistent touchscreen, web, and mobile user experience operate unchanged on whatever security equipment selected by a security system provider, with the system provider's choice of IP cameras, backend data center and central station software.

[0042] The integrated security system provides a complete system that integrates or layers on top of a conventional host security system available from a security system provider. The security system provider therefore can select different components or configurations to offer (e.g., CDMA, GPRS, no cellular, etc.) as well as have iControl modify the integrated security system configuration for the system provider's specific needs (e.g., change the functionality of the web or mobile portal, add a GE or Honeywell-compatible TouchScreen, etc.).

[0043] The integrated security system integrates with the security system provider infrastructure for central station reporting directly via Broadband and GPRS alarm transmissions. Traditional dial-up reporting is supported via the standard panel connectivity. Additionally, the integrated security system provides interfaces for advanced functionality to the CMS, including enhanced alarm events, system installation optimizations, system test verification, video verification, 2-way voice over IP and GSM.

[0044] The integrated security system is an IP centric system that includes broadband connectivity so that the gateway augments the existing security system with broadband and GPRS connectivity. If broadband is down or unavailable GPRS may be used, for example. The integrated security system supports GPRS connectivity using an optional wireless package that includes a GPRS modem in the gateway. The integrated security system treats the GPRS connection as a higher cost though flexible option for data transfers. In an embodiment the GPRS connection is only used to route alarm events (e.g., for cost), however the gateway can be configured (e.g., through the iConnect server interface) to act as a primary channel and pass any or all events over GPRS. Consequently, the integrated security system does not

interfere with the current plain old telephone service (POTS) security panel interface. Alarm events can still be routed through POTS; however the gateway also allows such events to be routed through a broadband or GPRS connection as well. The integrated security system provides a web application interface to the CSR tool suite as well as XML web services interfaces for programmatic integration between the security system provider's existing call center products. The integrated security system includes, for example, APIs that allow the security system provider to integrate components of the integrated security system into a custom call center interface. The APIs include XML web service APIs for integration of existing security system provider call center applications with the integrated security system service. All functionality available in the CSR Web application is provided with these API sets. The Java and XML-based APIs of the integrated security system support provisioning, billing, system administration, CSR, central station, portal user interfaces, and content management functions, to name a few. The integrated security system can provide a customized interface to the security system provider's billing system, or alternatively can provide security system developers with APIs and support in the integration effort.

[0045] The integrated security system provides or includes business component interfaces for provisioning, administration, and customer care to name a few. Standard templates and examples are provided with a defined customer professional services engagement to help integrate OSS/BSS systems of a Service Provider with the integrated security system.

[0046] The integrated security system components support and allow for the integration of customer account creation and deletion with a security system. The iConnect APIs provides access to the provisioning and account management system in iConnect and provide full support for account creation, provisioning, and deletion. Depending on the requirements of the security system provider, the iConnect APIs can be used to completely customize any aspect of the integrated security system backend operational system.

[0047] The integrated security system includes a gateway that supports the following standards-based interfaces, to name a few: Ethernet IP communications via Ethernet ports on the gateway, and standard XML/TCP/IP protocols and ports are employed over secured SSL sessions; USB 2.0 via ports on the gateway; 802.11b/g/n IP communications; GSM/GPRS RF WAN communications; CDMA 1xRTT RF WAN communications (optional, can also support EVDO and 3G technologies).

[0048] The gateway supports the following proprietary interfaces, to name a few: interfaces including Dialog RF network (319.5 MHz) and RS485 Superbus 2000 wired interface; RF mesh network (908 MHz); and interfaces including RF network (345 MHz) and RS485/RS232bus wired interfaces.

[0049] Regarding security for the IP communications (e.g., authentication, authorization, encryption, anti-spoofing, etc), the integrated security system uses SSL to encrypt all IP traffic, using server and client-certificates for authentication, as well as authentication in the data sent over the SSL-encrypted channel. For encryption, integrated security system issues public/private key pairs at the time/place of manufacture, and certificates are not stored in any online storage in an embodiment.

[0050] The integrated security system does not need any special rules at the customer premise and/or at the security system provider central station because the integrated security system makes outgoing connections using TCP over the standard HTTP and HTTPS ports. Provided outbound TCP connections are allowed then no special requirements on the firewalls are necessary.

[0051] Figure 1 is a block diagram of the integrated security system 100, under an embodiment. The integrated security system 100 of an embodiment includes the gateway 102 and the security servers 104 coupled to the conventional home security system 110. At a customer's home or business, the gateway 102 connects and manages the diverse variety of home security and self-monitoring devices. The gateway 102 communicates with the iConnect Servers 104 located in the service provider's data center 106 (or hosted in integrated security system data center), with the communication taking place via a communication network 108 or other network (e.g., cellular network, internet, etc.). These servers 104 manage the system integrations necessary to deliver the integrated system service described herein. The combination of the gateway 102 and the iConnect servers 104 enable a wide variety of remote client devices 120 (e.g., PCs, mobile phones and PDAs) allowing users to remotely stay in touch with their home, business and family. In addition, the technology allows home security and self-monitoring information, as well as relevant third party content such as traffic and weather, to be presented in intuitive ways within the home, such as on advanced touchscreen keypads.

[0052] The integrated security system service (also referred to as iControl service) can be managed by a service provider via browser-based Maintenance and Service Management applications that are provided with the iConnect Servers. Or, if desired, the service can be more tightly integrated with existing OSS/BSS and service delivery systems via the iConnect web services-based XML APIs.

[0053] The integrated security system service can also coordinate the sending of alarms to the home security Central Monitoring Station (CMS) 199. Alarms are passed to the CMS 199 using standard protocols such as Contact ID or SIA and can be generated from the home security panel location as well as by iConnect server 104 conditions (such as lack of communications with the integrated security system). In addition, the link between the security servers 104 and CMS 199 provides tighter integration between home security and self-monitoring devices and the gateway 102. Such integration

enables advanced security capabilities such as the ability for CMS personnel to view photos taken at the time a burglary alarm was triggered. For maximum security, the gateway 102 and iConnect servers 104 support the use of a mobile network (both GPRS and CDMA options are available) as a backup to the primary broadband connection.

[0054] The integrated security system service is delivered by hosted servers running software components that communicate with a variety of client types while interacting with other systems. Figure 2 is a block diagram of components of the integrated security system 100, under an embodiment. Following is a more detailed description of the components.

[0055] The iConnect servers 104 support a diverse collection of clients 120 ranging from mobile devices, to PCs, to in-home security devices, to a service provider's internal systems. Most clients 120 are used by end-users, but there are also a number of clients 120 that are used to operate the service.

[0056] Clients 120 used by end-users of the integrated security system 100 include, but are not limited to, the following:

Clients based on gateway client applications 202 (e.g., a processor-based device running the gateway technology that manages home security and automation devices).

A web browser 204 accessing a Web Portal application, performing end-user configuration and customization of the integrated security system service as well as monitoring of in-home device status, viewing photos and video, etc. Device and user management can also be performed by this portal application.

A mobile device 206 (e.g., PDA, mobile phone, etc.) accessing the integrated security system Mobile Portal. This type of client 206 is used by end-users to view system status and perform operations on devices (e.g., turning on a lamp, arming a security panel, etc.) rather than for system configuration tasks such as adding a new device or user.

PC or browser-based "widget" containers 208 that present integrated security system service content, as well as other third-party content, in simple, targeted ways (e.g. a widget that resides on a PC desktop and shows live video from a single in-home camera). "Widget" as used herein means applications or programs in the system.

Touchscreen home security keypads 208 and advanced in-home devices that present a variety of content widgets via an intuitive touchscreen user interface.

Notification recipients 210 (e.g., cell phones that receive SMS-based notifications when certain events occur (or don't occur), email clients that receive an email message with similar information, etc.).

Custom-built clients (not shown) that access the iConnect web services XML API to interact with users' home security and self-monitoring information in new and unique ways. Such clients could include new types of mobile devices, or complex applications where integrated security system content is integrated into a broader set of application features.

[0057] In addition to the end-user clients, the iConnect servers 104 support PC browser-based Service Management clients that manage the ongoing operation of the overall service. These clients run applications that handle tasks such as provisioning, service monitoring, customer support and reporting.

[0058] There are numerous types of server components of the iConnect servers 104 of an embodiment including, but not limited to, the following: Business Components which manage information about all of the home security and self-monitoring devices; End-User Application Components which display that information for users and access the Business Components via published XML APIs; and Service Management Application Components which enable operators to administer the service (these components also access the Business Components via the XML APIs, and also via published SNMP MIBs).

[0059] The server components provide access to, and management of, the objects associated with an integrated security system installation. The top-level object is the "network." It is a location where a gateway 102 is located, and is also commonly referred to as a site or premises; the premises can include any type of structure (e.g., home, office, warehouse, etc.) at which a gateway 102 is located. Users can only access the networks to which they have been granted permission. Within a network, every object monitored by the gateway 102 is called a device. Devices include the sensors, cameras, home security panels and automation devices, as well as the controller or processor-based device running the gateway applications.

[0060] Various types of interactions are possible between the objects in a system. Automations define actions that occur as a result of a change in state of a device. For example, take a picture with the front entry camera when the front door sensor changes to "open". Notifications are messages sent to users to indicate that something has occurred, such as the front door going to "open" state, or has not occurred (referred to as an iWatch notification). Schedules define changes in device states that are to take place at predefined days and times. For example, set the security panel to "Armed" mode every weeknight at 11:00pm.

[0061] The iConnect Business Components are responsible for orchestrating all of the low-level service management activities for the integrated security system service. They define all of the users and devices associated with a network (site), analyze how the devices interact, and trigger associated actions (such as sending notifications to users). All changes in device states are monitored and logged. The Business Components also manage all interactions with external systems as required, including sending alarms and other related self-monitoring data to the home security Central

Monitoring System (CMS) 199. The Business Components are implemented as portable Java J2EE Servlets, but are not so limited.

[0062] The following iConnect Business Components manage the main elements of the integrated security system service, but the embodiment is not so limited:

A Registry Manager 220 defines and manages users and networks. This component is responsible for the creation, modification and termination of users and networks. It is also where a user's access to networks is defined.

A Network Manager 222 defines and manages security and self-monitoring devices that are deployed on a network (site). This component handles the creation, modification, deletion and configuration of the devices, as well as the creation of automations, schedules and notification rules associated with those devices.

A Data Manager 224 manages access to current and logged state data for an existing network and its devices. This component specifically does not provide any access to network management capabilities, such as adding new devices to a network, which are handled exclusively by the Network Manager 222.

To achieve optimal performance for all types of queries, data for current device states is stored separately from historical state data (a.k.a. "logs") in the database. A Log Data Manager 226 performs ongoing transfers of current device state data to the historical data log tables.

[0063] Additional iConnect Business Components handle direct communications with certain clients and other systems, for example:

An iHub Manager 228 directly manages all communications with gateway clients, including receiving information about device state changes, changing the configuration of devices, and pushing new versions of the gateway client to the hardware it is running on.

A Notification Manager 230 is responsible for sending all notifications to clients via SMS (mobile phone messages), email (via a relay server like an SMTP email server), etc.

An Alarm and CMS Manager 232 sends critical server-generated alarm events to the home security Central Monitoring Station (CMS) and manages all other communications of integrated security system service data to and from the CMS.

The Element Management System (EMS) 234 is an iControl Business Component that manages all activities associated with service installation, scaling and monitoring, and filters and packages service operations data for use by service management applications. The SNMP MIBs published by the EMS can also be incorporated into any third party monitoring system if desired.

[0064] The iConnect Business Components store information about the objects that they manage in the iControl Service Database 240 and in the iControl Content Store 242. The iControl Content Store is used to store media objects like video, photos and widget content, while the Service Database stores information about users, networks, and devices. Database interaction is performed via a JDBC interface. For security purposes, the Business Components manage all data storage and retrieval.

[0065] The iControl Business Components provide web services-based APIs that application components use to access the Business Components' capabilities. Functions of application components include presenting integrated security system service data to end-users, performing administrative duties, and integrating with external systems and back-office applications.

[0066] The primary published APIs for the iConnect Business Components include, but are not limited to, the following:

A Registry Manager API 252 provides access to the Registry Manager Business Component's functionality, allowing management of networks and users.

A Network Manager API 254 provides access to the Network Manager Business Component's functionality, allowing management of devices on a network.

A Data Manager API 256 provides access to the Data Manager Business Component's functionality, such as setting and retrieving (current and historical) data about device states.

A Provisioning API 258 provides a simple way to create new networks and configure initial default properties.

[0067] Each API of an embodiment includes two modes of access: Java API or XML API. The XML APIs are published as web services so that they can be easily accessed by applications or servers over a network. The Java APIs are a programmer-friendly wrapper for the XML APIs. Application components and integrations written in Java should generally

use the Java APIs rather than the XML APIs directly.

[0068] The iConnect Business Components also have an XML-based interface 260 for quickly adding support for new devices to the integrated security system. This interface 260, referred to as DeviceConnect 260, is a flexible, standards-based mechanism for defining the properties of new devices and how they can be managed. Although the format is flexible enough to allow the addition of any type of future device, pre-defined XML profiles are currently available for adding common types of devices such as sensors (SensorConnect), home security panels (PanelConnect) and IP cameras (CameraConnect).

[0069] The iConnect End-User Application Components deliver the user interfaces that run on the different types of clients supported by the integrated security system service. The components are written in portable Java J2EE technology (e.g., as Java Servlets, as JavaServer Pages (JSPs), etc.) and they all interact with the iControl Business Components via the published APIs.

[0070] The following End-User Application Components generate CSS-based HTML/JavaScript that is displayed on the target client. These applications can be dynamically branded with partner-specific logos and URL links (such as Customer Support, etc.). The End-User Application Components of an embodiment include, but are not limited to, the following:

An iControl Activation Application 270 that delivers the first application that a user sees when they set up the integrated security system service. This wizard-based web browser application securely associates a new user with a purchased gateway and the other devices included with it as a kit (if any). It primarily uses functionality published by the Provisioning API.

An iControl Web Portal Application 272 runs on PC browsers and delivers the web-based interface to the integrated security system service. This application allows users to manage their networks (e.g. add devices and create automations) as well as to view/change device states, and manage pictures and videos. Because of the wide scope of capabilities of this application, it uses three different Business Component APIs that include the Registry Manager API, Network Manager API, and Data Manager API, but the embodiment is not so limited.

An iControl Mobile Portal 274 is a small-footprint web-based interface that runs on mobile phones and PDAs. This interface is optimized for remote viewing of device states and pictures/videos rather than network management. As such, its interaction with the Business Components is primarily via the Data Manager API.

Custom portals and targeted client applications can be provided that leverage the same Business Component APIs used by the above applications.

A Content Manager Application Component 276 delivers content to a variety of clients. It sends multimedia-rich user interface components to widget container clients (both PC and browser-based), as well as to advanced touchscreen keypad clients. In addition to providing content directly to end-user devices, the Content Manager 276 provides widget-based user interface components to satisfy requests from other Application Components such as the iControl Web 272 and Mobile 274 portals.

[0071] A number of Application Components are responsible for overall management of the service. These pre-defined applications, referred to as Service Management Application Components, are configured to offer off-the-shelf solutions for production management of the integrated security system service including provisioning, overall service monitoring, customer support, and reporting, for example. The Service Management Application Components of an embodiment include, but are not limited to, the following:

A Service Management Application 280 allows service administrators to perform activities associated with service installation, scaling and monitoring/alerting. This application interacts heavily with the Element Management System (EMS) Business Component to execute its functionality, and also retrieves its monitoring data from that component via protocols such as SNMP MIBs.

A Kitting Application 282 is used by employees performing service provisioning tasks. This application allows home security and self-monitoring devices to be associated with gateways during the warehouse kitting process.

A CSR Application and Report Generator 284 is used by personnel supporting the integrated security system service, such as CSRs resolving end-user issues and employees enquiring about overall service usage. Pushes of new gateway firmware to deployed gateways is also managed by this application.

[0072] The iConnect servers 104 also support custom-built integrations with a service provider's existing OSS/BSS, CSR and service delivery systems 290. Such systems can access the iConnect web services XML API to transfer data to and from the iConnect servers 104. These types of integrations can compliment or replace the PC browser-based Service Management applications, depending on service provider needs.

[0073] As described above, the integrated security system of an embodiment includes a gateway, or iHub. The gateway of an embodiment includes a device that is deployed in the home or business and couples or connects the various third-party cameras, home security panels, sensors and devices to the iConnect server over a WAN connection as described in detail herein. The gateway couples to the home network and communicates directly with the home security panel in both wired and wireless sensor installations. The gateway is configured to be low-cost, reliable and thin so that it complements the integrated security system network-based architecture.

[0074] The gateway supports various wireless protocols and can interconnect with a wide range of home security control panels. Service providers and users can then extend the system's capabilities by adding IP cameras, lighting modules and additional security devices. The gateway is configurable to be integrated into many consumer appliances, including set-top boxes, routers and security panels. The small and efficient footprint of the gateway enables this portability and versatility, thereby simplifying and reducing the overall cost of the deployment.

[0075] **Figure 3** is a block diagram of the gateway 102 including gateway software or applications, under an embodiment. The gateway software architecture is relatively thin and efficient, thereby simplifying its integration into other consumer appliances such as set-top boxes, routers, touch screens and security panels. The software architecture also provides a high degree of security against unauthorized access. This section describes the various key components of the gateway software architecture.

[0076] The gateway application layer 302 is the main program that orchestrates the operations performed by the gateway. The Security Engine 304 provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine 304 of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.

Bi-directional authentication between the gateway and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.

Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The gateway provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.

802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.

A gateway-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying gateway-enabled devices have the knowledge that only a gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

[0077] As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

[0078] A Remote Firmware Download module 306 allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server 104, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Gateway firmware can be remotely download either for one gateway at a time, a group of gateways, or in batches.

[0079] The Automations engine 308 manages the user-defined rules of interaction between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

[0080] DeviceConnect 310 includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module 310 offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect 312 is provided for adding new sensors, CameraConnect 316 for adding IP cameras, and PanelConnect 314 for adding home security panels.

[0081] The Schedules engine 318 is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application. The Schedules Engine 318 then interfaces with SensorConnect 312 to ensure that scheduled events occur at precisely the desired time.

[0082] The Device Management module 320 is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters - to simplify the user experience and reduce the customer support burden, the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

[0083] The video routing engine 322 is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

[0084] **Figure 4** is a block diagram of components of the gateway 102, under an embodiment. Depending on the specific set of functionality desired by the service provider deploying the integrated security system service, the gateway 102 can use any of a number of processors 402, due to the small footprint of the gateway application firmware. In an embodiment, the gateway could include the Broadcom BCM5354 as the processor for example. In addition, the gateway 102 includes memory (e.g., FLASH 404, RAM 406, etc.) and any number of input/output (I/O) ports 408.

[0085] Referring to the WAN portion 410 of the gateway102 , the gateway 102 of an embodiment can communicate with the iConnect server using a number of communication types and/or protocols, for example Broadband 412, GPRS 414 and/or Public Switched Telephone Network (PTSN) 416 to name a few. In general, broadband communication 412 is the primary means of connection between the gateway 102 and the iConnect server 104 and the GPRS/CDMA 414 and/or PSTN 416 interfaces acts as backup for fault tolerance in case the user's broadband connection fails for whatever reason, but the embodiment is not so limited.

[0086] Referring to the LAN portion 420 of the gateway 102, various protocols and physical transceivers can be used to communicate to off-the-shelf sensors and cameras. The gateway 102 is protocol-agnostic and technology-agnostic and as such can easily support almost any device networking protocol. The gateway 102 can, for example, support GE and Honeywell security RF protocols 422, Z-Wave 424, serial (RS232 and RS485) 426 for direct connection to security panels as well as WiFi 428 (802.11b/g) for communication to WiFi cameras.

[0087] The system of an embodiment uses or includes a system user interface (SUI) that provides an iconic, at-a-glance representation of security system status. The SUI is for use across all client types as described above with reference to Figure 1. The SUI includes a number of display elements that are presented across all types of client devices used to monitor status of the security system. The clients of an embodiment include, but are not limited to, the iPhone®, the iPad®, a mobile portal, a web portal, and a touchscreen. The display elements of the SUI of an embodiment include, but are not limited to, an orb icon, text summary, security button, device and system warnings, interesting sensors, and quiet sensors, as described in detail below. The SUI thus provides system status summary information (e.g., security and sensors) uniformly across all clients. Additionally, the SUI provides consistent iconography, terminology, and display rules across all clients as well as consistent sensor and system detail across clients.

[0088] Following is a description of the various states of the iControl sensors, and how these states are indicated uniformly across all clients using the SUI and other sensor information displays such as sensor lists and timelines.

[0089] Regarding the display elements of the SUI, the orb icon visually indicates the current arm state and sensor status of a single site. **Figure 5** (collectively Figures 5A and 5B) shows the orb icon and corresponding text summary display elements, under an embodiment. Across all clients, when sensor detail is shown in a list or timeline, state is indicated using the proper icon, text summary and grouping. The orb icons and text summary elements of an embodiment generally represent system state 4001 to include the following states: "Disarmed" or "Subdisarmed; "Armed (Doors and Windows, Stay, Away, All, Night Stay, Instant, Motion, Maximum)"; "Disarmed", or "Subdisarmed" (sensor absent; sensor tripped; sensor tampered; low battery; uncleared alarm); "Armed (Doors and Windows, Stay, Away, All, Night Stay, Instant, Motion, Maximum)" (sensor absent; sensor tripped; sensor tampered; low battery); "Alarm"; and "No iHub Connection" (broadband offline, etc.) (no security panel connection). In addition to representing system state, the orb icons and text summary elements of an embodiment generally represent system status 4002 to include the following status: "All Quiet"; "Motion"; "Open"; "Open & Motion".

[0090] Using various combinations of system state 4001 and status 4002, the orb icons of an embodiment indicate or represent numerous system states.

[0091] When the system state 4001 is "Disarmed" or "Subdisarmed", the orb icons of an embodiment indicate or represent status 4002 as follows: Disarmed (status: all quiet) 4010 (e.g., icon color is green); Disarmed (status: motion) 4011 (e.g., icon color is green); Disarmed, (number of sensors open) Sensor(s) Open (status: open) 4012 (e.g., icon color is green, bottom region for sensor number is yellow); Disarmed, (number of sensors open) Sensor(s) Open (status: open and motion) 4013 (e.g., icon color is green, bottom region for sensor number is yellow).

[0092] When the system state 4001 is "Armed (Doors and Windows, Stay, Away, All, Night Stay, Instant, Motion, Maximum)", the orb icons of an embodiment indicate or represent status 4002 as follows: Armed Doors & Windows (status: all quiet) 4014 (e.g., icon color is red); Armed Doors & Windows (status: motion) 4015 (e.g., icon color is red); Armed Doors & Windows, (number of sensors open) Sensor(s) Open (status: open) 4016 (e.g., icon color is red, bottom region for sensor number is yellow); Armed Doors & Windows, (number of sensors open) Sensor(s) Open (status: open and motion) 4017 (e.g., icon color is red, bottom region for sensor number is yellow).

[0093] When the system state 4001 is "Disarmed", or "Subdisarmed" (sensor absent; sensor tripped; sensor tampered; low battery; uncleared alarm), the orb icons of an embodiment indicate or represent status 4002 as follows: Disarmed, sensor problem (status: all quiet) 4018 (e.g., icon color is green, badge in top region with "!" symbol is red); Disarmed, sensor problem (status: motion) 4019 (e.g., icon color is green, badge in top region with "!" symbol is red); Disarmed, sensor problem (status: open) 4020 (e.g., icon color is green, badge in top region with "!" symbol is red, bottom region for sensor number is yellow); Disarmed, sensor problem (status: open and motion) 4021 (e.g., icon color is green, badge in top region with "!" symbol is red, bottom region for sensor number is yellow).

[0094] When the system state 4001 is "Armed (Doors and Windows, Stay, Away, All, Night Stay, Instant, Motion, Maximum)" (sensor absent; sensor tripped; sensor tampered; low battery), the orb icons of an embodiment indicate or represent status 4002 as follows: Armed Doors & Windows, sensor problem (status: all quiet) 4022 (e.g., icon color is red, badge in top region with "!" symbol is red); Armed Doors & Windows, sensor problem (status: motion) 4023 (e.g., icon color is red, badge in top region with "!" symbol is red); Armed Doors & Windows, sensor problem (status: open) 4024 (e.g., icon color is red, badge in top region with "!" symbol is red, bottom region for sensor number is yellow); Armed Doors & Windows, sensor problem (status: open & motion) 4025 (e.g., icon color is red, badge in top region with "!" symbol is red, bottom region for sensor number is yellow).

[0095] When the system state 4001 is "Alarm", the orb icons of an embodiment indicate or represent status 4002 as follows: Armed Away/Stay, (alarm type) ALARM 4026 (e.g., icon color is red).

[0096] When the system state 4001 is "No iHub Connection" (broadband offline, etc.) (no security panel connection), the orb icons of an embodiment indicate or represent status 4002 as follows: Status Unavailable 4027 (e.g., icon color is grey).

[0097] When the client of an embodiment is a touchscreen, a mini orb is presented at the bottom of the touch screen in all widgets and settings screens. The mini orb is green when the security panel is disarmed, and it is red when the security panel is armed, but is not so limited. The form factor of the mini orb, and the text corresponding to the mini orb, is the same or similar to that described above as corresponding to the orb icon on the home screen.

[0098] The orb icons of an embodiment include motion indicators that animate to indicate motion detected by a corresponding sensor or detector. Furthermore, the orb icons of an embodiment show an animation during the exit delay when arming the security system and, additionally, indicate a countdown time showing the time remaining before the security system is fully armed. Moreover, selection of the orb of an embodiment causes additional information (e.g., list of sensors, etc.) of the security system and/or premise to be displayed.

[0099] The text summary display element of the SUI includes or displays information including a direct description of the current state of the security system to support the visual appearance of the orb icon. In an embodiment, two phrases are shown, including a first phrase for security state and a second phrase for sensor status (e.g., "Armed Stay. All Quiet"), as described herein. **Figure 6** is a table of security state and the corresponding sensor status displayed on the SUI, under an embodiment. The possible values for the text summary are (in priority order): Status Unavailable; if the security panel and control box are online and there are no current alarms, the text summary section is a combination of one phrase from each of the security state 4030 and the sensor status 4032. The security state 4030 of an embodiment is selected from among the following, but is not so limited: Armed Doors & Windows; Armed All; Armed Stay; Armed Away; Disarmed; Armed Maximum; Armed Night Stay; Armed Stay Instant; Armed Away Instant; Armed Motion; Subdisarmed. The sensor status 4032 of an embodiment is selected from among the following, but is not so limited: Uncleared Alarm; Sensor Tripped; Sensor Problem; Sensor(s) Bypassed; Motion; All Quiet; (number of sensors open) Sensor(s) Open.

[0100] The display elements of the SUI also include security buttons. The security buttons are used to control or arm/disarm the security panel. A single arm button (e.g., button labeled "Arm") can be used on the SUI of a first client device type (e.g., Touchscreen, iPhone®, etc.). Two different buttons (e.g., buttons labeled "Arm Away/Arm Stay" or "Arm All/Doors and Windows") can be used on the SUI of a second client device type (e.g., web portal, mobile portal, etc.). In either embodiment, when the system is armed, the arm button (e.g., "Arm", "Arm Stay" and "Arm Away") label will change to a "Disarm" label. If the system is in the process of arming, the button is disabled.

[0101] The display elements of the SUI include system and device warnings, as described above. The system and

device warning are informational warnings that are not associated with specific sensors, and involve more detail than can be displayed in the text summary display element. **Figure 7** is a table of system state and the corresponding icons and warning text displayed as system warnings on the SUI, under an embodiment. Where an icon is displayed, an embodiment uses a red color for the icon, but it is not so limited. The system states/warnings of an embodiment include, but are not limited to, the following: primary connection is broadband, broadband is down, cellular is being used/using cellular connection; primary connection is broadband, broadband and cellular are down/no cellular connection; primary connection is broadband, broadband is down, no cellular backup installed/broadband connection unknown; primary connection is cellular, cellular is down/no cellular connection; security panel not connected to AC power/security panel AC power loss; security panel low battery/security panel low battery; security panel tampered/security panel tampered; sensor(s) bypassed/sensor bypassed.

[0102] The device warnings of an embodiment include, but are not limited to, the following: camera(s) offline; light(s) offline; thermostat(s) offline. The device and system warnings may be combined into one box, or indicated separately in respective regions or portions of the SUI, depending on a type of the client device (e.g., combined into one box on a web portal or a mobile portal, but indicated in separate boxes on a Touchscreen or iPhone® device).

[0103] The device and system warnings display element is cumulative (e.g., built up in a list), but is not so limited. On the web and mobile portals the system and device warnings of an embodiment are combined into one area, but are not so limited. On the touchscreen device and mobile phone (e.g., iPhone®), device warnings are indicated separately so that, in an embodiment, the iPhone® tab bar and the touchscreen home screen indicate device warnings with icon badges, and system warnings are placed on the sensors screen.

[0104] The list of all sensors includes, but is not limited to, door/window sensors, motion detectors, smoke, flood, fire, glass break, etc. The list of all sensors of an embodiment does not include cameras or locks, or non-security related devices such as lights, thermostats, energy, water etc. The list of sensors is split into groups that, in an embodiment, include interesting sensors as a first group, and quiet sensors as a second group. The interesting sensor group is positioned above or sorted to the top portion of the sensor list and the quiet sensors are sorted to the bottom portion of the sensor list. Any sensor that is triggered (e.g. open, motion, etc.) is categorized as an interesting sensor and placed in the interesting sensor group and list. Additionally, other sensor states such as tampered, tripped, absent, installing, low battery, or bypassed make a sensor "interesting" regardless of their state.

[0105] **Figure 8** is a table of sensor state/sort order and the corresponding icon, sensor name and status text of the SUI, under an embodiment. Generally, the list of interesting sensors is sorted according to the following categories: motion; open/tripped; tampered; low battery; offline; installing; bypassed. Sensors are sorted alphabetically by sensor name within each category or interest type when multiple interesting sensors have the same state. The sensor state/sort order of an embodiment includes, but is not limited to, the following: breached & any sensor state (e.g., red icon) (interesting sensor); tripped (smoke, water, gas, freeze, etc.) (e.g., red icon) (interesting sensor); tampered (e.g., red icon) (interesting sensor); low battery (e.g., red icon) (interesting sensor); offline/AWOL (e.g., red icon) (interesting sensor); unknown (if the iHub or Security Panel is offline, all sensors have a grey diamond icon and "Unknown" for the status text) (e.g., grey icon) (interesting sensor); installing (e.g., grey icon) (interesting sensor); open (e.g., yellow icon) (interesting sensor); motion (e.g., yellow icon) (interesting sensor); bypassed (e.g., yellow or green icon) (interesting sensor); okay, closed, no motion (e.g., green icon) (quiet sensor).

[0106] The interesting sensors are shown or displayed with an icon. **Figure 9** shows icons of the interesting sensors, under an embodiment. A red diamond bang icon represents tamper, offline, bypassed, installing, and/or battery. A yellow triangle icon represents open or triggered. A wavy lines icon represents motion. It is possible for an interesting sensor to have a green/closed icon (e.g., any quiet sensor that has been bypassed).

[0107] Following the state icon and the sensor name an embodiment displays status text. The status of an embodiment includes, but is not limited to, the following: ALARM, (sensor state); tripped; tampered, (sensor state); low battery, (sensor state); offline; unknown; installing; bypassed, (sensor state). If a sensor is offline or tampered, it will show that text; otherwise the status text will show the tripped state: open, motion, tripped, etc. In addition, if a sensor is bypassed its state is "Bypassed, (sensor state)". For example, a bypassed motion sensor that has recently detected motion would have the status: "Motion, bypassed". If a sensor has a low battery its state does not change, but it still joins the interesting sensors group.

[0108] The quiet sensors include the remaining sensors that are not currently active, and so are not categorized as interesting sensors. Quiet sensor states of an embodiment include closed, no motion or otherwise not tripped or faulted. **Figure 10** shows the quiet sensor icon, under an embodiment. A green circle icon is a quiet sensor icon in an embodiment, and represents closed/no motion/okay/quiet. In addition to the state icon and sensor name, each quiet sensor shows status text as follows: if a door/window sensor is closed its state is "closed"; if a motion sensor has not recently detected motion then its state is "no motion"; other sensors, such as a smoke detector, indicate "quiet" or "okay". Quiet sensors are listed alphabetically.

[0109] The SUI of an embodiment includes control icons for a Home Management Mode (HMM). If the user deselects the "Set home management modes automatically" setting via the web portal, then the Home Management Mode (HMM)

screen will appear in the web and mobile Portals. **Figure 11** is an example Home Management Mode (HMM) screen presented via the web portal SUI, under an embodiment. The HMM screen includes an orb icon and corresponding text summary display elements, along with security buttons that control or arm/disarm the security panel. Furthermore, the HMM screen includes sensor status information (e.g., "Door", status is "open", icon is yellow; "Basement Motion", status is "motion", icon is yellow; "Family Room North Motion", status is "motion", icon is yellow; "Water", status is "okay", icon is green).

[0110] **Figure 12** is an example Home Management Mode (HMM) screen presented via the mobile portal SUI, under an embodiment. The HMM screen of the mobile portal includes an orb icon and corresponding text summary display elements, along with security buttons that control or arm/disarm the security panel.

[0111] The SUI of an embodiment is supported on numerous client types, for example, mobile telephones (e.g., iPhone®, etc.), client access via mobile portal, client access via web portal, and touchscreen to name a few. All clients types supported in an embodiment have the same status related sections, but their locations change slightly depending on the client. The status related sections of an embodiment include the following: orb; arm state/sensor summary; change mode; device summary and system warnings; interesting sensors; and quiet sensors.

[0112] **Figure 13** is a block diagram of an iPhone® client device SUI, under an embodiment. The client interface of the iPhone®, as one example client, has the orb on the security page. The text summary is below the orb. The security button (e.g., arm, disarm, etc.) is below the text summary. A tab bar is presented at the bottom of the screen. The SUI of an embodiment represents device warnings by the icons in the bottom horizontal tab bar. If a camera, light, lock, or thermostat is offline then a red circle will badge the corresponding icon in the tab bar. The number of offline devices is shown in the badge. **Figure 14** is a first example iPhone® client device SUI, under an embodiment. In this first example screenshot, the security page indicates one camera is offline, as indicated by the "1" in a "circle" badge displayed corresponding to the "camera" icon in the tab bar.

[0113] System warnings appear as a group in an area (e.g., yellow area) at the top of the sensor status screen. This area at the top of the sensor status screen appears only when there is a device or system warning; otherwise, it is not presented. Multiple messages appear as a vertical list with one message on each line. The yellow bar will grow in length to fit additional messages. If there are no system warnings then the interesting sensors group is at the top of the sensor status screen. Interesting sensors are presented below system warnings. Quiet sensors are presented below interesting sensors. **Figure 15** is a second example iPhone® client device SUI, under an embodiment. In this second example screenshot, the sensor status page indicates at least one sensor is bypassed, as indicated by the "Sensor(s) bypassed" message displayed at the top of the sensor status screen.

[0114] **Figure 16** is a block diagram of a mobile portal client device SUI, under an embodiment. The mobile portal of an embodiment comprises three (3) pages or screens presented to the client, including a summary page ("summary"), a security panel page ("security panel"), and a sensor status page ("sensors status"), but the embodiment is not so limited. The client interface of the mobile portal, as one example client, has the orb at the top of the summary page below the site name. The text summary is below the orb. The security buttons (e.g., arm, disarm, etc.) (plural on mobile portal) are on the security panel page (accessible via the "Security" link on the summary page). Device and system warnings are presented in an area (e.g., yellow area) below the text summary; in an embodiment this area is presented only when device or system warnings are present. Interesting sensors presented are at the top of the sensor status page. Quiet sensors are presented below interesting sensors on the sensor status page.

[0115] **Figure 17** is an example summary page or screen presented via the mobile portal SUI, under an embodiment. **Figure 18** is an example security panel page or screen presented via the mobile portal SUI, under an embodiment. **Figure 19** is an example sensor status page or screen presented via the mobile portal SUI, under an embodiment.

[0116] **Figure 20** is an example interface page or screen presented via the web portal SUI, under an embodiment. The client interface of the web portal, as one example client, has the orb in the center of the security widget. The text summary is below the orb. The security button (plurality in the web portal) is adjacent to the orb's right side. System warnings are presented in an area (e.g., yellow area) below the text summary; in an embodiment this area is presented only when device or system warnings are present. Multiple system warning messages are presented as a vertical list with one message on each line, and the area dedicated to the system warnings grows in length to accommodate additional messages. Interesting sensors span across the entire security widget below the text summary. Quiet sensors span across the entire security widget below interesting sensors.

[0117] **Figure 21** is an example summary page or screen presented via the touchscreen SUI, under an embodiment. The summary page of the touchscreen, as one example, has the orb in the center of the security bar. The text summary is split into sections or parts on each side of the orb. The security button is presented on the right side of the security bar.

[0118] In addition to the orb, text summary, and security button, the summary page also includes one or more icons that enable a transfer of content to and from the remote network, as described in detail herein. The touchscreen integrates the content with access and control of the security system. The content includes interactive content in the form of internet widgets. The summary page of an embodiment also comprises at least one icon enabling communication and control of the premise devices coupled to the subnetwork. The summary page also comprises one or more icons enabling

access to live video from a camera, wherein the camera is an Internet Protocol (IP) camera.

[0119] **Figure 22** is an example sensor status page or screen presented via the touchscreen SUI, under an embodiment. The sensor status page of the touchscreen, as one example, displays widget badges or icons representing device warnings. System warnings are at the top of the sensor status screen; in an embodiment this area is presented only when system warnings are present. Multiple system warning messages are presented as a vertical list with one message on each line, and the area dedicated to the system warnings grows in length to accommodate additional messages. Interesting sensors are below system warnings. Quiet sensors are below interesting sensors. The sensors screen also includes the mini-orb which indicates the arm state with text and color.

[0120] The integrated security system of an embodiment includes a component referred to herein as "Home View" that provides end users an at-a-glance representation of their home security status using the layout of their home. Like the System Icon or "orb" as described in detail herein, Home View is intended to complement a set of common elements including, but not limited to, the security text summary, arm/disarm button, system warnings, and sensor status list. These UI elements are in the primary display of every iControl client application, and Home View adds to that set of UI elements.

[0121] Home View can be an alternative to the System Icon, adding sensor location and information about other devices like lights, thermostats, cameras, locks, and energy devices, to name a few. Home View is an optional view, and users who set up Home View are able to switch between the System Icon view and Home View. Home View provides the user or installer a way to express the floor plans of their home, where the layout of Home View is representational and, as such, is not meant to be a precise rendering of a home. The rendering of Home View can vary on each device depending on screen size and display capabilities.

[0122] **Figure 23** is an example Home View display 4000, under an embodiment. Using this example, Home View 4000 expresses or represents with a display the floor plan 4002 of a relatively large premise (e.g., home) or structure (e.g., 5 rooms wide and 5 rooms tall). Home View accommodates multi-story homes or structures (e.g., 4 stories). This mechanism can also be used to express other parts of a property, such as outbuildings. Home View allows the user to see all devices 4010 present on a selected floor, and indications if other floors have interesting/active devices (such as an open door, or a light that is on).

[0123] Home View information defined on one client affects all clients. In other words, if a change is made to the floor plans on one client, all clients display that change if they are using Home View. Home View is provided on the iPhone, and is also supported on one or more clients common to all users (web portal and/or touch screen).

[0124] Home View of an embodiment includes an editing tool that supports basic sensors and common devices. Using the sensor state display of Home View, and while editing, the user can position each sensor device on each floor, and the sensor icon is displayed over each floor plan.

[0125] Under an embodiment and as further described below, basic device states are represented by device and/or sensor state icons in Home View. **Figure 24** shows a table of sensor state icons displayed on the Home View floor plan, under an embodiment. The sensor states displayed in an embodiment include, but are not limited to, the following: breached or alarmed, tripped, or tampered (e.g., red icon) (interesting sensor); low battery (e.g., red icon) (interesting sensor); offline/AWOL (e.g., red icon) (interesting sensor); unknown (if the iHub or Security Panel is offline, all sensors have a grey diamond icon and "Unknown" for the status text) (e.g., grey icon) (interesting sensor); installing (e.g., grey icon) (interesting sensor); open door/window (e.g., yellow icon) (interesting sensor); motion sensor active (e.g., yellow icon) (interesting sensor); okay, closed, no motion (e.g., green icon) (quiet sensor). The states of each sensor icon of an embodiment are updated periodically (typically 15-30 seconds) to reflect their status.

[0126] A touch sensed anywhere in Home View navigates the UI to the sensor list available in System Icon view. The user can also touch any sensor icon in Home View and see a popup display showing the sensor name. The popup box is presented above the sensor with a connector pointing to and indicating the sensor selected. If the sensor is at the top of the screen, the popup box may appear below the sensor with a connector pointing up to and indicating the selected sensor. The popup box also includes a "more" button for navigating to detailed information about that sensor (in this case, sensor history). An embodiment presents sensor icon, name, and status text, and the last event for that sensor, plus a navigation arrow e.g., (a blue circle on some UIs) the selection of which switches screens to the sensor detail or history (same as clicking sensor name in each client).

[0127] Using the device state display of Home View, a set of device and/or sensor icons can be placed on each floor. **Figure 25** shows example sensor status and device icons of Home View, under an embodiment. The device icons include, but are not limited to, icons representing lights, thermostats, cameras, locks, and energy devices, to name a few. Each of the device icons change states in the same way they change in their device list. These states include offline, installing, quiet, and active states but are not so limited. In an embodiment, cameras do no indicate an active state with an icon change. When the user touches a device icon, the device name pops up or is displayed. The popup box includes a "more" button for navigating to more information about that device as follows: camera icon (the popup box "more" button jumps to live video for that camera; exiting live video returns to Home View); lights, thermostats, energy, locks icon ("more" button jumps to the detail screen for controlling each device; the back buttons from those screens behave

as they always do).

[0128] Home View visually indicates changes in device state under an embodiment. Under one embodiment device icons represent an underlying device component and its current state by modeling the device itself. For example (and as set forth in Figure 25), an iconic image of a lock represents an actual lock device. As another example (and as set forth in Figure 25), an iconic image of a lamp represents an actual lamp device monitored/controlled by the integrated security system. Home View may then use the device icon itself to indicate change in state. For example, Home View may express an unlocked or open status of a lock device by replacing the symbol of a closed or engaged lock with a symbol clearly depicting a lock that is unlocked or disengaged. As another example, Home View may indicate an inactive lamp device by replacing an iconic lamp representation in an "on" state (i.e., indicating emanation of light) with a darkened lamp representation (using a darkened lamp shade) indicating an "off" status. In other words, change in appearance of the device icon expresses a change in state of the underlying device.

[0129] Under another embodiment a generic sensor icon may be used to represent a device and its operational status. For example, a user may use an edit feature of Home View (described in greater detail below) to place a generic sensor icon on the Home View floor plan. When the user touches the icon on an iPhone client or mouses over the icon in a web application, the name/type of device appears above the icon (along with other relevant information and options as further described herein). The icon itself then displays status by shifting to a state specific status icon. As described above, Home View may use one of the status icons described in Figure 24 as appropriate to the operational status of the represented device but is not so limited.

[0130] Under another embodiment, Home View may indicate a change in state of the device by simply replacing the device icon with a status icon. For example, a lock device may be offline at which time the Home View would replace the lock icon representation with a status icon representation that indicates an offline status. The offline status icon may correspond to the offline status symbol set forth in Figure 24 but is not so limited.

[0131] Under another embodiment, Home View may visually superimpose or visually annotate a device icon with status representations. As an example, Home View may visually annotate a lock device icon with a status icon to indicate its current operational status. The Home View may use the status icons described in Figure 24 to visually append status information to device representations but is not so limited. Under an embodiment, the Home View may use smaller representations of such icons to serve as status badges on a portion of the device icons. The Home View may also superimpose a partially transparent status icon as a palimpsest layer over the device icon or alternatively integrate a partially transparent status icon into the device icon as a watermark representation. Home View may use one of the status icons described in Figure 24 as appropriate to the operational status of the represented device but is not so limited.

[0132] Under yet another embodiment, Home View may use any combination and/or manipulation of status/device icons to represent operational status of system components.

[0133] If more than one floor has been defined in Layout mode of Home View, thumbnails on a portion of the display indicate that there are floors above or below the current one, and a means provided to switch floors. Figure 26 shows a Home View display 4100 that includes indicators 4101/4102 for multiple floors, under an embodiment. In this example, two icons are presented to indicate a first (lower) floor 4101 and a second (upper) floor 4102. The currently-displayed floor 4101 (e.g., first (lower) floor) is outlined in white or otherwise highlighted. The last-viewed floor will be remembered across sessions.

[0134] The display of indicators for multiple floors through a mobile portal includes numbered links on a portion of the display (e.g., right), starting from "1". The currently-displayed floor is shown as bold, and not a link, as in:

Floor: 1 **2** 3

[0135] Like the System Icon, Home View indicates the overall system state by using background color. For accessibility, this may also be presented using corresponding text located adjacent to the icon. **Figure 27** shows the system states along with the corresponding Home View display and system or orb icon, under an embodiment. Across all clients, system state is indicated using a representative color. The disarmed or subdisarmed system state is displayed in Home View using a green background or green border 4202 on the floor plan. The armed (any type) system state is displayed in Home View using a red background or red border 4204 on the floor plan. The alarm system state is displayed in Home View using a red background (with or without black diagonal stripes) 4206 on the floor plan. The offline (iHub or panel) system state is displayed in Home View using a grey background 4208 on the floor plan.

[0136] The System Icon of some client device UIs (e.g., the iPhone, the Touch Screen) also includes a warning badge to indicate that there are warnings to see in the sensor list. In Home View, a general warning indicator 4302 is shown in a region (e.g., on one side) of the Home View floor display. **Figure 28** shows a Home View floor display (disarmed 4202) that includes a warning indicator 4302, under an embodiment. The Home View display and warning indicator correspond to the system icon or "orb" set forth in the upper left corner of Figure 28.

[0137] The use of Home View as a user interface includes Summary Text as described in detail herein, and the Summary Text provides definitive information on the current arm state, and a summary of any sensor issues. Additionally,

the system arm/disarm buttons are displayed separately. **Figure 29** shows an example of the Home View 4402 using the iPhone security tab, under an embodiment.. System state information 4404 is displayed ("Disarmed. 1 Sensor Open"), and an "Arm" button 4406 is displayed by which a user arms the system.

[0138] Home View is an alternative to the System Icon, as described herein, and is configured via site settings. Each application retains the user's preferred mode across sessions. **Figure 30** shows an example screen for site Settings 4500, under an embodiment. The Settings screen 4500 includes a list of sites 4502 that can be selected, along with a Sign Out button 4504. The Settings screen 4500 also includes a Security Tab Options button 4506. Selection of the Security Tab Options button 4506 displays the Security Tab Options screen 4600.

[0139] **Figure 31** shows an example screen for Security Tab Options 4600, under an embodiment. The Security Tab Options screen 4600 displays a list of options 4602 to select what the security tab displays (i.e., the System Icon display or the Home View display), along with an Edit Home View button 4604. When the user first attempts to switch to Home View from the Security Tab Options screen 4600 the following modal dialog is displayed: "Home View must be set up before use." This dialog includes but is not limited to the following two buttons: "Set Up Now" and "Cancel".

[0140] Any time the user wants to alter their Home View floor plans or device positions, they can choose Settings 4500, then select the Security Tab Options button 4506, then the Edit Home View button 4604. If a device has been deleted, then the Home View display code removes it from the device settings table. If a device has been installed or added to the system, it does not automatically appear in Home View, but it will be available in Edit Home View mode, ready to be placed on a floor.

[0141] The Home View mode of an embodiment includes an editor or Edit Mode. On the Settings screen 4500, the user can select Security Tab Options 4506, then Edit Home View 4604, as described above. This puts the user in Edit mode, where they can make changes to device positions, floor plans, and add/remove floors, for example. When editing is complete, selection of a "Done" button on the screen returns a user to the Security Tab Options screen 4600. If the user has made changes, then a dialog slides up that includes buttons for "Save Changes", "Don't Save", and "Cancel". Once saved, Home View data is saved on the iHub/iServer with other site settings, and can appear in any client that has Home View enabled for display.

[0142] When the user first enters Edit mode, the user selects a basic floor plan which defines the perimeter shape of each floor of the premise. Figure 32 shows an example "Add Floor" screen for use in selecting a floor plan, under an embodiment. Numerous floor plan selections are presented in a region of the screen labeled "Select a floor plan" 4702, and the floor plan selections 4702 of an embodiment comprise, but are not limited to, the following: square; horizontal; vertical; four different L-shapes; four different U-shapes; four different zigzag shapes. The title bar of the "Add Floor" screen 4700 includes a Cancel button 4704. At the point when there are no floors, there are no other buttons.

[0143] Upon selection of a basic floor plan, the editor is displayed. **Figure 33** shows an "Edit Home View" screen 4800 of the editor, under an embodiment. The title bar includes an add floor button [+] 4802. In this example only one floor is defined, so there is no delete button (cannot delete the last floor). In addition to adding and deleting floors, the editor of an embodiment displays selection buttons 4810-4814 for three editing modes: Devices mode 4810 (used for placing devices on each floor); Walls mode 4812 (used for adding or changing walls); Erase mode 4814 (used for deleting walls). If the default floor plan matches the user's home, then the user has only to position devices on that floor. However, if the user wishes to modify a floor plan or define interiors then the Walls Mode and Erase mode are used to make changes.

[0144] Devices are represented by icons in the editor, and the icons can be positioned by dragging to the appropriate location on the floor plan 4804. Below the displayed floor 4804 is a dock area 4806 that includes all devices displayed in rows. The user can drag a device to any tile on the floor 4804 that does not already contain a device icon. Devices can also be dragged back off the floor 4804 and onto the dock 4806. To identify a device the user can tap a device icon or start dragging and the name will appear above the device icon. **Figure 34** shows an example of dragging a device icon during which a name of the device 4900 ("Front Door") is displayed, under an embodiment. Devices are not required to be placed on floors, and any devices left in the dock 4806 are ignored when Home View is displayed. These can be added to any floor at a subsequent time. Newly installed devices are also left on the dock 4806, ready to be placed when editing.

[0145] The dock 4806 has a grid of tiles, similar to the floor plans. The user can move devices around on that grid. Upon exiting the editor and then returning, the dock is drawn in ordered rows. Devices of an embodiment are placed every-other-tile, up to 11 devices per row and up to 3 rows for a total of up to 33 devices on screen, but are not so limited. If the site has more than 33 devices in the dock, they are not shown until some devices are moved onto the floor, so that the dock condenses after each device is placed on a floor.

[0146] The selected floor plan provides a basic perimeter for the floor. If the user wishes to change the default perimeter walls or define interior walls, the user can switch to Walls mode. The user can tap any tile to customize that tile, and tapping a tile cycles the tile through twelve different tile shapes. Tile cycles start with the best-fit tile based on context, then cycle through all possible tile shapes in best-fit order. For example, if the user taps a blank tile with a horizontal line to the right and a vertical line below it, then the first tile drawn will be a corner tile that connects those lines, then a tile that connects one line, then the other line, etc.

[0147] For example, a typical task is to draw an interior wall. Each tile should require only one tap to draw as a user progresses across tiles of the floor plan. **Figure 35** is an example of a U-shaped floor plan 5000 customized by changing interior tiles to define walls 5002, under an embodiment.

[0148] The editor of an embodiment includes a Walls mode and an Erase mode, as described above. In the Walls mode and the Erase mode the device icons are hidden. Erase mode is used to change wall tiles into blank tiles, to remove mistakes, and/or begin to move a wall. For example, a user wanting to narrow a rectangular floor plan by moving an entire wall inward first switches to Erase mode and taps every tile of the vertical wall they wish to move, and then switches to Walls mode and taps every tile where they wish a wall to be placed.

[0149] An embodiment may adopt an alternative floor plan editing scheme in the form of a commercial diagramming tool. The alternative approach replaces the tile based diagramming described above with a vector based graphics approach. A user may choose design primitives to establish and subsequently manipulate (via touch/drag interactions or keyboard/mouse operations) basic floor plan shapes and representations. Such approach may incorporate a "free hand" ability to trace lines or other floor plan elements (via touch/drag interactions or keyboard/mouse operations).

[0150] While editing tiles or positioning sensors, more precision may be needed in which case the user can toggle the zoom level of the editor (includes the dock) in any edit mode. To zoom to 300%, for example, the user taps the + magnifying glass 5004, and to return to 100% zoom, the user taps the - magnifying glass 5102. If there are multiple floors, tapping a floor thumbnail returns to 100% zoom. Once zoomed, the user scrolls around the floor by a dragging operation. **Figure 36** shows an example in which the zoom level is increased and dragging has been used to focus on a sensor location 5100, under an embodiment. When zoomed in, if the user touches and drags a device, the device moves and not the floor. If the user taps and drags a tile, the floor scrolls around and the tile is not altered.

[0151] Home View of an embodiment supports up to four (4) floors but is not so limited. These floors can also be used for other physical spaces, such as outbuildings or garages for example, so floor numbering is generally avoided. To define a new floor in Edit mode, the user touches a + button 4802 at the top of the screen and the Add Floor page appears. **Figure 37** is an example "Add Floor" page 5200, under an embodiment. If at least one floor has previously been defined, a new control appears to help add this new floor above ("Add Above" 5202) or below ("Add Below" 5204) the current floor. The default option adds the new floor above ("Add Above") the current floor. By selecting a floor in Edit mode, touching +, and changing this control in the Add Floor page, the user can add basements, insert floors etc.

[0152] When more than one floor is defined in Home View, some differences appear on the Edit Home View screen. Among the changes, a column of floor thumbnails appears on the right portion of the screen. The currently selected floor thumbnail is highlighted, and the user can tap any floor to switch to that floor. For example, the user can move a device to the dock, switch floors by touching the other floor thumbnail, then drag the device onto the new floor. **Figure 38** is an example Edit Home View screen 5300 showing the floor thumbnails 5302/5304 for use in selecting a floor, under an embodiment.

[0153] An additional change displayed on the Edit Home View screen includes the display of a delete floor button [-] in the title bar of the editor, to the right of the add floor button [+]. If more than one floor is defined, the user selects the [-] button to delete the current floor. The user is prompted with a warning with the options to Delete Floor or Cancel 5404. **Figure 39** shows the Edit Home View screen 5400 with a delete floor selector 5402, under an embodiment.

[0154] Selection of the Done button on the Edit Home View screen allows the user to exit the editor. If upon selecting the Done button the user has made changes to the floors or device locations, the user is prompted to save the changes before exiting back to the Settings screen. **Figure 40** is an example Edit Home View screen 5500 displaying options to "Save" 5502 and "Don't Save" 5504 changes following selection of the Done button, under an embodiment.

[0155] For each premise, Home View allows users to define the floors of their home and the locations of all devices on those floors using the Edit Home View layout editor described above. The output of the layout editor includes two strings that are stored in site preferences on the server. All client applications share this static definition of the site layout, and locally combine it with the current state of the sensors and panel to produce a graphical view.

[0156] Home View is presented in an embodiment using tiles, and allows a user to define up to a pre-specified number of floors (e.g., four floors, etc.), but is not so limited. Each floor in Home View is presented as a layout of tiles in two layers or structures. A first layer, or bottom layer, is a static layout of a single floor (e.g., 19 tiles by 19 tiles, etc.). **Figure 41** is an example of the floor grid data, under an embodiment. A second layer, or top layer, is a set of sensor/device icons (states changing) placed or overlaid over the grid (first layer). **Figure 42** is an example sensor hash table for a single-floor site, under an embodiment.

[0157] The server (e.g., iServer) of an embodiment stores the two structures in two variables in site preferences, but the embodiment is not so limited. A first variable comprises a series of floor layouts corresponding to the number of floors. Each floor layout is a floor grid represented by a single string of characters (e.g., 19x19 or 361 ASCII characters), with one character corresponding to each tile as described above.

[0158] The homeViewLayouts preference strings represents between 1 and 4 tile grids. Each tile grid is 19 tiles by 19 tiles for a total of 361 tiles. The grids comprise odd numbers to support centering of walls. The first 361 tiles represent the first floor of the premise. If there are multiple floors, the next 361 tiles represent the second floor of the premise.

Therefore, homeViewLayouts length is 361 characters (premise having one floor), 722 characters (premise having two floors), 1083 characters (premise having three floors), or 1444 characters (premise having four floors). **Figure 43** shows an example homeViewLayouts string, under an embodiment.

[0159] A second variable comprises a hash table mapping specific tiles to sensors, separated by commas, and every sensor is represented. A homeViewDevice preference string represents such information and comprises key,value pairs separated by commas. As example homeViewDevices character string is as follows:

homeViewDevices="3,zone2,74,zone5,88,zone1,129,zone2,166, cameraFront Door Cam,200,lightUpstairs Light 2,226,thermoUpstairs".

[0160] The key of the key,value pair is an integer representing the absolute offset into the homeViewLayouts array. The value of the key,value pair represents a way to precisely identify the device. For sensors, this value is "zone" followed by the zone ID. For example, if the front door (zone id 7) is on the third tile over, then the key value pair is 2,zone7 (e.g., zero-based offset).

[0161] Each tile set includes twelve basic shapes. The shapes of an embodiment include, but are not limited to the following: empty; horizontal wall; vertical wall; top left corner; top right corner; bottom left corner; bottom right corner; T-shape down; T-shape right; T-shape up; T-shape left; 4 corner shape. **Figure 44** shows the twelve shapes of a tile set, under an embodiment. Wall lines are centered within each tile to ensure alignment. The user draws the floor(s) of their premise using the shapes, and the set of tile shapes is used while editing (generally blue, like blueprints), and for two of the rendered states of the security system: when alarmed (red and black striped) and when offline (gray tiles).

[0162] As stated above, the user defines the walls of each floor of their home using twelve basic tile shapes. However, when a floor is rendered, the building exteriors should be readily distinguished from the interiors. For rendering Home View in armed and disarmed states, algorithms determine the interior of the home and compute which tiles are transparent and which tiles are filled. For perimeter walls, the algorithm clears the exterior side but not the interior side. A larger set of tiles is used to handle all possible transparent/filled tile renderings. **Figure 45** shows the tile shapes and corresponding fill options for rendered tiles, under an embodiment.

[0163] As stated above, the user defines the walls of each floor of their home using twelve basic tile shapes. However, when a floor is rendered, the building exteriors should be readily distinguished from the interiors. This achieved when the editor is exited and tiles exterior to each building are replaced with transparent tiles. Similarly, tiles with walls facing the exterior are replaced with tiles where the exterior portions are transparent.

[0164] **Figure 46** is an example tile rendering for a room of a premise, under an embodiment. In this example, there are two perimeter versions of the top-right corner tile "t", and one perimeter version is filled on the bottom right (tile "u"), and one perimeter version is filled on the top left (tile "U").

[0165] A description follows for operation of the algorithm for determining an interior and an exterior. The algorithms generate a list of all tiles on the edge of each floor that are empty (top row, bottom row, left column, right column, up to 19+19+2*17=72 tiles per floor). With each tile, a function is called to clear the tile. In that function, the empty tile is changed to an empty exterior tile (for example, "e" changes to "E"). The algorithm then examines the four tiles on each side (top, right, bottom, left) of the current tile and, if they are non-empty, replaces them with tiles where the side facing the current tile is transparent. The algorithm then examines the four tiles diagonal to this exterior tile and, if they are non-empty and have a corner (T shapes, plus shape, corners), replaces them with tiles where the corner facing the current tile is transparent. A list is generated comprising any of the four tiles on each side (top, right, bottom, left) of the current tile that are empty. With each empty tile, a recursive function is called and the process repeats as described above.

[0166] In order to avoid stepping into "doors", the algorithm does not call the recursive function in response to empty tiles if there are wall edges touching the current tile. For example, the process only recurses down to an empty tile if the tiles to the right and left are not horizontal tiles (or similar) touching the current tile. This works for doors one and two tiles wide; wider openings get filled.

[0167] The fully computed floor definition is stored in the gateway (e.g., iHub) and/or server (e.g., iServer) but is not so limited. If the Home View editor is used, these computed tiles can be converted back to the twelve-tile set while editing. The Home View data output from Edit mode is checked to ensure integrity of parameters, for example: the number of tiles (and number of floors) is correct; the tile data only includes valid tile characters; all sensors and devices still exist. At the time Home View is rendered, the same checks are again performed to verify data integrity. If any checks fail, the user is presented a dialog, and the preference returns to the System Icon (the "orb"). Essentially the feature is turned off for display, but the data is still there until edited. If the user tries to edit home view and the data is corrupted, they are given the option to reset the data and start over.

[0168] An alternative embodiment of Home View also provides methods for generating and presenting floor plans and icons representing sensors overlaid on a floor plan for a home, thereby enabling users to quickly see the state of each sensor (such as open doors, status of lights and thermostats, etc.), and click on any sensor to get more information about that sensor. As described in detail herein, **Figure 24** shows a table of sensor state icons displayed on the Home

View floor plan, and **Figure 25** shows example sensor status and device icons of Home View, under an embodiment. The device icons include, but are not limited to, icons representing lights, thermostats, cameras, locks, and energy devices, to name a few. Each of the device icons change states in the same way they change in their device list. These states include offline, installing, quiet, and active states but are not so limited. The sensor states displayed in an embodiment include, but are not limited to, the following: breached or alarmed, tripped, or tampered (e.g., red icon) (interesting sensor); low battery (e.g., red icon) (interesting sensor); offline/AWOL (e.g., red icon) (interesting sensor); unknown (if the iHub or Security Panel is offline, all sensors have a grey diamond icon and "Unknown" for the status text) (e.g., grey icon) (interesting sensor); installing (e.g., grey icon) (interesting sensor); open door/window (e.g., yellow icon) (interesting sensor); motion sensor active (e.g., yellow icon) (interesting sensor); okay, closed, no motion (e.g., green icon) (quiet sensor). The states of each sensor icon of an embodiment are updated periodically (typically 15-30 seconds) to reflect their status.

[0169] A touch sensed anywhere in Home View navigates the user interface to the sensor list available in the System Icon view. The sensor icons of an embodiment update periodically (e.g., frequently) to reflect their current status (e.g., an open window). The sensor icon also represents the "health" of that sensor (offline, low battery etc.). A user can hover over (in desktop web browser) or tap (tablet/touch device) any sensor icon and see a popup display showing the name, state, and the last event for that sensor. **Figure 47** is an example popup display in response to hovering near/adjacent a sensor icon (e.g., "Garage" sensor), under an embodiment. If the device is at the very top of the screen, the popup box may appear below the sensor. Alternatively, if the device is on the edge of the screen the popup box may be pushed inward or displayed in another portion of the interface. Clicking (desktop) or double-tapping (tablets) in regions of the display causes the system to navigate to sensor history. When the interface is displayed on an iPhone, for example, the popup box may also have a blue "more" button for that same navigation.

[0170] If more than one floor has been defined in Layout mode of Home View, the display includes thumbnails on a portion of the display that indicate the existence of floors above or below the current one, and a process to switch floors. **Figure 48** shows a Home View display that includes a floor plan display 4800 of a selected floor along with indicators 4801/4802 for multiple floors, under an embodiment. In this example, two icons are presented to indicate a first (lower) floor 4801 and a second (upper) floor 4802. Alternatively, other notations (e.g., dots, etc.) can be used to indicate multiple floors. The currently-displayed floor 4801 (e.g., first (lower) floor) is highlighted. The last-viewed floor will be remembered across sessions. When accessing Home View via a mobile portal, the display of indicators for multiple floors through the mobile portal includes numbered links on a portion of the display (e.g., right), starting from "1". The currently-displayed floor is shown as bold, and not a link, for example:

Floor: 1 **2** 3

[0171] The use of Home View as a user interface includes a system icon or Summary Text that provides definitive information on the current arm state, and a summary of any sensor issues. Additionally, the system arm/disarm buttons are displayed separately. **Figure 49** shows an example of the Home View user interface displayed via a mobile device (e.g., iPhone), under an embodiment. The user interface 4900 includes a floor plan display 4901 of a selected floor along with indicators 4902 for selecting among corresponding multiple floors of a building. System state information is displayed 4903 ("Disarmed. All Quiet."), and an "Arm" button 4904 is displayed by which a user controls arming of the system. A toolbar 4905 is included by which a user selects a device type (e.g., security, cameras, lights, thermostats, etc.) for which status and control information is available via Home View.

[0172] Home View is configured via site settings as described in detail herein. Each application retains or remembers the user's preferred mode across sessions. **Figure 50** shows an example of a Settings page of Home View, under an embodiment. The Settings page includes a Sites list, a "Home View" button 5001, and a corresponding On/Off switch 5002. For site owners, there is also a "Set Up Home View" button (not shown), the selection of which directs the system to the editor. Once Home View is defined by a user, the interface presents the "Set Up Home View" button as an "Edit Home View" button 5003. In the web portal of an embodiment, Home View can be enabled and edited using a Customize link on the Summary tab. Users can check the box to show Home View, and site owners will have an Edit button.

[0173] Any time the user wants to alter their Home View floor plans or device positions, they can choose Settings and then select the Edit Home View button. If a device has been deleted, then the Home View display code removes it from the device settings table. If a device has been installed or added to the system, it does not automatically appear in Home View, but it will be available in Edit Home View mode, ready to be placed on a floor.

[0174] The Home View mode of an embodiment includes an editor or Edit Mode, as described in detail herein. On the Settings screen, the user can select the Edit Home View button, as described above. This puts the user in Edit mode, where they can make changes to device positions, floor plans, labels, and add/remove floors, for example. When editing is complete, selection of a "Done" button on the screen returns a user to the Security Tab Options screen. If the user has made changes, then a dialog slides up that includes buttons for "Save Changes", "Don't Save", and "Cancel". Once saved, Home View data is saved on the iHub/iServer with other site settings, and can appear in any client that has Home

View enabled for display.

[0175] When the user first enters Edit mode, the user selects a basic floor plan that defines the perimeter shape of each floor of the premises. **Figure 51** shows an example "Home View Setup" editor page 5100 for use in selecting a floor plan, under an embodiment. Numerous floor plan selections 5102 are presented in a region of the screen labeled "Select a floor plan" 5102, and the floor plan selections of an embodiment comprise, but are not limited to, the following: square; horizontal; vertical; numerous different L-shapes; numerous different U-shapes; numerous different zigzag shapes. The title bar 5103 is labeled "Home View Setup" and includes a Back button 5104.

[0176] Upon selection of a basic floor plan, the selected floor plan is displayed. **Figure 52** shows a "Home View Setup" editor screen 5200 with a selected floor plan 5201, under an embodiment. The editor screen 5200 displays a selected floor plan 5201, and includes a device dock 5202, or dock 5202, that includes devices 5203 as represented by icons. The editor 5200 includes an "Options" 5204 icon, the selection of which presents editing options. For example, **Figure 59** shows a Home View Setup page 5900 with options displayed, under an embodiment. The editor 5200 includes numerous editing operations including, but not limited to, positioning devices (dragging device icons from the dock and placing devices on the floor), editing walls (adding new horizontal or vertical walls, or deleting existing walls), and adding or editing labels (changing or deleting room labels). If the default floor plan matches the user's home, then the user has only to position devices on that floor plan. Optionally, the user can add labels. If the user wishes to modify a floor plan or define interiors, however, then walls can be drawn or erased.

[0177] Devices are represented by icons that are presented in a device icon dock 5202 of the interface. The interface includes a dock area that includes device icons displayed in rows. Device icons are positioned on the floor plan by dragging them from the dock to the appropriate location on the floor plan. To identify a device the user can tap a device icon or start dragging the device and the name will appear above the device icon. Devices can also be dragged back off the floor and into the dock. Furthermore, labels can be added to devices of the home (e.g., front door 5301). **Figure 53** shows an example editor screen 5300 for which a label 5301 with a name of the device ("Front Door") is displayed, under an embodiment.

[0178] There is no requirement under an embodiment for devices to be placed on floors, and any device left in the dock is ignored when Home View is displayed. The devices remaining in the dock can be added to any floor of a floor plan at a subsequent time. Newly installed devices are also left on the dock, ready to be placed when editing. The dock of an embodiment is rendered in ordered rows, and the dock can be scrolled vertically to access all devices in the dock.

[0179] The selected floor plan of Home View provides a basic perimeter for the floor, but is not so limited. A user wishing to draw new perimeter walls or define interior walls drags across the grid lines to create new walls. The user deletes walls in much the same way by dragging along the gridline over an existing wall. The process of erasing old walls then drawing new ones can be used to "move" a wall but the embodiment is not so limited. For example, the process of narrowing a rectangular floor plan by moving an entire wall inward includes dragging over the vertical wall that is to be moved and then dragging on the new gridline where the wall is to be placed. **Figure 54** shows a Home View Setup page 5400 with a selected floor plan 5201 that has been edited to add numerous interior walls 5401, under an embodiment.

[0180] A user can edit labels on any location of a floor plan, where editing includes adding, editing, and deleting labels. **Figure 55** shows a Home View Setup page with a label editing prompt 5501, under an embodiment. To add a new label, the user selects the option to add a room label and then touches a location for that label. In response the interface presents a label editing prompt 5501 for the label text. In order to edit an existing label, the user taps that location and the same label editing prompt 5501 is presented for use in editing the label. To delete a label the user clears the text.

[0181] The floor plan editing of an embodiment includes zoom editing in order to offer increased precision when editing. **Figure 56** shows a Home View Setup page 5600 in a zoomed editing mode to zoom on one room 5601 in a building, under an embodiment. The user edits in a zoomed mode by tapping a magnifying glass icon 5206 displayed on Home View Setup. When using zoom editing, the magnifying glass icon 5206 of the Home View Setup page is replaced with a floor plan icon 5602 displaying the entire floor plan with an overlay 5603 showing the region of the floor plan on which the user has zoomed. Once zoomed, the user scrolls around the floor by dragging the view rectangle in the zoom thumbnail area. Tapping the zoom thumbnail area returns the display to full zoom. When zoom editing, the touching and dragging of a device results in the device being moved instead of the floor. When the user draws a wall and drags the wall, the editor scrolls the floor automatically.

[0182] Home View of an embodiment supports the addition of multiple floors, and these floors can also be used for other physical spaces (e.g., outbuildings, garages, etc.). **Figure 57** shows a Home View Setup page for adding at least one floor to a floor plan, under an embodiment. In order to define a new floor in Edit mode, the user touches the Options button 5204 at the top of the Home View Setup page and chooses Add Floor Above (e.g., Figure 59, element 5902). In response the Add Floor page 5700 appears. In addition to the predefined floor plans, the current user floor is also available for copying to a new floor. The Add Floor page 5702 presents a prompt 5703 to select a floor plan along with numerous floor plans 5704 available for selection.

[0183] The Home View editor supports editing with multiple floors. **Figure 58** shows a Home View Setup page 5800

with editing for multiple floors, under an embodiment. When more than one floor is defined, the editor has a few changes. For example, a column of floor thumbnails 5802 appears in a portion of the interface, and the currently selected floor thumbnail 5801 is highlighted. At any time, the user can tap any floor to switch to that floor. As another example, a Remove Floor option is available in the Options menu (see Figure 59, element 5902).

[0184] The Home View editor enables the setting of a default floor when multiple floors are included. Generally, the first floor is drawn first on any client. However, if multiple floors are included and the bottom floor is not the default (e.g., a basement is included), Home View enables changing of this default. The default floor is changed, for example, by tapping the icon for the second floor and then choosing the option "Set As Default Floor" (see Figure 59, element 5902).

[0185] The Home View editor supports the moving of devices between floors when multiple floors are included. At any time, the user can move a device to the dock, switch floors by touching the floor thumbnail corresponding to the desired floor, then drag the device onto the new floor.

[0186] The Home View editor of an embodiment includes auto-fill interiors. By default, the interiors of each floor of an embodiment are "filled" to look different from the exteriors, and the interior walls are less prominent than the exterior walls. The auto-fill interiors can be selectively enabled.

[0187] The Home View editor is exited by tapping a "Done" button 5204. If changes have been introduced to the floors, device locations, or labels during an editing session, the editor prompts the user to save the changes before exiting back to the Settings screen. **Figure 60** shows a Home View Setup page 6000 with editor exit option prompts 6001 displayed, under an embodiment.

[0188] Home View of an embodiment includes or couples to a common data model. For each site, the site owner can use the Edit Home View layout editor to define the floors of the home, label the rooms of the home, and indicate the locations of the devices in the home. **Figure 61** is an example floor plan, under an embodiment. The output of the layout editor of an embodiment is represented using compact ASCII strings stored in site preferences on the server, but is not so limited. This storage scheme uses a virtual grid, and stores simple vector and x,y locations on that grid. For example, given a single-story home, the data describes the visual components as follows: the lighter-shade interior tile areas are described as two large rectangles; the stronger, exterior walls are described as four horizontal and three vertical vectors; the lighter interior walls are described as one horizontal and one vertical vector; the two device icons are each described with an x,y coordinate plus device identifier; the two room labels are each described with an x,y coordinate plus the text.

[0189] This static ASCII data model of the home is stored by the editor so that client applications can fetch this static data model and combine it locally with the current state of their devices to render a graphical view. The only thing that subsequently changes are the device icons as users take actions that affect the status of devices (e.g., open doors, turn on lights, etc.).

[0190] The data model strings are stored in three variables in site preferences on the server. The three variables include homeview/floors, homeview/devices, and homeview/labels. The variable homeview/floors specifies where the walls should be drawn for each floor, and whether interior floor space should be filled. The variable homeview/floors includes a single floor, or multiple floors (separated in the data by semicolons). If multiple floors are included, a default floor can be indicated so apps will display the default floor first.

[0191] The variable homeview/devices includes a list of floor locations and device IDs to draw on those locations. For multi-floor homes, per-floor data is separated by semicolons, but is not so limited. The list of floor locations and device IDs may be a subset of devices (the data model does not include information about devices that have not been placed on a floor).

[0192] The variable homeview/labels includes a list of locations, and text labels to draw centered on those locations. For multi-floor homes the data per floor is separated by semicolons.

[0193] Home View of an embodiment includes a compact method for storing numbers wherein, throughout this model, numbers such as x,y coordinates and vector lengths are compactly represented using an ASCII-offset model starting with the lowercase alphabet (plus a few characters that follow z in ASCII for > 26), as follows:

$$a=0,\ b=1,\ c=2,\ \ldots,\ x=23,\ y=24,\ z=25,\ \{=26,\ |=27,\ \}=28$$

The use of this model enables specification of any (x,y) coordinate using two characters. For example, a horizontal line drawn from x,y position 2,5 with a length of 20 (2,5,20) can be represented by storing the "2" as "c", storing "5" as "f", and storing 20 as t, compactly storing the line as "cft".

[0194] The homeview/floors variable includes specific data elements, but the embodiments are not so limited. The data elements of an embodiment include the following: [max # of tiles across] [optional flag: don't autofill interiors]; [floorplan data for 1st floor] [; floorplan data for 2nd floor] [; 3rd floor] [; 4th floor] [; 5th floor].

[0195] The data element "max # of tiles across" is saved as 28 by default. The result is that the user can draw a floor plan using up to 28 walls horizontally (29 walls vertically), containing 28 "tiles," which supports a house with up to five rooms across.

[0196] The data element optional flag to prevent autofill interiors, when included, instructs the Home View editor to never fill any floor interiors when exporting the floor data. While the data may not include any interior tiles, depending on how the walls were drawn, but this flag prevents any interior tiles from being computed by the editor.

[0197] The data element "semicolon" separates the general settings from the first floor data.

[0198] The data element "floorplan data for a single floor" includes an optional flag plus a number of blocks of text representing vectors to draw, each block separated by spaces. The first character of each block indicates the type of vector to draw, and the characters that follow represent the vectors. When a floor should be shown first, the flag "default " is added before the vector data for that floor. Generally, the first floor is the default, so in that case (or in a single-floor house) this flag is not needed. The blocks of text representing the vectors include but are not limited to an H block, V block, h block, v block, and t block.

[0199] The H block, when there are horizontal exterior walls to draw, starts with a capital H, followed by three characters for each horizontal wall to draw (startX, startY, length). For example, a 15-tile wall drawn from the top corner is represented as H(0,0,15), which is compactly represented as Haap. A second horizontal wall drawn elsewhere appends another block of three coordinates. So Haap might become Haappph if there are two horizontal exterior walls. In the full example there are four exterior walls to draw so the data block is H followed by 4 triples: Haappphxpfa}}.

[0200] The V block, when there are vertical exterior walls to draw, starts with a capital V, followed by three characters for each vertical wall to draw (startX, startY, length). A vertical exterior wall drawn down the left side is represented as V(0,0,28) as Vaa}. Again, another three characters are added for each additional vertical exterior wall to draw.

[0201] The h block is similar to the H block except these are rendered as horizontal interior walls. This block starts with the letter h, followed by three characters for each horizontal line to draw (startX, startY, length). For example, a 15-tile line drawn in the middle is represented as h(0,15,15), which is compactly represented as happ. Another wall drawn in another area appends another block of three coordinates for each additional wall.

[0202] The v block is similar to the V block except these are rendered as vertical interior walls. This block starts with the letter v, followed by three characters for each vertical wall to draw (startX, startY, length).

[0203] The t block, when there are interior tiles to draw, starts with the letter t, followed by four characters for each rectangle to draw (x, y, width, height). For example, a 15-tile square is drawn in the corner is represented as t(0,0,15,15), which is compactly represented as taapp. Another rectangle of tiles drawn in another area appends another block of four coordinates. So taapp might become taappap}n.

[0204] If there are multiple floors, a semicolon is added and then another block of floor plan data can be added. For an empty floor there can be nothing between floors. For example, a three-story house with nothing defined for the middle floor is represented as follows: 28; Haapppgxpfa Vaa}pap}pn; ; Haapppgxpfa Vaa}pap}pn.

[0205] **Figure 62** is an example Home View one-story floor plan, under an embodiment. This floor plan is represented in an embodiment as follows: 28 (draw on a grid 28 tiles wide by 28 tiles tall); taappap}n (draw interior tiles as two large rectangles (x,y,w,h): (0,0,15,15) and (0,15,28,13)); happ (draw an interior horizontal wall (x,y,w): (0,15,15)); vhui (draw an interior vertical wall (x,y,h): (7,20,8)); Haappphxpfa}} (draw 4 exterior horizontal walls); Vaa}pap}pn (draw 3 vertical exterior walls). The complete homeview/floors data for this single-story home would be: 28;taappap}n happ vhui Haappphxpfa}} Vaa}pap}pn.

[0206] The homeview/devices variable includes specific data elements, but the embodiments are not so limited. The data elements of an embodiment include the following: [device location + id on 1st floor] [another device location + id on 1st floor] [...] [; device data for 2nd floor] [; 3rd floor] [; 4th floor] [; 5th floor].

[0207] Regarding the device location data element, each device location starts with a letter indicating location type: t (center the device over the middle of a tile); h (center the device over the middle of a horizontal segment); v (center the device over the middle of a vertical segment). The device location is followed by two characters that specify the (x,y) location of that tile or wall segment. For example, to place a device in the center of the first tile an embodiment uses t(0,0), represented as taa.

[0208] The device identifier data element is the unique identifier for the device. Note that some IDs can be long, so an embodiment only stores the last six characters of the device ID. For example, if the identifier is "ZONE12VER1", an embodiment stores "12VER1", and if the identifier is "ZONE5VER1" the embodiment stores "E5VER1".

[0209] A complete device location + id element is a minimum of four characters (type, x, y, id) and can be up to nine characters. An example of a complete device location and identification is as follows: Draw camera "SC0FEBED" centered on the third horizontal wall segment across the top: t + (2, 0) + SC0FEBED, stored compactly as tca0FEBED. Another example of a complete device location and identification is as follows: Draw z-wave light with ID "7" centered over vertical wall segment 11 across and 5 down: vke7.

[0210] Data for multiple floors are separated by semicolons as described herein. Therefore, for a three-story house with just two devices on the third floor the data is as follows: ;; t{qE5VER1 h{w0FEBED.

[0211] **Figure 63** is an example Home View floor plan that includes two devices, under an embodiment. This floor plan is represented in an embodiment as follows: t{qE5VER1: draw a motion sensor "ZONE5VER1" centered over tile at x,y location (26, 16); h{w0FEBED: draw camera "SC0FEBED" centered over horizontal wall at x,y location (26, 22).

The complete homeview/devices data for this single-story home are: t{qE5VER1 h{w0FEBED.

[0212] The homeview/labels variable includes specific data elements, but the embodiments are not so limited. The data elements of an embodiment include the following: [label location + label text on 1st floor] [another location + label on 1st floor] [...] [; label data for 2nd floor] [; 3rd floor] [; 4th floor] [; 5th floor].

[0213] Each label location data element starts with a letter indicating location type: t (center the label over the middle of a tile; h (center the label over the middle of a horizontal segment; v (center the label over the middle of a vertical segment). The label location data element is followed by two characters that specify the (x,y) location of that tile or wall segment. For example, to place a label in the center of the first tile of an embodiment uses t(0,0), represented as taa.

[0214] The label text data element can be almost any string, enclosed in brackets []. The text encoding of an embodiment follows the W3C definition for encodeURLComponent() method in javascript, which encodes everything except ~!*()'.. The only characters not allowed in labels are brackets themselves ([]). These should be stripped out when labels are defined in the editor.

[0215] Empty labels should not be stored. A complete label location + text element includes a minimum of six characters (type, x, y, [text]), as in vhg[Bedroom].

[0216] **Figure 64** is an example Home View floor plan that includes two labels, under an embodiment. This floor plan is represented in an embodiment as follows: vhg[Bedroom]: draw label "Bedroom" centered over vertical wall at x,y location (7, 6); tsv[Living%20Room]: draw label "Living Room" centered over tile at x,y location (26, 22). The complete homeview/labels data for this single-story home are: vhg[Bedroom] tsv[Living%20Room].

[0217] As described in detail herein, the user defines the walls of each floor of a home by drawing basic vectors. However, when a floor is rendered, the building exteriors should be readily distinguished from the interiors. For rendering Home View, an embodiment includes algorithms that determine the interior of the home and compute which tiles should be transparent and which are filled. Perimeter walls are rendered to be more vivid than interior walls. The user may draw openings in the external walls.

[0218] The algorithm of an embodiment for determining interior and exterior walls begins by marking all tiles as interior tile. A list is generated of tiles on the edge of each floor that are empty (top row, bottom row, left column, right column), and a function is called to clear each tile having no outside wall. Any edge tiles having no walls outside of them are marked as exterior tiles. For each exterior tile, the algorithm recursively searches the surrounding tiles. If there are no walls separating that tile from the next, then the next one is also marked as exterior.

[0219] In this way, Home View recursively crawls into the house from the edges, marking tiles as "exterior" as operation proceeds. Once all exterior tiles are determined, walls adjacent to them are also considered "exterior", and any walls bounded by interior tiles are considered "interior". The algorithm identifies small openings, before recursing from one exterior tile to an adjacent tile, by examining the walls nearby to ensure the opening is wide enough before proceeding. This interior/exterior computation is computed by the Home View editor, and stored with the floor data on the server. Client renderers have an easier job since the data indicates interior/exterior information as defined above in homeview/floors.

[0220] The Home View data output from Edit mode is checked to ensure integrity through performance of the following: the home vectors fit without bounds of each floor; all sensors and devices still exist. At the time of rendering of the home view, the same checks are repeated to verify data integrity. If any checks fail, a dialog is presented to the user, and the preference returns to the System Icon (the "orb"). The feature therefore is turned off for display, but the data is still there until subsequently edited; if a user attempts to edit home view and the data is corrupted, the user is given the option to reset the data and start over.

[0221] The integrated security system includes couplings or connections among a variety of IP devices or components, and the device management module is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system of an embodiment uses a "sandbox" network to discover and manage all IP devices coupled or connected as components of the system. The IP devices of an embodiment include wired devices, wireless devices, cameras, interactive touchscreens, and security panels to name a few. These devices can be wired via ethernet cable or Wifi devices, all of which are secured within the sandbox network, as described below. The "sandbox" network is described in detail below.

[0222] **Figure 65** is a block diagram 500 of network or premise device integration with a premise network 250, under an embodiment. In an embodiment, network devices 255-257 are coupled to the gateway 102 using a secure network coupling or connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption). The network coupling or connection between the gateway 102 and the network devices 255-257 is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway 102 is coupled to the premise router/firewall 252 via a coupling with a premise LAN 250. The premise router/firewall 252 is coupled to a broadband modem 251, and the broadband modem 251 is coupled to a WAN 200 or other network outside the premise. The gateway 102 thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN 250 of the host premises. The gateway sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and

security touchscreens, to name a few. The gateway 102 manages or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited. Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the gateway 102.

[0223] **Figure 66** is a block diagram 600 of network or premise device integration with a premise network 250, under an alternative embodiment. The network or premise devices 255-257 are coupled to the gateway 102. The network coupling or connection between the gateway 102 and the network devices 255-257 is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway 102 is coupled or connected between the premise router/firewall 252 and the broadband modem 251. The broadband modem 251 is coupled to a WAN 200 or other network outside the premise, while the premise router/firewall 252 is coupled to a premise LAN 250. As a result of its location between the broadband modem 251 and the premise router/firewall 252, the gateway 102 can be configured or function as the premise router routing specified data between the outside network (e.g., WAN 200) and the premise router/firewall 252 of the LAN 250. As described above, the gateway 102 in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices 255-257 and is coupled or connected between the LAN 250 of the host premises and the WAN 200. The gateway sub-network can include, but is not limited to, any number of network or premise devices 255-257 like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway 102 manages or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited. Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the gateway 102.

[0224] The examples described above with reference to Figures 47 and 48 are presented only as examples of IP device integration. The integrated security system is not limited to the type, number and/or combination of IP devices shown and described in these examples, and any type, number and/or combination of IP devices is contemplated within the scope of this disclosure as capable of being integrated with the premise network.

[0225] The integrated security system of an embodiment includes a touchscreen (also referred to as the iControl touchscreen or integrated security system touchscreen), as described above, which provides core security keypad functionality, content management and presentation, and embedded systems design. The networked security touchscreen system of an embodiment enables a consumer or security provider to easily and automatically install, configure and manage the security system and touchscreen located at a customer premise. Using this system the customer may access and control the local security system, local IP devices such as cameras, local sensors and control devices (such as lighting controls or pipe freeze sensors), as well as the local security system panel and associated security sensors (such as door/window, motion, and smoke detectors). The customer premise may be a home, business, and/or other location equipped with a wired or wireless broadband IP connection.

[0226] The system of an embodiment includes a touchscreen with a configurable software user interface and/or a gateway device (e.g., iHub) that couples or connects to a premise security panel through a wired or wireless connection, and a remote server that provides access to content and information from the premises devices to a user when they are remote from the home. The touchscreen supports broadband and/or WAN wireless connectivity. In this embodiment, the touchscreen incorporates an IP broadband connection (e.g., Wifi radio, Ethernet port, etc.), and/or a cellular radio (e.g., GPRS/GSM, CDMA, WiMax, etc.). The touchscreen described herein can be used as one or more of a security system interface panel and a network user interface (UI) that provides an interface to interact with a network (e.g., LAN, WAN, internet, etc.).

[0227] The touchscreen of an embodiment provides an integrated touchscreen and security panel as an all-in-one device. Once integrated using the touchscreen, the touchscreen and a security panel of a premise security system become physically co-located in one device, and the functionality of both may even be co-resident on the same CPU and memory (though this is not required).

[0228] The touchscreen of an embodiment also provides an integrated IP video and touchscreen UI. As such, the touchscreen supports one or more standard video CODECs/players (e.g., H.264, Flash Video, MOV, MPEG4, M-JPEG, etc.). The touchscreen UI then provides a mechanism (such as a camera or video widget) to play video. In an embodiment the video is streamed live from an IP video camera. In other embodiments the video comprises video clips or photos sent from an IP camera or from a remote location.

[0229] The touchscreen of an embodiment provides a configurable user interface system that includes a configuration supporting use as a security touchscreen. In this embodiment, the touchscreen utilizes a modular user interface that allows components to be modified easily by a service provider, an installer, or even the end user. Examples of such a modular approach include using Flash widgets, HTML-based widgets, or other downloadable code modules such that the user interface of the touchscreen can be updated and modified while the application is running. In an embodiment the touchscreen user interface modules can be downloaded over the internet. For example, a new security configuration widget can be downloaded from a standard web server, and the touchscreen then loads such configuration app into memory, and inserts it in place of the old security configuration widget. The touchscreen of an embodiment is configured

to provide a self-install user interface.

[0230] Embodiments of the networked security touchscreen system described herein include a touchscreen device with a user interface that includes a security toolbar providing one or more functions including arm, disarm, panic, medic, and alert. The touchscreen therefore includes at least one screen having a separate region of the screen dedicated to a security toolbar. The security toolbar of an embodiment is present in the dedicated region at all times that the screen is active.

[0231] The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing home-based functions. The home-based functions of an embodiment include managing, viewing, and/or controlling IP video cameras. In this embodiment, regions of the home screen are allocated in the form of widget icons; these widget icons (e.g. for cameras, thermostats, lighting, etc) provide functionality for managing home systems. So, for example, a displayed camera icon, when selected, launches a Camera Widget, and the Camera widget in turn provides access to video from one or more cameras, as well as providing the user with relevant camera controls (take a picture, focus the camera, etc.)

[0232] The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing, viewing, and/or controlling internet-based content or applications. For example, the Widget Manager UI presents a region of the home screen (up to and including the entire home screen) where internet widgets icons such as weather, sports, etc. may be accessed). Each of these icons may be selected to launch their respective content services.

[0233] The touchscreen of an embodiment is integrated into a premise network using the gateway, as described above. The gateway as described herein functions to enable a separate wireless network, or sub-network, that is coupled, connected, or integrated with another network (e.g., WAN, LAN of the host premises, etc.). The sub-network enabled by the gateway optimizes the installation process for IP devices, like the touchscreen, that couple or connect to the sub-network by segregating these IP devices from other such devices on the network. This segregation of the IP devices of the sub-network further enables separate security and privacy policies to be implemented for these IP devices so that, where the IP devices are dedicated to specific functions (e.g., security), the security and privacy policies can be tailored specifically for the specific functions. Furthermore, the gateway and the sub-network it forms enables the segregation of data traffic, resulting in faster and more efficient data flow between components of the host network, components of the sub-network, and between components of the sub-network and components of the network.

[0234] The touchscreen of an embodiment includes a core functional embedded system that includes an embedded operating system, required hardware drivers, and an open system interface to name a few. The core functional embedded system can be provided by or as a component of a conventional security system (e.g., security system available from GE Security). These core functional units are used with components of the integrated security system as described herein. Note that portions of the touchscreen description below may include reference to a host premise security system (e.g., GE security system), but these references are included only as an example and do not limit the touchscreen to integration with any particular security system.

[0235] As an example, regarding the core functional embedded system, a reduced memory footprint version of embedded Linux forms the core operating system in an embodiment, and provides basic TCP/IP stack and memory management functions, along with a basic set of low-level graphics primitives. A set of device drivers is also provided or included that offer low-level hardware and network interfaces. In addition to the standard drivers, an interface to the RS 485 bus is included that couples or connects to the security system panel (e.g., GE Concord panel). The interface may, for example, implement the Superbus 2000 protocol, which can then be utilized by the more comprehensive transaction-level security functions implemented in PanelConnect technology (e.g SetAlarmLevel (int level, int partition, char *accessCode)). Power control drivers are also provided.

[0236] **Figure 67** is a block diagram of a touchscreen 700 of the integrated security system, under an embodiment. The touchscreen 700 generally includes an application/presentation layer 702 with a resident application 704, and a core engine 706. The touchscreen 700 also includes one or more of the following, but is not so limited: applications of premium services 710, widgets 712, a caching proxy 714, network security 716, network interface 718, security object 720, applications supporting devices 722, PanelConnect API 724, a gateway interface 726, and one or more ports 728.

[0237] More specifically, the touchscreen, when configured as a home security device, includes but is not limited to the following application or software modules: RS 485 and/or RS-232 bus security protocols to conventional home security system panel (e.g., GE Concord panel); functional home security classes and interfaces (e.g. Panel ARM state, Sensor status, etc.); Application/Presentation layer or engine; Resident Application; Consumer Home Security Application; installer home security application; core engine; and System bootloader/Software Updater. The core Application engine and system bootloader can also be used to support other advanced content and applications. This provides a seamless interaction between the premise security application and other optional services such as weather widgets or IP cameras.

[0238] An alternative configuration of the touchscreen includes a first Application engine for premise security and a second Application engine for all other applications. The integrated security system application engine supports content

standards such as HTML, XML, Flash, etc. and enables a rich consumer experience for all 'widgets', whether security-based or not. The touchscreen thus provides service providers the ability to use web content creation and management tools to build and download any 'widgets' regardless of their functionality.

[0239] As discussed above, although the Security Applications have specific low-level functional requirements in order to interface with the premise security system, these applications make use of the same fundamental application facilities as any other 'widget', application facilities that include graphical layout, interactivity, application handoff, screen management, and network interfaces, to name a few.

[0240] Content management in the touchscreen provides the ability to leverage conventional web development tools, performance optimized for an embedded system, service provider control of accessible content, content reliability in a consumer device, and consistency between 'widgets' and seamless widget operational environment. In an embodiment of the integrated security system, widgets are created by web developers and hosted on the integrated security system Content Manager (and stored in the Content Store database). In this embodiment the server component caches the widgets and offers them to consumers through the web-based integrated security system provisioning system. The servers interact with the advanced touchscreen using HTTPS interfaces controlled by the core engine and dynamically download widgets and updates as needed to be cached on the touchscreen. In other embodiments widgets can be accessed directly over a network such as the Internet without needing to go through the iControl Content Manager

[0241] Referring to **Figure 67**, the touchscreen system is built on a tiered architecture, with defined interfaces between the Application/Presentation Layer (the Application Engine) on the top, the Core Engine in the middle, and the security panel and gateway APIs at the lower level. The architecture is configured to provide maximum flexibility and ease of maintenance.

[0242] The application engine of the touchscreen provides the presentation and interactivity capabilities for all applications (widgets) that run on the touchscreen, including both core security function widgets and third party content widgets. **Figure 68** is an example screenshot 800 of a networked security touchscreen, under an embodiment. This example screenshot 800 includes three interfaces or user interface (UI) components 802-806, but is not so limited. A first UI 802 of the touchscreen includes icons by which a user controls or accesses functions and/or components of the security system (e.g., "Main", "Panic", "Medic", "Fire", state of the premise alarm system (e.g., disarmed, armed, etc.), etc.); the first UI 802, which is also referred to herein as a security interface, is always presented on the touchscreen. A second UI 804 of the touchscreen includes icons by which a user selects or interacts with services and other network content (e.g., clock, calendar, weather, stocks, news, sports, photos, maps, music, etc.) that is accessible via the touchscreen. The second UI 804 is also referred to herein as a network interface or content interface. A third UI 806 of the touchscreen includes icons by which a user selects or interacts with additional services or componets (e.g., intercom control, security, cameras coupled to the system in particular regions (e.g., front door, baby, etc.) available via the touchscreen.

[0243] A component of the application engine is the Presentation Engine, which includes a set of libraries that implement the standards-based widget content (e.g., XML, HTML, JavaScript, Flash) layout and interactivity. This engine provides the widget with interfaces to dynamically load both graphics and application logic from third parties, support high level data description language as well as standard graphic formats. The set of web content-based functionality available to a widget developer is extended by specific touchscreen functions implemented as local web services by the Core Engine.

[0244] The resident application of the touchscreen is the master service that controls the interaction of all widgets in the system, and enforces the business and security rules required by the service provider. For example, the resident application determines the priority of widgets, thereby enabling a home security widget to override resource requests from a less critical widget (e.g. a weather widget). The resident application also monitors widget behavior, and responds to client or server requests for cache updates.

[0245] The core engine of the touchscreen manages interaction with other components of the integrated security system, and provides an interface through which the resident application and authorized widgets can get information about the home security system, set alarms, install sensors, etc. At the lower level, the Core Engine's main interactions are through the PanelConnect API, which handles all communication with the security panel, and the gateway Interface, which handles communication with the gateway. In an embodiment, both the iHub Interface and PanelConnect API are resident and operating on the touchscreen. In another embodiment, the PanelConnect API runs on the gateway or other device that provides security system interaction and is accessed by the touchscreen through a web services interface.

[0246] The Core Engine also handles application and service level persistent and cached memory functions, as well as the dynamic provisioning of content and widgets, including but not limited to: flash memory management, local widget and content caching, widget version management (download, cache flush new/old content versions), as well as the caching and synchronization of user preferences. As a portion of these services the Core engine incorporates the bootloader functionality that is responsible for maintaining a consistent software image on the touchscreen, and acts as the client agent for all software updates. The bootloader is configured to ensure full update redundancy so that unsuccessful downloads cannot corrupt the integrated security system.

[0247] Video management is provided as a set of web services by the Core Engine. Video management includes the

retrieval and playback of local video feeds as well as remote control and management of cameras (all through iControl CameraConnect technology).

[0248] Both the high level application layer and the mid-level core engine of the touchscreen can make calls to the network. Any call to the network made by the application layer is automatically handed off to a local caching proxy, which determines whether the request should be handled locally. Many of the requests from the application layer are web services API requests; although such requests could be satisfied by the iControl servers, they are handled directly by the touchscreen and the gateway. Requests that get through the caching proxy are checked against a white list of acceptable sites, and, if they match, are sent off through the network interface to the gateway. Included in the Network Subsystem is a set of network services including HTTP, HTTPS, and server-level authentication functions to manage the secure client-server interface. Storage and management of certificates is incorporated as a part of the network services layer.

[0249] Server components of the integrated security system servers support interactive content services on the touchscreen. These server components include, but are not limited to the content manager, registry manager, network manager, and global registry, each of which is described herein.

[0250] The Content Manager oversees aspects of handling widget data and raw content on the touchscreen. Once created and validated by the service provider, widgets are 'ingested' to the Content Manager, and then become available as downloadable services through the integrated security system Content Management APIs. The Content manager maintains versions and timestamp information, and connects to the raw data contained in the backend Content Store database. When a widget is updated (or new content becomes available) all clients registering interest in a widget are systematically updated as needed (a process that can be configured at an account, locale, or system-wide level).

[0251] The Registry Manager handles user data, and provisioning accounts, including information about widgets the user has decided to install, and the user preferences for these widgets.

[0252] The Network Manager handles getting and setting state for all devices on the integrated security system network (e.g., sensors, panels, cameras, etc.). The Network manager synchronizes with the gateway, the advanced touchscreen, and the subscriber database.

[0253] The Global Registry is a primary starting point server for all client services, and is a logical referral service that abstracts specific server locations/addresses from clients (touchscreen, gateway 102, desktop widgets, etc.). This approach enables easy scaling/migration of server farms.

[0254] The touchscreen of an embodiment operates wirelessly with a premise security system. The touchscreen of an embodiment incorporates an RF transceiver component that either communicates directly with the sensors and/or security panel over the panel's proprietary RF frequency, or the touchscreen communicates wirelessly to the gateway over 802.11, Ethernet, or other IP-based communications channel, as described in detail herein. In the latter case the gateway implements the PanelConnect interface and communicates directly to the security panel and/or sensors over wireless or wired networks as described in detail above.

[0255] The touchscreen of an embodiment is configured to operate with multiple security systems through the use of an abstracted security system interface. In this embodiment, the PanelConnect API can be configured to support a plurality of proprietary security system interfaces, either simultaneously or individually as described herein. In one embodiment of this approach, the touchscreen incorporates multiple physical interfaces to security panels (e.g. GE Security RS-485, Honeywell RF, etc.) in addition to the PanelConnect API implemented to support multiple security interfaces. The change needed to support this in PanelConnect is a configuration parameter specifying the panel type connection that is being utilized.

[0256] So for example, the setARMState() function is called with an additional parameter (e.g., Armstate = setARMState(type="ARM STAY| ARM AWAY| DISARM", Parameters="ExitDelay=30 |Lights=OFF", panelType ="GE Concord4 RS485")). The 'panelType' parameter is used by the setARMState function (and in practice by all of the PanelConnect functions) to select an algorithm appropriate to the specific panel out of a plurality of algorithms.

[0257] The touchscreen of an embodiment is self-installable. Consequently, the touchscreen provides a 'wizard' approach similar to that used in traditional computer installations (e.g. InstallShield). The wizard can be resident on the touchscreen, accessible through a web interface, or both. In one embodiment of a touchscreen self-installation process, the service provider can associate devices (sensors, touchscreens, security panels, lighting controls, etc.) remotely using a web-based administrator interface.

[0258] The touchscreen of an embodiment includes a battery backup system for a security touchscreen. The touchscreen incorporates a standard Li-ion or other battery and charging circuitry to allow continued operation in the event of a power outage. In an embodiment the battery is physically located and connected within the touchscreen enclosure. In another embodiment the battery is located as a part of the power transformer, or in between the power transformer and the touchscreen.

[0259] The example configurations of the integrated security system described above with reference to Figures 47 and 48 include a gateway that is a separate device, and the touchscreen couples to the gateway. However, in an alternative embodiment, the gateway device and its functionality can be incorporated into the touchscreen so that the

device management module, which is now a component of or included in the touchscreen, is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system with the integrated touchscreen/gateway uses the same "sandbox" network to discover and manage all IP devices coupled or connected as components of the system.

[0260] The touchscreen of this alternative embodiment integrates the components of the gateway with the components of the touchscreen as described herein. More specifically, the touchscreen of this alternative embodiment includes software or applications described above with reference to Figure 3. In this alternative embodiment, the touchscreen includes the gateway application layer 302 as the main program that orchestrates the operations performed by the gateway. A Security Engine 304 of the touchscreen provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine 304 of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.

Bi-directional authentication between the touchscreen and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.

Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The touchscreen provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.

802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.

A touchscreen-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying touchscreen-enabled devices have the knowledge that only a gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

[0261] As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

[0262] A Remote Firmware Download module 306 of the touchscreen allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server 104, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Touchscreen firmware can be remotely download either for one touchscreen at a time, a group of touchscreen, or in batches.

[0263] The Automations engine 308 of the touchscreen manages the user-defined rules of interaction between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

[0264] DeviceConnect 310 of the touchscreen touchscreen includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module 310 offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect 312 is provided for adding new sensors, Camera-Connect 316 for adding IP cameras, and PanelConnect 314 for adding home security panels.

[0265] The Schedules engine 318 of the touchscreen is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application of the touchscreen. The Schedules Engine 318 then interfaces with SensorConnect 312 to ensure that scheduled events occur at precisely the desired time.

[0266] The Device Management module 320 of the touchscreen is in charge of all discovery, installation and config-

uration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters, and the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

[0267] The video routing engine 322 of the touchscreen is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing. The video routing engine is described in detail in the Related Applications.

[0268] **Figure 69** is a block diagram 900 of network or premise device integration with a premise network 250, under an embodiment. In an embodiment, network devices 255, 256, 957 are coupled to the touchscreen 902 using a secure network connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption), and the touchscreen 902 coupled to the premise router/firewall 252 via a coupling with a premise LAN 250. The premise router/firewall 252 is coupled to a broadband modem 251, and the broadband modem 251 is coupled to a WAN 200 or other network outside the premise. The touchscreen 902 thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN 250 of the host premises. The touchscreen sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and IP devices, to name a few. The touchscreen 902 manages or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited. Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the touchscreen 902.

[0269] **Figure 70** is a block diagram 1000 of network or premise device integration with a premise network 250, under an alternative embodiment. The network or premise devices 255, 256, 1057 are coupled to the touchscreen 1002, and the touchscreen 1002 is coupled or connected between the premise router/firewall 252 and the broadband modem 251. The broadband modem 251 is coupled to a WAN 200 or other network outside the premise, while the premise router/firewall 252 is coupled to a premise LAN 250. As a result of its location between the broadband modem 251 and the premise router/firewall 252, the touchscreen 1002 can be configured or function as the premise router routing specified data between the outside network (e.g., WAN 200) and the premise router/firewall 252 of the LAN 250. As described above, the touchscreen 1002 in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices 255, 156, 1057 and is coupled or connected between the LAN 250 of the host premises and the WAN 200. The touchscreen sub-network can include, but is not limited to, any number of network or premise devices 255, 256, 1057 like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The touchscreen 1002 manages or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited. Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the touchscreen 1002.

[0270] The gateway of an embodiment, whether a stand-along component or integrated with a touchscreen, enables couplings or connections and thus the flow or integration of information between various components of the host premises and various types and/or combinations of IP devices, where the components of the host premises include a network (e.g., LAN) and/or a security system or subsystem to name a few. Consequently, the gateway controls the association between and the flow of information or data between the components of the host premises. For example, the gateway of an embodiment forms a sub-network coupled to another network (e.g., WAN, LAN, etc.), with the sub-network including IP devices. The gateway further enables the association of the IP devices of the sub-network with appropriate systems on the premises (e.g., security system, etc.). Therefore, for example, the gateway can form a sub-network of IP devices configured for security functions, and associate the sub-network only with the premises security system, thereby segregating the IP devices dedicated to security from other IP devices that may be coupled to another network on the premises.

[0271] The gateway of an embodiment, as described herein, enables couplings or connections and thus the flow of information between various components of the host premises and various types and/or combinations of IP devices, where the components of the host premises include a network, a security system or subsystem to name a few. Consequently, the gateway controls the association between and the flow of information or data between the components of the host premises. For example, the gateway of an embodiment forms a sub-network coupled to another network (e.g., WAN, LAN, etc.), with the sub-network including IP devices. The gateway further enables the association of the IP devices of the sub-network with appropriate systems on the premises (e.g., security system, etc.). Therefore, for example, the gateway can form a sub-network of IP devices configured for security functions, and associate the sub-network only with the premises security system, thereby segregating the IP devices dedicated to security from other IP devices that may be coupled to another network on the premises.

[0272] **Figure 71** is a flow diagram for a method 1100 of forming a security network including integrated security system components, under an embodiment. Generally, the method comprises coupling 1102 a gateway comprising a connection management component to a local area network in a first location and a security server in a second location.

The method comprises forming 1104 a security network by automatically establishing a wireless coupling between the gateway and a security system using the connection management component. The security system of an embodiment comprises security system components located at the first location. The method comprises integrating 1106 communications and functions of the security system components into the security network via the wireless coupling.

[0273] **Figure 72** is a flow diagram for a method 1200 of forming a security network including integrated security system components and network devices, under an embodiment. Generally, the method comprises coupling 1202 a gateway to a local area network located in a first location and a security server in a second location. The method comprises automatically establishing 1204 communications between the gateway and security system components at the first location, the security system including the security system components. The method comprises automatically establishing 1206 communications between the gateway and premise devices at the first location. The method comprises forming 1208 a security network by electronically integrating, via the gateway, communications and functions of the premise devices and the security system components.

[0274] In an example embodiment, **Figure 73** is a flow diagram 1300 for integration or installation of an IP device into a private network environment, under an embodiment. The IP device includes any IP-capable device that, for example, includes the touchscreen of an embodiment. The variables of an embodiment set at time of installation include, but are not limited to, one or more of a private SSID/Password, a gateway identifier, a security panel identifier, a user account TS, and a Central Monitoring Station account identification.

[0275] An embodiment of the IP device discovery and management begins with a user or installer activating 1302 the gateway and initiating 1304 the install mode of the system. This places the gateway in an install mode. Once in install mode, the gateway shifts to a default (Install) Wifi configuration. This setting will match the default setting for other integrated security system-enabled devices that have been pre-configured to work with the integrated security system. The gateway will then begin to provide 1306 DHCP addresses for these IP devices. Once the devices have acquired a new DHCP address from the gateway, those devices are available for configuration into a new secured Wifi network setting.

[0276] The user or installer of the system selects 1308 all devices that have been identified as available for inclusion into the integrated security system. The user may select these devices by their unique IDs via a web page, Touchscreen, or other client interface. The gateway provides 1310 data as appropriate to the devices. Once selected, the devices are configured 1312 with appropriate secured Wifi settings, including SSID and WPA/WPA-2 keys that are used once the gateway switches back to the secured sandbox configuration from the "Install" settings. Other settings are also configured as appropriate for that type of device. Once all devices have been configured, the user is notified and the user can exit install mode. At this point all devices will have been registered 1314 with the integrated security system servers.

[0277] The installer switches 1316 the gateway to an operational mode, and the gateway instructs or directs 1318 all newly configured devices to switch to the "secured" Wifi sandbox settings. The gateway then switches 1320 to the "secured" Wifi settings. Once the devices identify that the gateway is active on the "secured" network, they request new DHCP addresses from the gateway which, in response, provides 1322 the new addresses. The devices with the new addresses are then operational 1324 on the secured network.

[0278] In order to ensure the highest level of security on the secured network, the gateway can create or generate a dynamic network security configuration based on the unique ID and private key in the gateway, coupled with a randomizing factor that can be based on online time or other inputs. This guarantees the uniqueness of the gateway secured network configuration.

[0279] To enable the highest level of performance, the gateway analyzes the RF spectrum of the 802.11x network and determines which frequency band/channel it should select to run.

[0280] An alternative embodiment of the camera/IP device management process leverages the local ethernet connection of the sandbox network on the gateway. This alternative process is similar to the Wifi discovery embodiment described above, except the user connects the targeted device to the ethernet port of the sandbox network to begin the process. This alternative embodiment accommodates devices that have not been pre-configured with the default "Install" configuration for the integrated security system.

[0281] This alternative embodiment of the IP device discovery and management begins with the user/installer placing the system into install mode. The user is instructed to attach an IP device to be installed to the sandbox Ethernet port of the gateway. The IP device requests a DHCP address from the gateway which, in response to the request, provides the address. The user is presented the device and is asked if he/she wants to install the device. If yes, the system configures the device with the secured Wifi settings and other device-specific settings (e.g., camera settings for video length, image quality etc.). The user is next instructed to disconnect the device from the ethernet port. The device is now available for use on the secured sandbox network.

[0282] **Figure 74** is a block diagram showing communications among integrated IP devices of the private network environment, under an embodiment. The IP devices of this example include a security touchscreen 1403, gateway 1402 (e.g., "iHub"), and security panel (e.g., "Security Panel 1", "Security Panel 2", "Security Panel n"), but the embodiment is not so limited. In alternative embodiments any number and/or combination of these three primary component types

may be combined with other components including IP devices and/or security system components. For example, a single device which comprises an integrated gateway, touchscreen, and security panel is merely another embodiment of the integrated security system described herein. The description that follows includes an example configuration that includes a touchscreen hosting particular applications. However, the embodiment is not limited to the touchscreen hosting these applications, and the touchscreen should be thought of as representing any IP device.

[0283] Referring to Figure 74, the touchscreen 1403 incorporates an application 1410 that is implemented as computer code resident on the touchscreen operating system, or as a web-based application running in a browser, or as another type of scripted application (e.g., Flash, Java, Visual Basic, etc.). The touchscreen core application 1410 represents this application, providing user interface and logic for the end user to manage their security system or to gain access to networked information or content (Widgets). The touchscreen core application 1410 in turn accesses a library or libraries of functions to control the local hardware (e.g. screen display, sound, LEDs, memory, etc.) as well as specialized librarie(s) to couple or connect to the security system.

[0284] In an embodiment of this security system connection, the touchscreen 1403 communicates to the gateway 1402, and has no direct communication with the security panel. In this embodiment, the touchscreen core application 1410 accesses the remote service APIs 1412 which provide security system functionality (e.g. ARM/DISARM panel, sensor state, get/set panel configuration parameters, initiate or get alarm events, etc.). In an embodiment, the remote service APIs 1412 implement one or more of the following functions, but the embodiment is not so limited: Armstate = setARMState(type="ARM STAY| ARM AWAY| DISARM", Parameters="ExitDelay=30 |Lights=OFF"); sensorState=getSensors(type="ALL| SensorName I SensorNameList"); result = setSensorState(SensorName, parameters="Option1, Options2,...Option n"); interruptHandler =SensorEvent(); and, interruptHandler=alarmEvent().

[0285] Functions of the remote service APIs 1412 of an embodiment use a remote PanelConnect API 1424 which resides in memory on the gateway 1402. The touchscreen 1403 communicates with the gateway 1402 through a suitable network interface such as an Ethernet or 802.11 RF connection, for example. The remote PanelConnect API 1424 provides the underlying Security System Interfaces 1426 used to communicate with and control one or more types of security panel via wired link 1430 and/or RF link 3. The PanelConnect API 1224 provides responses and input to the remote services APIs 1426, and in turn translates function calls and data to and from the specific protocols and functions supported by a specific implementation of a Security Panel (e.g. a GE Security Simon XT or Honeywell Vista 20P). In an embodiment, the PanelConnect API 1224 uses a 345MHz RF transceiver or receiver hardware/firmware module to communicate wirelessly to the security panel and directly to a set of 345 MHz RF-enabled sensors and devices, but the embodiment is not so limited.

[0286] The gateway of an alternative embodiment communicates over a wired physical coupling or connection to the security panel using the panel's specific wired hardware (bus) interface and the panel's bus-level protocol.

[0287] In an alternative embodiment, the Touchscreen 1403 implements the same PanelConnect API 1414 locally on the Touchscreen 1403, communicating directly with the Security Panel 2 and/or Sensors 2 over the proprietary RF link or over a wired link for that system. In this embodiment the Touchscreen 1403, instead of the gateway 1402, incorporates the 345 MHz RF transceiver to communicate directly with Security Panel 2 or Sensors 2 over the RF link 2. In the case of a wired link the Touchscreen 1403 incorporates the real-time hardware (e.g. a PIC chip and RS232-variant serial link) to physically connect to and satisfy the specific bus-level timing requirements of the SecurityPanel2.

[0288] In yet another alternative embodiment, either the gateway 1402 or the Touchscreen 1403 implements the remote service APIs. This embodiment includes a Cricket device ("Cricket") which comprises but is not limited to the following components: a processor (suitable for handling 802.11 protocols and processing, as well as the bus timing requirements of SecurityPanel1); an 802.11 (WiFi) client IP interface chip; and, a serial bus interface chip that implements variants of RS232 or RS485, depending on the specific Security Panel.

[0289] The Cricket also implements the full PanelConnect APIs such that it can perform the same functions as the case where the gateway implements the PanelConnect APIs. In this embodiment, the touchscreen core application 1410 calls functions in the remote service APIs 1412 (such as setArmState()). These functions in turn couple or connect to the remote Cricket through a standard IP connection ("Cricket IP Link") (e.g., Ethernet, Homeplug, the gateway's proprietary Wifi network, etc.). The Cricket in turn implements the PanelConnect API, which responds to the request from the touchscreen core application, and performs the appropriate function using the proprietary panel interface. This interface uses either the wireless or wired proprietary protocol for the specific security panel and/or sensors.

[0290] **Figure 75** is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment. Operations begin when the system is powered on 1510, involving at a minimum the power-on of the gateway device, and optionally the power-on of the connection between the gateway device and the remote servers. The gateway device initiates 1520 a software and RF sequence to locate the extant security system. The gateway and installer initiate and complete 1530 a sequence to 'learn' the gateway into the security system as a valid and authorized control device. The gateway initiates 1540 another software and RF sequence of instructions to discover and learn the existence and capabilities of existing RF devices within the extant security system, and store this information in the system. These operations under the system of an embodiment are described in further

detail below.

[0291] Unlike conventional systems that extend an existing security system, the system of an embodiment operates utilizing the proprietary wireless protocols of the security system manufacturer. In one illustrative embodiment, the gateway is an embedded computer with an IP LAN and WAN connection and a plurality of RF transceivers and software protocol modules capable of communicating with a plurality of security systems each with a potentially different RF and software protocol interface. After the gateway has completed the discovery and learning 1540 of sensors and has been integrated 1550 as a virtual control device in the extant security system, the system becomes operational. Thus, the security system and associated sensors are presented 1550 as accessible devices to a potential plurality of user interface subsystems.

[0292] The system of an embodiment integrates 1560 the functionality of the extant security system with other non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms, which may be controlled via RF, wired, or powerline-based networking mechanisms supported by the gateway or servers.

[0293] The system of an embodiment provides a user interface subsystem 1570 enabling a user to monitor, manage, and control the system and associated sensors and security systems. In an embodiment of the system, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX/Flash presentation of a monitoring and control application, enabling users to view the state of all sensors and controllers in the extant security system from a web browser or equivalent operating on a computer, PDA, mobile phone, or other consumer device.

[0294] In another illustrative embodiment of the system described herein, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX presentation of a monitoring and control application, enabling users to combine the monitoring and control of the extant security system and sensors with the monitoring and control of non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms.

[0295] In another illustrative embodiment of the system described herein, a user interface subsystem is a mobile phone application enabling users to monitor and control the extant security system as well as other non-security devices.

[0296] In another illustrative embodiment of the system described herein, a user interface subsystem is an application running on a keypad or touchscreen device enabling users to monitor and control the extant security system as well as other non-security devices.

[0297] In another illustrative embodiment of the system described herein, a user interface subsystem is an application operating on a TV or set-top box connected to a TV enabling users to monitor and control the extant security system as well as other non-security devices.

[0298] **Figure 76** is a block diagram of an integrated security system 1600 wirelessly interfacing to proprietary security systems, under an embodiment. A security system 1610 is coupled or connected to a Gateway 1620, and from Gateway 1620 coupled or connected to a plurality of information and content sources across a network 1630 including one or more web servers 1640, system databases 1650, and applications servers 1660. While in one embodiment network 1630 is the Internet, including the World Wide Web, those of skill in the art will appreciate that network 1630 may be any type of network, such as an intranet, an extranet, a virtual private network (VPN), a mobile network, or a non- TCP/IP based network.

[0299] Moreover, other elements of the system of an embodiment may be conventional, well-known elements that need not be explained in detail herein. For example, security system 1610 could be any type home or business security system, such devices including but not limited to a standalone RF home security system or a non-RF-capable wired home security system with an add-on RF interface module. In the integrated security system 1600 of this example, security system 1610 includes an RF-capable wireless security panel (WSP) 1611 that acts as the master controller for security system 1610. Well-known examples of such a WSP include the GE Security Concord, Networx, and Simon panels, the Honeywell Vista and Lynx panels, and similar panels from DSC and Napco, to name a few. A wireless module 1614 includes the RF hardware and protocol software necessary to enable communication with and control of a plurality of wireless devices 1613. WSP 1611 may also manage wired devices 1614 physically connected to WSP 1611 with an RS232 or RS485 or Ethernet connection or similar such wired interface.

[0300] In an implementation consistent with the systems and methods described herein, Gateway 1620 provides the interface between security system 1610 and LAN and/or WAN for purposes of remote control, monitoring, and management. Gateway 1620 communicates with an external web server 1640, database 1650, and application server 1660 over network 1630 (which may comprise WAN, LAN, or a combination thereof). In this example system, application logic, remote user interface functionality, as well as user state and account are managed by the combination of these remote servers. Gateway 1620 includes server connection manager 1621, a software interface module responsible for all server communication over network 1630. Event manager 1622 implements the main event loop for Gateway 1620, processing events received from device manager 1624 (communicating with non-security system devices including but not limited to IP cameras, wireless thermostats, or remote door locks). Event manager 1622 further processes events and control messages from and to security system 1610 by utilizing WSP manager 1623.

[0301] WSP manager 1623 and device manager 1624 both rely upon wireless protocol manager 1626 which receives and stores the proprietary or standards-based protocols required to support security system 1610 as well as any other

devices interfacing with gateway 1620. WSP manager 1623 further utilizes the comprehensive protocols and interface algorithms for a plurality of security systems 1610 stored in the WSP DB client database associated with wireless protocol manager 1626. These various components implement the software logic and protocols necessary to communicate with and manager devices and security systems 1610. Wireless Transceiver hardware modules 1625 are then used to implement the physical RF communications link to such devices and security systems 1610. An illustrative wireless transceiver 1625 is the GE Security Dialog circuit board, implementing a 319.5MHz two-way RF transceiver module. In this example, RF Link 1670 represents the 319.5MHz RF communication link, enabling gateway 1620 to monitor and control WSP 1611 and associated wireless and wired devices 1613 and 1614, respectively.

[0302] In one embodiment, server connection manager 1621 requests and receives a set of wireless protocols for a specific security system 1610 (an illustrative example being that of the GE Security Concord panel and sensors) and stores them in the WSP DB portion of the wireless protocol manager 1626. WSP manager 1623 then utilizes such protocols from wireless protocol manager 1626 to initiate the sequence of processes detailed in Figure 57 and Figure 58 for learning gateway 1620 into security system 1610 as an authorized control device. Once learned in, as described with reference to Figure 58 (and above), event manager 1622 processes all events and messages detected by the combination of WSP manager 1623 and the GE Security wireless transceiver module 1625.

[0303] In another embodiment, gateway 1620 incorporates a plurality of wireless transceivers 1625 and associated protocols managed by wireless protocol manager 1626. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP 1611, wireless devices 1613, and wired devices 1614. For example a wireless sensor from one manufacturer may be utilized to control a device using a different protocol from a different manufacturer.

[0304] In another embodiment, gateway 1620 incorporates a wired interface to security system 1610, and incorporates a plurality of wireless transceivers 1625 and associated protocols managed by wireless protocol manager 1626. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP 1611, wireless devices 1613, and wired devices 1614.

[0305] Of course, while an illustrative embodiment of an architecture of the system of an embodiment is described in detail herein with respect to Figure 58, one of skill in the art will understand that modifications to this architecture may be made without departing from the scope of the description presented herein. For example, the functionality described herein may be allocated differently between client and server, or amongst different server or processor-based components. Likewise, the entire functionality of the gateway 1620 described herein could be integrated completely within an existing security system 1610. In such an embodiment, the architecture could be directly integrated with a security system 1610 in a manner consistent with the currently described embodiments.

[0306] **Figure 77** is a flow diagram for wirelessly 'learning' the Gateway into an existing security system and discovering extant sensors, under an embodiment. The learning interfaces gateway 1620 with security system 1610. Gateway 1620 powers up 1710 and initiates software sequences 1720 and 1725 to identify accessible WSPs 1611 and wireless devices 1613, respectively (e.g., one or more WSPs and/or devices within range of gateway 1620). Once identified, WSP 1611 is manually or automatically set into 'learn mode' 1730, and gateway 1620 utilizes available protocols to add 1740 itself as an authorized control device in security system 1610. Upon successful completion of this task, WSP 1611 is manually or automatically removed from 'learn mode' 1750.

[0307] Gateway 1620 utilizes the appropriate protocols to mimic 1760 the first identified device 1614. In this operation gateway 1620 identifies itself using the unique or pseudo-unique identifier of the first found device 1614, and sends an appropriate change of state message over RF Link 1670. In the event that WSP 1611 responds to this change of state message, the device 1614 is then added 1770 to the system in database 1650. Gateway 1620 associates 1780 any other information (such as zone name or token-based identifier) with this device 1614 in database 1650, enabling gateway 1620, user interface modules, or any application to retrieve this associated information.

[0308] In the event that WSP 1611 does not respond to the change of state message, the device 1614 is not added 1770 to the system in database 1650, and this device 1614 is identified as not being a part of security system 1610 with a flag, and is either ignored or added as an independent device, at the discretion of the system provisioning rules. Operations hereunder repeat 1785 operations 1760, 1770, 1780 for all devices 1614 if applicable. Once all devices 1614 have been tested in this way, the system begins operation 1790.

[0309] In another embodiment, gateway 1620 utilizes a wired connection to WSP 1611, but also incorporates a wireless transceiver 1625 to communicate directly with devices 1614. In this embodiment, operations under 1720 above are removed, and operations under 1740 above are modified so the system of this embodiment utilizes wireline protocols to add itself as an authorized control device in security system 1610.

[0310] A description of an example embodiment follows in which the Gateway (Figure 58, element 1620) is the iHub available from iControl Networks, Palo Alto, CA, and described in detail herein. In this example the gateway is "automatically" installed with a security system.

[0311] The automatic security system installation begins with the assignment of an authorization key to components of the security system (e.g., gateway, kit including the gateway, etc.). The assignment of an authorization key is done in lieu of creating a user account. An installer later places the gateway in a user's premises along with the premises

security system. The installer uses a computer to navigate to a web portal (e.g., integrated security system web interface), logs in to the portal, and enters the authorization key of the installed gateway into the web portal for authentication. Once authenticated, the gateway automatically discovers devices at the premises (e.g., sensors, cameras, light controls, etc.) and adds the discovered devices to the system or "network". The installer assigns names to the devices, and tests operation of the devices back to the server (e.g., did the door open, did the camera take a picture, etc.). The security device information is optionally pushed or otherwise propagated to a security panel and/or to the server network database. The installer finishes the installation, and instructs the end user on how to create an account, username, and password. At this time the user enters the authorization key which validates the account creation (uses a valid authorization key to associate the network with the user's account). New devices may subsequently be added to the security network in a variety of ways (e.g., user first enters a unique ID for each device/sensor and names it in the server, after which the gateway can automatically discover and configure the device).

[0312] A description of another example embodiment follows in which the security system (Figure 58, element 1610) is a Dialog system and the WSP (Figure 58, element 1611) is a SimonXT available from General Electric Security, and the Gateway (Figure 58, element 1620) is the iHub available from iControl Networks, Palo Alto, CA, and described in detail herein. Descriptions of the install process for the SimonXT and iHub are also provided below.

[0313] GE Security's Dialog network is one of the most widely deployed and tested wireless security systems in the world. The physical RF network is based on a 319.5 MHz unlicensed spectrum, with a bandwidth supporting up to 19Kbps communications. Typical use of this bandwidth -even in conjunction with the integrated security system-is far less than that. Devices on this network can support either one-way communication (either a transmitter or a receiver) or two-way communication (a transceiver). Certain GE Simon, Simon XT, and Concord security control panels incorporate a two-way transceiver as a standard component. The gateway also incorporates the same two-way transceiver card. The physical link layer of the network is managed by the transceiver module hardware and firmware, while the coded payload bitstreams are made available to the application layer for processing.

[0314] Sensors in the Dialog network typically use a 60-bit protocol for communicating with the security panel transceiver, while security system keypads and the gateway use the encrypted 80-bit protocol. The Dialog network is configured for reliability, as well as low-power usage. Many devices are supervised, i.e. they are regularly monitored by the system 'master' (typically a GE security panel), while still maintaining excellent power usage characteristics. A typical door window sensor has a battery life in excess of 5-7 years.

[0315] The gateway has two modes of operation in the Dialog network: a first mode of operation is when the gateway is configured or operates as a 'slave' to the GE security panel; a second mode of operation is when the gateway is configured or operates as a 'master' to the system in the event a security panel is not present. In both configurations, the gateway has the ability to 'listen' to network traffic, enabling the gateway to continually keep track of the status of all devices in the system. Similarly, in both situations the gateway can address and control devices that support setting adjustments (such as the GE wireless thermostat).

[0316] In the configuration in which the gateway acts as a 'slave' to the security panel, the gateway is 'learned into' the system as a GE wireless keypad. In this mode of operation, the gateway emulates a security system keypad when managing the security panel, and can query the security panel for status and 'listen' to security panel events (such as alarm events).

[0317] The gateway incorporates an RF Transceiver manufactured by GE Security, but is not so limited. This transceiver implements the Dialog protocols and handles all network message transmissions, receptions, and timing. As such, the physical, link, and protocol layers of the communications between the gateway and any GE device in the Dialog network are totally compliant with GE Security specifications.

[0318] At the application level, the gateway emulates the behavior of a GE wireless keypad utilizing the GE Security 80-bit encrypted protocol, and only supported protocols and network traffic are generated by the gateway. Extensions to the Dialog RF protocol of an embodiment enable full control and configuration of the panel, and iControl can both automate installation and sensor enrollment as well as direct configuration downloads for the panel under these protocol extensions.

[0319] As described above, the gateway participates in the GE Security network at the customer premises. Because the gateway has intelligence and a two-way transceiver, it can 'hear' all of the traffic on that network. The gateway makes use of the periodic sensor updates, state changes, and supervisory signals of the network to maintain a current state of the premises. This data is relayed to the integrated security system server (e.g., Figure 2, element 260) and stored in the event repository for use by other server components. This usage of the GE Security RF network is completely non-invasive; there is no new data traffic created to support this activity.

[0320] The gateway can directly (or indirectly through the Simon XT panel) control two-way devices on the network. For example, the gateway can direct a GE Security Thermostat to change its setting to 'Cool' from 'Off', as well as request an update on the current temperature of the room. The gateway performs these functions using the existing GE Dialog protocols, with little to no impact on the network; a gateway device control or data request takes only a few dozen bytes of data in a network that can support 19 Kbps.

[0321] By enrolling with the Simon XT as a wireless keypad, as described herein, the gateway includes data or information of all alarm events, as well as state changes relevant to the security panel. This information is transferred to the gateway as encrypted packets in the same way that the information is transferred to all other wireless keypads on the network.

[0322] Because of its status as an authorized keypad, the gateway can also initiate the same panel commands that a keypad can initiate. For example, the gateway can arm or disarm the panel using the standard Dialog protocol for this activity. Other than the monitoring of standard alarm events like other network keypads, the only incremental data traffic on the network as a result of the gateway is the infrequent remote arm/disarm events that the gateway initiates, or infrequent queries on the state of the panel.

[0323] The gateway is enrolled into the Simon XT panel as a 'slave' device which, in an embodiment, is a wireless keypad. This enables the gateway for all necessary functionality for operating the Simon XT system remotely, as well as combining the actions and information of non-security devices such as lighting or door locks with GE Security devices. The only resource taken up by the gateway in this scenario is one wireless zone (sensor ID).

[0324] The gateway of an embodiment supports three forms of sensor and panel enrollment/installation into the integrated security system, but is not limited to this number of enrollment/installation options. The enrollment/installation options of an embodiment include installer installation, kitting, and panel, each of which is described below.

[0325] Under the installer option, the installer enters the sensor IDs at time of installation into the integrated security system web portal or iScreen. This technique is supported in all configurations and installations.

[0326] Kits can be pre-provisioned using integrated security system provisioning applications when using the kitting option. At kitting time, multiple sensors are automatically associated with an account, and at install time there is no additional work required.

[0327] In the case where a panel is installed with sensors already enrolled (i.e. using the GE Simon XT enrollment process), the gateway has the capability to automatically extract the sensor information from the system and incorporate it into the user account on the integrated security system server.

[0328] The gateway and integrated security system of an embodiment uses an auto-learn process for sensor and panel enrollment in an embodiment. The deployment approach of an embodiment can use additional interfaces that GE Security is adding to the Simon XT panel. With these interfaces, the gateway has the capability to remotely enroll sensors in the panel automatically. The interfaces include, but are not limited to, the following: EnrollDevice(ID, type, name, zone, group); SetDeviceParameters(ID, type, Name, zone, group), GetDeviceParameters(zone); and RemoveDevice(zone).

[0329] The integrated security system incorporates these new interfaces into the system, providing the following install process. The install process can include integrated security system logistics to handle kitting and pre-provisioning. Pre-kitting and logistics can include a pre-provisioning kitting tool provided by integrated security system that enables a security system vendor or provider ("provider") to offer pre-packaged initial 'kits'. This is not required but is recommended for simplifying the install process. This example assumes a 'Basic' kit is preassembled and includes one (1) Simon XT, three (3) Door/ window sensors, one (1) motion sensor, one (1) gateway, one (1) keyfob, two (2) cameras, and ethernet cables. The kit also includes a sticker page with all Zones (1-24) and Names (full name list).

[0330] The provider uses the integrated security system kitting tool to assemble 'Basic' kit packages. The contents of different types of starter kits may be defined by the provider. At the distribution warehouse, a worker uses a bar code scanner to scan each sensor and the gateway as it is packed into the box. An ID label is created that is attached to the box. The scanning process automatically associates all the devices with one kit, and the new ID label is the unique identifier of the kit. These boxes are then sent to the provider for distribution to installer warehouses. Individual sensors, cameras, etc. are also sent to the provider installer warehouse. Each is labeled with its own barcode/ ID.

[0331] An installation and enrollment procedure of a security system including a gateway is described below as one example of the installation process.

1. Order and Physical Install Process

a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the provider for assignment to an installer.

b. The assigned installer picks up his/her ticket(s) and fills his/her truck with Basic and/or Advanced starter kits. He/she also keeps a stock of individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.

c. The installer arrives at the address on the ticket, and pulls out the Basic kit. The installer determines sensor locations from a tour of the premises and discussion with the homeowner. At this point assume the homeowner requests additional equipment including an extra camera, two (2) additional door/window sensors, one (1) glass break detector, and one (1) smoke detector.

d. Installer mounts SimonXT in the kitchen or other location in the home as directed by the homeowner, and routes the phone line to Simon XT if available. GPRS and Phone numbers pre-programmed in SimonXT to

point to the provider Central Monitoring Station (CMS).
e. Installer places gateway in the home in the vicinity of a router and cable modem. Installer installs an ethernet line from gateway to router and plugs gateway into an electrical outlet.

2. Associate and Enroll gateway into SimonXT

a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with installer ID/pass.
b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer for kit ID (on box's barcode label).
c. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add gateway as a wireless keypad. It is noted that this step is for security only and can be automated in an embodiment.
d. Installer enters the installer code into the Simon XT. Installer Learns 'gateway' into the panel as a wireless keypad as a group 1 device.
e. Installer goes back to Web portal, and clicks the 'Finished Adding SimonXT' button.

3. Enroll Sensors into SimonXT via iControl

a. All devices in the Basic kit are already associated with the user's account.
b. For additional devices, Installer clicks 'Add Device' and adds the additional camera to the user's account (by typing in the camera ID/Serial #).
c. Installer clicks 'Add Device' and adds other sensors (two (2) door/window sensors, one (1) glass break sensor, and one (1) smoke sensor) to the account (e.g., by typing in IDs).
d. As part of Add Device, Installer assigns zone, name, and group to the sensor. Installer puts appropriate Zone and Name sticker on the sensor temporarily.
e. All sensor information for the account is pushed or otherwise propagated to the iConnect server, and is available to propagate to CMS automation software through the CMS application programming interface (API).
f. Web interface displays 'Installing Sensors in System....' and automatically adds all of the sensors to the Simon XT panel through the GE RF link.
g. Web interface displays 'Done Installing' --> all sensors show green.

4. Place and Tests Sensors in Home

a. Installer physically mounts each sensor in its desired location, and removes the stickers.
b. Installer physically mounts WiFi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
c. Installer goes to Web interface and is prompted for automatic camera install. Each camera is provisioned as a private, encrypted Wifi device on the gateway secured sandbox network, and firewall NAT traversal is initiated. Upon completion the customer is prompted to test the security system.
d. Installer selects the 'Test System' button on the web portal -- the SimonXT is put into Test mode by the gateway over GE RF.
e. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
f. gateway sends test data directly to CMS over broadband link, as well as storing the test data in the user's account for subsequent report generation.
g. Installer exits test mode from the Web portal.

5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the iControl web and mobile portals. Customer creates a username/password at this time.

6. Installer instructs customer how to change Simon XT user code from the Web interface. Customer changes user code which is pushed to SimonXT automatically over GE RF.

[0332] An installation and enrollment procedure of a security system including a gateway is described below as an alternative example of the installation process. This installation process is for use for enrolling sensors into the SimonXT and integrated security system and is compatible with all existing GE Simon panels.

[0333] The integrated security system supports all pre-kitting functionality described in the installation process above. However, for the purpose of the following example, no kitting is used.

1. Order and Physical Install Process

a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the security system provider for assignment to an installer.
b. The assigned installer picks up his/her ticket(s) and fills his/her truck with individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.
c. The installer arrives at the address on the ticket, and analyzes the house and talks with the homeowner to determine sensor locations. At this point assume the homeowner requests three (3) cameras, five (5) door/window sensors, one (1) glass break detector, one (1) smoke detector, and one (1) keyfob.
d. Installer mounts SimonXT in the kitchen or other location in the home. The installer routes a phone line to Simon XT if available. GPRS and Phone numbers are pre-programmed in SimonXT to point to the provider CMS.
e. Installer places gateway in home in the vicinity of a router and cable modem, and installs an ethernet line from gateway to the router, and plugs gateway into an electrical outlet.

2. Associate and Enroll gateway into SimonXT

a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with an installer ID/pass.
b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer to add devices.
c. Installer types in ID of gateway, and it is associated with the user's account.
d. Installer clicks 'Add Device' and adds the cameras to the user's account (by typing in the camera ID/Serial #).
e. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add gateway as a wireless keypad.
f. Installer goes to Simon XT and enters the installer code into the Simon XT. Learns 'gateway' into the panel as a wireless keypad as group 1 type sensor.
g. Installer returns to Web portal, and clicks the 'Finished Adding SimonXT' button.
h. Gateway now is alerted to all subsequent installs over the security system RF.

3. Enroll Sensors into SimonXT via iControl

a. Installer clicks 'Add Simon XT Sensors' -- Displays instructions for adding sensors to Simon XT.
b. Installer goes to Simon XT and uses Simon XT install process to add each sensor, assigning zone, name, group. These assignments are recorded for later use.
c. The gateway automatically detects each sensor addition and adds the new sensor to the integrated security system.
d. Installer exits install mode on the Simon XT, and returns to the Web portal.
e. Installer clicks 'Done Adding Devices'.
f. Installer enters zone/sensor naming from recorded notes into integrated security system to associate sensors to friendly names.
g. All sensor information for the account is pushed to the iConnect server, and is available to propagate to CMS automation software through the CMS API.

4. Place and Tests Sensors in Home

a. Installer physically mounts each sensor in its desired location.
b. Installer physically mounts Wifi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
c. Installer puts SimonXT into Test mode from the keypad.
d. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
e. Installer exits test mode from the Simon XT keypad.
f. Installer returns to web interface and is prompted to automatically set up cameras. After waiting for completion cameras are now provisioned and operational.

5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the integrated security system web and mobile portals. Customer creates a username/password at this time.
6. Customer and Installer observe that all sensors/cameras are green.

7. Installer instructs customer how to change Simon XT user code from the keypad. Customer changes user code and stores in SimonXT.
8. The first time the customer uses the web portal to Arm/Disarm system the web interface prompts the customer for the user code, which is then stored securely on the server. In the event the user code is changed on the panel the web interface once again prompts the customer.

[0334] The panel of an embodiment can be programmed remotely. The CMS pushes new programming to SimonXT over a telephone or GPRS link. Optionally, iControl and GE provide a broadband link or coupling to the gateway and then a link from the gateway to the Simon XT over GE RF.

[0335] In addition to the configurations described above, the gateway of an embodiment supports takeover configurations in which it is introduced or added into a legacy security system. A description of example takeover configurations follow in which the security system (Figure 2, element 210) is a Dialog system and the WSP (Figure 2, element 211) is a GE Concord panel (e.g., equipped with POTS, GE RF, and Superbus 2000 RS485 interface (in the case of a Lynx takeover the Simon XT is used) available from General Electric Security. The gateway (Figure 2, element 220) in the takeover configurations is an iHub (e.g., equipped with built-in 802.11b/g router, Ethernet Hub, GSM/GPRS card, RS485 interface, and iControl Honeywell-compatible RF card) available from iControl Networks, Palo Alto, CA. While components of particular manufacturers are used in this example, the embodiments are not limited to these components or to components from these vendors.

[0336] The security system can optionally include RF wireless sensors (e.g., GE wireless sensors utilizing the GE Dialog RF technology), IP cameras, a GE-iControl Touchscreen (the touchscreen is assumed to be an optional component in the configurations described herein, and is thus treated separately from the iHub; in systems in which the touchscreen is a component of the base security package, the integrated iScreen (available from iControl Networks, Palo Alto, CA) can be used to combine iHub technology with the touchscreen in a single unit), and Z-Wave devices to name a few.

[0337] The takeover configurations described below assume takeover by a "new" system of an embodiment of a security system provided by another third party vendor, referred to herein as an "original" or "legacy" system. Generally, the takeover begins with removal of the control panel and keypad of the legacy system. A GE Concord panel is installed to replace the control panel of the legacy system along with an iHub with GPRS Modem. The legacy system sensors are then connected or wired to the Concord panel, and a GE keypad or touchscreen is installed to replace the control panel of the legacy system. The iHub includes the iControl RF card, which is compatible with the legacy system. The iHub finds and manages the wireless sensors of the legacy system, and learns the sensors into the Concord by emulating the corresponding GE sensors. The iHub effectively acts as a relay for legacy wireless sensors.

[0338] Once takeover is complete, the new security system provides a homogeneous system that removes the compromises inherent in taking over or replacing a legacy system. For example, the new system provides a modern touchscreen that may include additional functionality, new services, and supports integration of sensors from various manufacturers. Furthermore, lower support costs can be realized because call centers, installers, etc. are only required to support one architecture. Additionally, there is minimal install cost because only the panel is required to be replaced as a result of the configuration flexibility offered by the iHub.

[0339] The system takeover configurations described below include but are not limited to a dedicated wireless configuration, a dedicated wireless configuration that includes a touchscreen, and a fished Ethernet configuration. Each of these configurations is described in detail below.

[0340] **Figure 78** is a block diagram of a security system in which the legacy panel is replaced with a GE Concord panel wirelessly coupled to an iHub, under an embodiment. All existing wired and RF sensors remain in place. The iHub is located near the Concord panel, and communicates with the panel via the 802.11 link, but is not so limited. The iHub manages cameras through a built-in 802.11 router. The iHub listens to the existing RF HW sensors, and relays sensor information to the Concord panel (emulating the equivalent GE sensor). The wired sensors of the legacy system are connected to the wired zones on the control panel.

[0341] **Figure 79** is a block diagram of a security system in which the legacy panel is replaced with a GE Concord panel wirelessly coupled to an iHub, and a GE-iControl Touchscreen, under an embodiment. All existing wired and RF sensors remain in place. The iHub is located near the Concord panel, and communicates with the panel via the 802.11 link, but is not so limited. The iHub manages cameras through a built-in 802.11 router. The iHub listens to the existing RF HW sensors, and relays sensor information to the Concord panel (emulating the equivalent GE sensor). The wired sensors of the legacy system are connected to the wired zones on the control panel.

[0342] The GE-iControl Touchscreen can be used with either of an 802.11 connection or Ethernet connection with the iHub. Because the takeover involves a GE Concord panel (or Simon XT), the touchscreen is always an option. No extra wiring is required for the touchscreen as it can use the 4-wire set from the replaced keypad of the legacy system. This provides power, battery backup (through Concord), and data link (RS485 Superbus 2000) between Concord and touchscreen. The touchscreen receives its broadband connectivity through the dedicated 802.11 link to the iHub.

[0343] **Figure 80** is a block diagram of a security system in which the legacy panel is replaced with a GE Concord

panel connected to an iHub via an Ethernet coupling, under an embodiment. All existing wired and RF sensors remain in place. The iHub is located near the Concord panel, and wired to the panel using a 4-wire Superbus 2000 (RS485) interface, but is not so limited. The iHub manages cameras through a built-in 802.11 router. The iHub listens to the existing RF HW sensors, and relays sensor information to the Concord panel (emulating the equivalent GE sensor). The wired sensors of the legacy system are connected to the wired zones on the control panel.

[0344] The takeover installation process is similar to the installation process described above, except the control panel of the legacy system is replaced; therefore, only the differences with the installation described above are provided here. The takeover approach of an embodiment uses the existing RS485 control interfaces that GE Security and iControl support with the iHub, touchscreen, and Concord panel. With these interfaces, the iHub is capable of automatically enrolling sensors in the panel. The exception is the leverage of an iControl RF card compatible with legacy systems to 'takeover' existing RF sensors. A description of the takeover installation process follows.

[0345] During the installation process, the iHub uses an RF Takeover Card to automatically extract all sensor IDs, zones, and names from the legacy panel. The installer removes connections at the legacy panel from hardwired wired sensors and labels each with the zone. The installer pulls the legacy panel and replaces it with the GE Concord panel. The installer also pulls the existing legacy keypad and replaces it with either a GE keypad or a GE-iControl touchscreen. The installer connects legacy hardwired sensors to appropriate wired zone (from labels) on the Concord. The installer connects the iHub to the local network and connects the iHub RS485 interface to the Concord panel. The iHub automatically 'enrolls' legacy RF sensors into the Concord panel as GE sensors (maps IDs), and pushes or otherwise propagates other information gathered from HW panel (zone, name, group). The installer performs a test of all sensors back to CMS. In operation, the iHub relays legacy sensor data to the Concord panel, emulating equivalent GE sensor behavior and protocols.

[0346] The areas of the installation process particular to the legacy takeover include how the iHub extracts sensor info from the legacy panel and how the iHub automatically enrolls legacy RF sensors and populates Concord with wired zone information. Each of these areas is described below.

[0347] In having the iHub extract sensor information from the legacy panel, the installer 'enrolls' iHub into the legacy panel as a wireless keypad (use install code and house ID-available from panel). The iHub legacy RF Takeover Card is a compatible legacy RF transceiver. The installer uses the web portal to place iHub into 'Takeover Mode', and the web portal the automatically instructs the iHub to begin extraction. The iHub queries the panel over the RF link (to get all zone information for all sensors, wired and RF). The iHub then stores the legacy sensor information received during the queries on the iConnect server.

[0348] The iHub also automatically enrolls legacy RF sensors and populates Concord with wired zone information. In so doing, the installer selects 'Enroll legacy Sensors into Concord' (next step in 'Takeover' process on web portal). The iHub automatically queries the iConnect server, and downloads legacy sensor information previously extracted. The downloaded information includes an ID mapping from legacy ID to 'spoofed' GE ID. This mapping is stored on the server as part of the sensor information (e.g., the iConnect server knows that the sensor is a legacy sensor acting in GE mode). The iHub instructs Concord to go into install mode, and sends appropriate Superbus 2000 commands for sensor learning to the panel. For each sensor, the 'spoofed' GE ID is loaded, and zone, name, and group are set based on information extracted from legacy panel. Upon completion, the iHub notifies the server, and the web portal is updated to reflect next phase of Takeover (e.g., 'Test Sensors').

[0349] Sensors are tested in the same manner as described above. When a HW sensor is triggered, the signal is captured by the iHub legacy RF Takeover Card, translated to the equivalent GE RF sensor signal, and pushed to the panel as a sensor event on the SuperBus 2000 wires.

[0350] In support of remote programming of the panel, CMS pushes new programming to Concord over a phone line, or to the iConnect CMS/Alarm Server API, which in turn pushes the programming to the iHub. The iHub uses the Concord Superbus 2000 RS485 link to push the programming to the Concord panel.

[0351] **Figure 81** is a flow diagram for automatic takeover 2100 of a security system, under an embodiment. Automatic takeover includes establishing 2102 a wireless coupling between a takeover component running under a processor and a first controller of a security system installed at a first location. The security system includes some number of security system components coupled to the first controller. The automatic takeover includes automatically extracting 2104 security data of the security system from the first controller via the takeover component. The automatic takeover includes automatically transferring 2106 the security data to a second controller and controlling loading of the security data into the second controller. The second controller is coupled to the security system components and replaces the first controller.

[0352] **Figure 82** is a flow diagram for automatic takeover 2200 of a security system, under an alternative embodiment. Automatic takeover includes automatically forming 2202 a security network at a first location by establishing a wireless coupling between a security system and a gateway. The gateway of an embodiment includes a takeover component. The security system of an embodiment includes security system components. The automatic takeover includes automatically extracting 2204 security data of the security system from a first controller of the security system. The automatic takeover includes automatically transferring 2206 the security data to a second controller. The second controller of an

embodiment is coupled to the security system components and replaces the first controller.

[0353] Home View as described herein enables users to quickly access and view state, and control devices from a single user experience. Home View provides an easy way for users to represent each floor of their home and indicate the location of security sensors, cameras, lights, thermostats, locks, and any other devices in the home automation system. Using this interface, users can easily check on the state of their home from anywhere using a mobile phone or web browser. To further enhance the "glanceable" experience of home management, the Home View of an embodiment includes a three-dimensional version referred to herein as "Home View 3D". Home View 3D provides the added ability to see all locations in a multi-floor dwelling at once. For example, a user can instantly notice an open window upstairs, turn off a light, view temperature on each floor, and access cameras outside with a single click, to name a few.

[0354] **Figure 83** is an example status interface of Home View 3D, under an embodiment. **Figure 84** is an example user interface of Home View 3D, under an embodiment.

[0355] To enable Home View 3D, the user can edit the representation of their home using one or more of a web browser, smart phone, and tablet computer, and select or click the Home View 3D option. That setting is saved in the cloud-based environment or other server environment, and changes the user's web and mobile devices to use a 3D view. Home View 3D provides unique and powerful visualization of the home lets the user feel connected and in control of their home from anywhere in the world. **Figure 85** is an example user interface showing "enable" control of Home View 3D, under an embodiment.

[0356] Home View 3D is disabled by default, and a user can enable it in any editor of an embodiment. Home View 3D includes options in the editor menu to toggle the 3D option. These settings affect or are applied to all client devices that interface with the site (e.g., after next login, depending on caching). **Figure 86** is an example user interface showing "disable" control of Home View 3D, under an embodiment.

[0357] Additionally, when Home View 3D is enabled, the editor displays an indicator to that effect using the thumbnails, but the embodiment is not so limited. **Figure 87** is an example editor interface with indicators of Home View 3D being enabled, under an embodiment.

[0358] The 3D of an embodiment is a render-time feature, but is not so limited. The interaction with Home View 3D is as described in detail herein with a single-floor rendering (e.g., devices include popups indicating state, double-clicking devices causes navigation, etc.). In Home View 3D of an embodiment, if the canvas is non-square, the rendering stretches to fit the canvas (or display viewer). For example, on tablets the renderer can be wider than it is tall. Additionally, floating text for devices at the top edge of lower floors flips over to render below the device, just as they did for the 2D renderer described herein.

[0359] Regarding general rendering and scaling rules of an embodiment, Home View 3D primarily affects walls with isometric skewing to make them look tipped back. As an example, the front wall is full width, and the back wall is approximately 80% of normal width, giving the illusion of depth. Devices and text are not skewed and the device or text appears as if sitting upright on the tipped floors. Devices and text of an embodiment are scaled to match horizontal scaling. Specifically, devices and text on the front edge are approximately 100% normal size, and devices and text on the back edge are approximately 80% of normal size.

[0360] Furthermore, floors are tapered so that a top floor is slightly wider than the bottom floor to add to the 3D illusion. Specifically, the front corners of the bottom floor render as they would in 2D (e.g., with a gutter on left/right), but the front corners of the top floor is approximately one pixel away from canvas edge, but the embodiment is not so limited.

[0361] Home view 3D of an example embodiment supports between one and five floors, but is not so limited. **Figure 88** is an example user interface showing five floors, under an embodiment.

[0362] Home View 3D includes customization and branding but is not so limited. **Figure 89** is an example interface of Home View 3D showing variables, under an embodiment. Home View branding variables are as follows, but are not so limited:

A. threeDScaleBackRowByPct = 0.8; //horizontally scale back wall (and icons and text) this %, 80% width of front edge
B. threeDVertScaleSingleFloorPct = 0.75; //if rending single floor 3D, scale vertically by this percent
C. threeDVertFloorGapInTiles = 1.2; //insert vertical gap betwen floors, height is this many tiles
D. threeDTopFloorColorStops = [{stop: 0, color: "rgb(180,180,180)"}, //color for back edge of top floor
E. {stop: 1, color: "rgb(180,180,180)"}]; //color for front edge of top floor
F. threeDBotFloorColorStops = [{stop: 0 , color: "rgb(180,180,180)"}, //color for back edge of shadow on lower floors
G. {stop: 0.75, color: "rgb(180,180,180)"}, //color for front edge of shadow on lower floors
H. {stop: 0.9 , color: "rgb(180,180,180)"}, //color for back edge of lighted section of lower floors
I. {stop: 1 , color: "rgb(180,180,180)"}]; //color for front edge of lighted section of lower floors
J. threeDSubShadowGapInTiles = 2.5; //gap between bottom floor and sub-shadow; height is this many tiles
K. threeDSubShadowColor = "rgba(0,0,0,0.15)"; //color and transparency of shadow (same shape as bottom floor)
L. threeDSubShadowBlur = 20; //radius of blur for sub-shadow

[0363] Home View 3D presents more information when a device (e.g., tablet, phone, touch screen, etc.) is in landscape mode. When 3D is enabled and the host device is in landscape mode, the rendering of an embodiment is approximately 40% wider than it is tall, but the embodiment is not so limited. Further, it should also center both vertically and horizontally. **Figure 90** shows example renderings for square, wide, and tall canvases, 3D single-floor premises, and 3D multi-floor premises, under an embodiment.

[0364] In addition to rendering 3D, Home View 3D includes historical activity data or information for sensors, like a "heat map" for history that fades with time. For example, if a door opens or closes, the device icon will have a bright glow around it that will fade with time. At a glance the user can tell where there has been recent activity. **Figure 91** is an example user interface showing a "heat map" of Home View 3D, under an embodiment. In this example, sensors in the "family room" and "living room" are displayed with a bright glow indicating recent activity, the but embodiment is not so limited.

[0365] This feature is activated on each client when the user selects or taps the history icon and enables history view by choosing a time period. Once a time period is selected, that client shows a history glow for all sensors that have had activity within that time period. For example, with 1 Week selected, a sensor that has been tripped today will have a strong glow, a sensor tripped 3 days ago will be half faded, a sensor tripped 6 days ago will have a very faint glow, and a sensor tripped 7 days ago (or more) will have no glow at all.

[0366] The heat map feature includes three UI elements but is not so limited. An icon is used to enable and set the feature. By default, the icon is a standard history icon (clock in circle). But if history view is enabled, the circle contains the time period shown (10M = 10 minutes, 1D = 10 days etc.). Additionally, a popup dialog enables the user to enable the feature and select a time period. A glow ring is shown around sensors, and the glow ring is configured to fade with passage of time. **Figure 92** is an example user interface for configuring a "heat map" of Home View 3D, under an embodiment. **Figure 93** is another example user interface for configuring a "heat map" of Home View 3D, under an embodiment.

[0367] Embodiments display activity for the premises devices based on the type of device, but are not so limited. For example, activity presented for sensors includes a last update for any point in the instance (e.g., open/close, low battery, trouble, tamper, bypass, alarms, etc.). Activity presented for door locks and garage door controllers includes a last or most recent update for any point in the instance (e.g., open/close, lock/unlock, low battery, trouble, etc.). Activity presented for lights (w/o energy) includes last or most recent update for any point in the instance (e.g., on/off, dimmer level changes, offline, etc.). Activity presented for lights that report energy includes last or most recent update for any point in the instance (e.g., on/off, dimmer level changes, offline, etc.) (energy changes and related points may be ignored). Activity presented for thermostats includes last or most recent update for any point in the instance (e.g. heating/cooling, setpoint changes, mode changes, low battery, etc.). Activity presented for cameras includes last or most recent update for motion sensor (may not report camera taking pictures/clips). Activity presented for energy may not include report activity.

[0368] When computing coordinates in two dimensions (2D), an embodiment used a two-dimensional array (28x28) comprising information about each "tile" in the data grid for each floor. Here, a block of numbers from the serial data is provided to draw a large rectangle of floor tiles:

```
for (i=0; i<tilesArr.length; i++) {
  if (tilesArr[i].length > 4) {
    x = (tilesArr[i][1]);
    y = (tilesArr[i][2]);
    w = (tilesArr[i][3]);
    h = (tilesArr[i][4]);
    //save individual tile data for editing
    for (row=y; row < (y+h) && row<this.numTiles; row++) {
      for (col=x; col < (x+w) && col<this.numTiles; col++) this.t[row][col].shown=true;
      //turn on tile for each value in vector
     }
   //remember full tile blocks, ONLY for superfast rendering (not edit mode, where
segs are being changed constantly)
   point0 = this.pSkewXY(x *this.tileWidth + this.startPosX, y *this.tileWidth +
   this.startPosY);
   point1 = this.pSkewXY((x + w)*this.tileWidth + this.startPosX, y *this.tileWidth
   + this.startPosY);
   point2 = this.pSkewXY((x + w)*this.tileWidth + this.startPosX, (y +
   h)*this.tileWidth + this.startPosY);
   point3 = this.pSkewXY(x *this.tileWidth + this.startPosX, (y + h)*this.tileWidth
   + this.startPosY);
   this.tFastRender.push([point0, point1, point2, point3]);
```

```
  }
 }
```

[0369] For example, if the data included taadc, that becomes an array [0,0,3,2], meaning draw a rectangle from the origin, three tiles wide and two tiles high. The above code, computes the true pixel position for those locations, converting the parameters to 4 (x,y) corners of the rectangle to render:

$$\begin{array}{l} . \ . \ \Rightarrow .\text{point0} \ .\text{point1} \ \Rightarrow .(x0,y0) \ .(x1,y1) \\ . \ . \quad .\text{point3} \ .\text{point2} \quad .(x3,y3) \ .(x2,y2) \end{array}$$

[0370] The actual pixel location of each x,y coordinate is taking the abstract grid location and turning it into pixels. Each location is multiplied by the tileWidth, then offset by the rendering start positions startPosX and startPosY that account for gutters. To compute an abstract position like (3,2), the params are multiplied by the pixel width of a tile, and offset by the pixel position startPosX etc.

$$\text{pixelPosition for } (x,y) = (x*\text{this.tileWidth} + \text{this.startPosX},\ y*\text{this.tileWidth} + \text{this.startPosY})$$

[0371] For 2D rendering, the pSkewXY function does not alter these pixel positions, but returns them. For 3D rendering, each x,y position gets altered in several ways as follows, but the embodiment is not so limited:

1. If there are multiple floors, each y position is scaled vertically (for example, if there are 2 floors, every y value is divided by 2). The first floor would be drawn from the origin, but the 2nd floor would also be offset vertically so it draws halfway down. In addition, vertical offset is altered to provide a gap is between floors.
2. If there is a single floor, each position is scaled vertically to 60% of its height and offset to be vertically centered. This is controlled by a ppref.
3. All x positions are altered by shifting them toward the vertical midline. For example, in a 100px canvas, An x value of 50 it is unchanged. However, if x is 0, it needs to be skewed 20% toward the center. Since the back row is to be scaled to 80% width, we bring X to 80% of it's distance from the vertical midline. In this example, x would change to (50 - abs(x-50)*0.8). So an x at 0 shifted 20% to midline becomes x=10. This effect is reduced as we render lower rows (toward the front edge of the floor). Back row is squeezed to 80%, and front row is not horizontally squeezed at all, so 100% of original position.
4. A front-to-back scaling factor must be computed for later shrinking of device icons and label text. Devices in back (top) row are scaled to 80%, halfway back 90%, and front edge (bottom) devices are 100%.

[0372] An example follows of the core skewing algorithm of an embodiment, in code, but the embodiment is not so limited:

```
//---------------------------------------------------------------
// pSkewXY
// arguments: absolute canvas x and y positions
// return: object with x and y properties with new, skewed values
//
// In general, y skew is scaled by # floors (2 floors means y = y/2). X skew is more
subtle.
// If x is about halfway across, its unaffected. And if Y is the max, x is the front row and
// undaffected. But the farther "back" you go, the more skewed x is. For example, in the
first
// row, x==0 will be bent in by the 80% factor, or 10% increased towards the middle.
//-------------------------------------------------------------------------------------
ic_hvwFloorData.prototype.pSkewXY = function (px, py) {
 var devScale = 1; //computed amount to scale devices for each location. 1 for front
 edge (bottom row), .80 for back edge (top row)
 try {
  if (this.render3D) { //skewing ONLY affects render mode, not editor
```

```
   if (!this.cache) { //to ensure this is fast, precompute everything possible, only once
   per floor
     var scaleBackRowByPct= this.threeDScaleBackRowByPct, //horizontally
scale back wall (and icons and text) this %
      vertScaleSingleFloorPct = this.threeDVertScaleSingleFloorPct, //if rending
single floor 3D, scale vert by this %
      floorGapInTiles = this.threeDVertFloorGapInTiles, //vert gap btwn
      floors, height is this many tiles (scaled by # floors)
      gapBetweenFloors = (this.numFloors>1)?
(floorGapInTiles*this.tileHeight/(this.numFloors)) : 0; //gap in pixels if 3D & >1 flr
     this.cache = { }; //create or clear cache object
     this.cache.xSkewFactor = (1-scaleBackRowByPct); //constant controls amount of
skew, such as .8 = 80% horiz scale
     this.cache.ySkewFactor = (1 - (this.numFloors-
1)*(floorGapInTiles/this.numTiles)) / this.numFloors;
     this.cache.drawWidth = this.tileWidth * this.numTiles;
     this.cache.drawHeight = this.tileHeight * this.numTiles;
     this.cache.yOffset = ((this.numFloors - 1) - this.floorNum) *
     //amount to shift each floor down
                      ((this.cache.drawHeight/this.numFloors) + gapBetweenFloors);
                      //offset by # floors + gap
     if (this.numFloors == 1) { //if single floor
      this.cache.ySkewFactor *= vertScaleSingleFloorPct; //scale
      vertically
      this.cache.yOffset = ((1 - vertScaleSingleFloorPct) / 2) *
      this.cache.drawHeight; //and offset vertically so centered
     }
     this.cache.halfDrawWidth = this.cache.drawWidth / 2; //precompute for speed
     this.cache.xSkewMultiplier = this.cache.drawHeight * (this.cache.xSkewFactor) / 2;
     this.cache.yScaleFactor = (1-(this.cache.xSkewFactor)*(this.cache.drawHeight -
     this.startPosY)/(this.cache.drawHeight));
    }
   //compute skewed x, y positions, and scale for this row
   devScale = py*this.cache.xSkewFactor/this.cache.drawHeight +
   this.cache.yScaleFactor; //device scale: compute before altering py
   px += (1 - (px-this.startPosX)/this.cache.halfDrawWidth) * //add normal X
   factor skewing
            (1 - (py-this.startPosY)/this.cache.drawHeight) * //but diminished by Y
            factor
            this.cache.xSkewMultiplier; //then scale overall
   py = (py-this.startPosY)*this.cache.ySkewFactor + this.startPosY +
   this.cache.yOffset; //remove start pos, skew, then add back
  }
 }
 catch (ev) {
  //console.log("Home View: pSkew failed "+ev);
 }
 return {x:px, y:py, scaleFor3D:devScale};
};
```

[0373] Tapering of the floors in Home View 3D, as described in detail herein, means that the top floor is rendered slightly wider than the bottom floor. Since the render naturally has vertical gutters on the left and right edge, and these gutters are wider than needed since the floors are skewed and smaller, the algorithm of an embodiment renders the bottom floor with gutter unchanged, and reduces the top floor gutter to approximately 35% of its normal width, as an example.

[0374] Before computing all the locations for rendering a floor, an embodiment shrinks this gutter for the higher floors. For example, with 3 floors, the gutters are approximately 35%, 57%, and 100% of their typical width, but are not so limited. Since the gutters are smaller, the floors are wider, so an embodiment grows the tile widths by that same approximate percent. An example algorithm is as follows, but is not so limited:

```
if (render3D) { //This block makes the higher floors a bit wider then tapers inward to
enhance 3D illusion
```

```
  this.cache = null; //need to clear pre-computed cache from lower floors
  var gutterPct = 0.35 + 0.65*((numFloors-1)-floorNum)/((numFloors>1)?(numFloors-
1):1); //top floor: 35% gutter, bottom floor: 100% gutter
  this.startPosX *= gutterPct; //shrink startPosX that
% to shift closer to edge
  this.tileWidth *= 1 + (2*(startPosX-this.startPosX)/(this.numTiles*this.tileWidth))
  //grow tileWidth by same percent gutter shrank
 }
```

[0375] Embodiments of the integrated system described herein include a user interface (UI) that is a cross-platform UI providing control over home automation and security systems and devices from client devices including but not limited to tablets, smart phones, iOS devices, and Android devices. While conventional UIs for accessing live video and captured camera content are not integrated and do not allow for future support of Continuous Video Recording (CVR) content, an embodiment includes a Video Timeline UI that is a consistent and seamless cross-platform UI for accessing live video, saved clips and saved pictures and CVR content in the future.

[0376] **Figure 94A** is a flow diagram showing an example flow for accessing camera data via a smart phone (e.g., iPhone), under an embodiment. Access to camera data via Home View involves a user selecting a camera icon displayed on the "Home View" UI to show the Home View camera popup ("HV Popup"). Tapping a specified icon (e.g., ">" icon, etc.) on the "HV Popup" causes full-screen live video to be displayed. Access to camera data via a displayed list of cameras ("Camera List") involves a user selecting a "LIVE" icon displayed on the camera list, which results in the display of full screen live video corresponding to the selected camera. Alternatively, selecting the camera name takes a user to a clips/pictures viewer ("Clips/Pic Viewer").

[0377] **Figure 94B** is a flow diagram showing an example flow for accessing camera data via a tablet device (e.g., iPad), under an embodiment. Access to camera data via Home View involves a user selecting a camera icon displayed on the "Home View" UI, which results in presentation of a live video preview popup ("HV Popup"). Selecting a particular live video preview on the "HV Popup" initiates display of full-screen live video. Alternatively, tapping the history icon takes a user to a clips/pictures viewer ("Clip/Pic Viewer"). Access to camera data is also available via a camera list comprising a carousel ("Camera Carousel") of live video preview "scones". Starting from the displayed camera list, the user selects a particular live video preview to show full-screen video ("Full-Screen Live"). Alternatively, selecting the history icon takes a user to a clips/pictures viewer ("Clip/Pic Viewer").

[0378] The video window of an embodiment renders or presents video in landscape mode but is not so limited. The UI elements (e.g., top bar, bottom bar, paging dots, etc.) are shown by default. The UI is configured so tapping of the video window once causes the UI to be hidden, while tapping again returns the UI to the display. Selecting a "Done" icon returns the UI to the camera list.

[0379] The UI is configured so a swipe switches between cameras. Swiping pauses playback of a current camera maintaining zoom level. A new camera resumes live playback when fully snapped to full-screen video. Swipe shows the UI if it is hidden, and the UI hides again after a predetermined period of time (e.g., 5 seconds, etc.).

[0380] Live video is shown when first viewing a camera full-screen. **Figure 95** is an example of a live view including the UI, under an embodiment. The UI is configured so a tap of a "Capture" icon displays live video capture options (e.g., take clip, take picture, etc.). The UI is configured so swiping left-right results in a switch between live camera feeds. Page dots indicate the position of the current camera in the list. The portion of the timeline right of the playback head ("LIVE") represents the future and is indicated by a grey patterned area, so that swiping to this area is not possible but a drag can rubber-band into it temporarily.

[0381] The UI is configured so a tap detected on the video section hides the UI (e.g., top bar, bottom bar, pagination dots, etc.). **Figure 96** is an example of a live view with the UI hidden, under an embodiment.

[0382] If a camera event occurs while viewing live video, the event notification is displayed beneath the top bar. **Figure 97** is an example of a live view with an event notification ("Motion detected") displayed during live viewing, and with the UI displayed, under an embodiment. The notification or message bar lasts for a pre-specified period of time (e.g., 5 seconds, etc.) and then disappears.

[0383] If a camera event occurs while viewing live video, and the UI is hidden, the event notification is displayed at the top of the screen or display. **Figure 98** is an example of a live view with an event notification ("Motion detected") displayed during live viewing, and with the UI hidden, under an embodiment. The notification or message bar lasts for a predetermined period of time (e.g., 5 seconds, etc.) and then disappears.

[0384] The UI of an embodiment includes a Timeline. **Figure 99** is an example of a UI including a live camera view and the Timeline, under an embodiment. The Timeline of an embodiment is configured to provide seamless navigation between live video, stored pictures and clips, and CVR data. The Timeline is presented or displayed over pictures and video clips, but is not so limited. The Timeline of an embodiment represents clips, pictures, and CVR data for a pre-specified period of time (e.g., 10 days, 30 days, etc.). The Timeline includes data for a pre-specified period of time (e.g.,

one 24-hour day, etc.) on screen at a time and includes one or more of the following time indicators or markings: Playback head (e.g., fixed at the center of the timeline and reflects the point in time currently being viewed; when first shown, the timeline is positioned at the "LIVE" position); Live video (e.g., indicated by a vertical bar (e.g., labeled "LIVE"); when centered at the playback position, the label and bar are red); Future (e.g., indicated by a patterned grey area to the right of the Live video indicator); Day marks (e.g., indicated by vertical grey bars labeled in a format (e.g., day name, month, date); Time stamp (e.g., shown above the timeline while being actively dragged; time displayed in the format hour:minute:AM/PM).

[0385] The Timeline of an embodiment includes camera-related events comprising one or more of captured clips, captured pictures or images, and motion events, but the embodiment is not so limited. The captured clips are indicated by a blue square with arrow (see Figure 108, element 9902), centered at the time of capture, but are not so limited. Captured pictures of an embodiment are indicated by a blue open square (see Figure 108, element 9904), centered on the time of capture. Motion events are indicated in the Timeline of an embodiment by a motion icon (see Figure 108, element 9906), centered on the time of capture, positioned on a higher "track" than the camera content, but are not limited to this embodiment.

[0386] If pictures, clips and CVR data are not available, a message is displayed (e.g., "No saved videos or photos", etc.). **Figure 100** is an example of a UI including the live camera view and Timeline, and a message regarding data, under an embodiment. The Timeline is configured so swiping left-right changes playback position for browsing stored video content. When the Timeline position indicator is no longer at the LIVE viewing position, the marker and LIVE label become grey.

[0387] **Figure 101** is an example of a UI including the Timeline offset ("5:19 PM") from the live viewing position, under an embodiment. As the Timeline of an embodiment is actively dragged, the timestamp of the media playback is shown above the playback head, and is updated while dragging. The Timeline is configured so that tapping or dragging anywhere on the Timeline moves that point to the playback head, and the timeline will snap to the nearest clip or picture. If CVR data is available, the tapping or dragging action goes to the selected point on the Timeline with no snapping. The Timeline is configured so that tapping the LIVE area at the far right edge of the timeline or swiping right-left until the live indicator reaches the playback head returns the UI to the live camera view.

[0388] The Timeline of an embodiment is configured so that in response to a tap or release from a dragging operation, the timeline snaps to the nearest saved picture or clip. The screen dims and the loading spinner is displayed as the clip or picture is loaded, if necessary. **Figure 102** is an example of a UI as a clip or picture is loaded, under an embodiment. Once the clip or picture is loaded, the spinner stops and the screen changes out of the dimmed state, and the selected clip or picture is displayed. The Timeline is configured so swiping left or right navigates to the beginning of the next or previous picture or clip.

[0389] **Figure 103** is an example of a UI displaying a loaded picture (Timeline position indicator located at captured picture indicator), under an embodiment. **Figure 104** is an example of a UI displaying a loaded video clip (Timeline position indicator located at captured clip indicator), under an embodiment. Once the clip is loaded, the spinner stops and the screen changes out of the dimmed state, and the selected clip is automatically played. The progress of the video clip download is indicated by a faint fill within the playback track, and the current position of playback is indicated by a playback thumb, which is draggable in an embodiment. The time remaining in the clip is also displayed (e.g., in a left portion of the UI) in an embodiment. The time of capture is shown (e.g., above the playback track). Tapping anywhere on the playback track will resume clip playback from that point.

[0390] The UI includes a pause icon, and playback can be paused by tapping the pause. **Figure 105** is an example of a UI displaying a paused video clip, under an embodiment. When pausing, the pause icon changes to a play icon and a pause symbol is shown on screen for a pre-specified period of time (e.g., 1 second, etc.), fading away automatically. When playing, the play icon changes to a pause icon and a play symbol is shown on screen for a pre-specified period of time, fading away automatically.

[0391] **Figure 106** is an example of a UI display having completed play of a video clip, under an embodiment. At the end of playback of a video clip, the pause/play icon becomes a replay icon.

[0392] The UI of an embodiment includes Timeline zooming, in which pinch gestures detected or received change the scale of the Timeline and reveal or hide timeline event icons. The UI is configured to pinch-out to zoom in to the Timeline. Zooming in spreads apart overlapping events, and allows finer control over moving the playhead. As the timeline zooms in, tick marks fade in and out to show the most appropriate time measurements.

[0393] Zoom Out is realized in a direction opposite that of zoom in (e.g., pinch-in). Zooming out can cause nearby event icons to overlap, but is not so limited. The most recent event is positioned on top (thus tappable).

[0394] The UI of an embodiment includes Timeline scaling in which zooming in and out scales the timeline to seamlessly cross fade to the new scale. New labels, icons and tick marks fade in, and original labels, icons and tick marks will fade out. The Timeline of an example embodiment presents 24 hours on-screen, with tick marks every twelve hours, and any zoom-in causes the Timeline to add hour tick marks (e.g., zoom-in more than 2x (12 hours on screen) adds half-hour tick marks, etc.). In this example, the largest scale includes a 5-day view showing five days of information, and having

tick marks presented in 24-hour increments. Another Timeline scale is a 24-hour view presents one day of information, and having tick marks presented in 12-hours apart. A one-hour increment view presents approximately two days of information, with tick marks presented in one-hour increments. A five-minute increment view presents approximately two hours of information, with tick marks presented in five-minute increments. The scaling of an embodiment also includes a one-minute increment view that includes tick marks presented in one-minute increments.

[0395] The UI of an embodiment includes a zoom map but is not so limited. The zoom map, which is positioned in a portion or region of the UI display, repositions itself depending on the size of the top bar. **Figure 107** is an example of a UI having no top bar and on which the zoom map is positioned in a top region of the display, under an embodiment. **Figure 108** is an example of a UI having a relatively minimal top bar, with a zoom map is positioned on the display just below the top bar, under an embodiment. **Figure 109** is an example of a UI having a relatively large top bar, with a zoom map is positioned on the display just below the top bar, under an embodiment.

[0396] **Figure 110** is an example of a UI including the Timeline with CVR data, under an embodiment. The UI of an embodiment indicates CVR content or data on the Timeline using filled portions. The filled portions may not be contiguous, but the embodiment is not so limited. The UI is configured so that a swipe or tap detected at any location on the timeline (where CVR data is indicated) causes play of the CVR data. On release, the screen dims and the loading spinner is shown. When loaded, the spinner stops, the screen returns to normal contrast, and the video plays. When CVR is available, concurrent pictures and/or video clips from server are not shown in an embodiment but the CVR material is shown, but the embodiment is not so limited. When a camera event occurs, the event notification is overlaid on the video clip, and an event marker is presented or displayed on the timeline.

[0397] A typical swipe on the Timeline provides 1:1 movement of the Timeline. A relatively fast swipe provides accelerated scrolling with inertia, allowing access to the entire span of the timeline within a pre-specified number of swipes (e.g., 10 swipes). Conversely, a slow drag provides fine-grained control with magnification, enabling selection of individual, closely spaced captured clips or pictures. Slow drag in an embodiment is activated or triggered by a long press; the Timeline remains magnified while dragging until touch end, but is not so limited.

[0398] The Timeline of an embodiment is configured for magnification. **Figure 111** is an example of a UI including the Timeline with magnification, under an embodiment. When magnified, a center portion (e.g., center 50%, etc.) of the Timeline zooms in to a pre-specified magnification (e.g., 24x magnification, etc.), decreasing its scope to show a pre-specified period of time (e.g., one hour, etc.). The non-magnified portion of the Timeline continues to move during dragging, but moves at a much slower rate than the zoomed portion of the Timeline. The relative rates of movement of the magnified and unmagnified portions of the Timeline are proportional to the relative sizes of the magnified and unmagnified portions. While magnified, tick marks or indicators presented on the Timeline become visible, time-interval indicators or time stamps become visible, and the unmagnified portion of the timeline is slightly tinted.

[0399] **Figure 112** is an example of a UI configured to include thumbnail images in the Timeline, under an embodiment. When the Timeline is configured to include thumbnail images, the picture and/or video clip icons are replaced with actual thumbnail images representing the image or video data.

Embodiments include a system comprising an automation network comprising a gateway at a premises, wherein the gateway is coupled to a remote network, wherein the gateway is configured to control a plurality of components at the premises including premises devices and a security system comprising security system components, wherein the plurality of components include at least one camera and a sensor user interface (SUI) coupled to the gateway and presented to a user via a plurality of remote client devices, wherein the SUI includes a plurality of display elements for managing and receiving data of the plurality of components agnostically across the plurality of remote client devices, wherein the plurality of display elements includes a timeline user interface comprising event data of the plurality of components positioned at a time corresponding to events.

[0400] The timeline user interface comprises a variable-length timeline.

[0401] A time scale of the timeline user interface can be dynamically changed.

[0402] The event data may comprise component state of the plurality of components presented in a timeline.

[0403] The event data of the plurality of components may include at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0404] The timeline user interface may include at least one icon corresponding to the at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0405] The timeline user interface may include at least one thumbnail image corresponding to the at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0406] A captured clip may include continuous video recording for a period of time.

[0407] An event captured in at least one of the live video, captured clips and captured pictures may be depicted on the timeline user interface using icons.

[0408] The event data of the plurality of components may include live video of the at least one camera.

[0409] The event data of the plurality of components may include captured clips of the at least one camera.

[0410] The event data of the plurality of components may include captured pictures of the at least one camera.

[0411] The event data of the plurality of components may include motion events of the at least one camera.

[0412] The timeline user interface may be configured to control navigation between live video, captured clips and captured pictures of the at least one camera.

[0413] A tap detected at a position on the timeline user interface may cause the timeline user interface to snap to and display one of a captured clip and captured picture nearest the position.

[0414] The timeline user interface may be configured to display concurrent ones of the captured clip and captured picture nearest the position.

[0415] When continuous video recording is available at the position, the continuous video recording may be presented instead of concurrent ones of the captured clip and captured picture nearest the position.

[0416] The system may include a dedicated coupling between a processor of the gateway and a controller of the security system, wherein the controller is coupled to the security system components.

[0417] The controlling of the plurality of components at the premises may include controlling interoperability among the plurality of components.

[0418] The gateway may be configured using data of the plurality of components.

[0419] At least one of the gateway and the plurality of remote devices may be configured to perform a synchronization to associate the plurality of remote devices with the plurality of components.

[0420] The plurality of remote devices may include applications that receive the data from and transmit control instructions to the plurality of components via the gateway.

[0421] The gateway may be coupled to the security system via a first network.

[0422] The first network may be a dedicated network.

[0423] The gateway may be coupled to the premises devices via a second network.

[0424] The plurality of remote client devices may include one or more of a smart phone, a mobile phone, a cellular phone, a tablet computer, a personal computer, and a touchscreen device.

[0425] The plurality of display elements may include an icon that visually indicates a state of the plurality of components.

[0426] The icon may be configured to control the plurality of components.

[0427] The plurality of display elements may include at least one warning that is an informational warning of the plurality of components.

[0428] The at least one warning may correspond to at least one of a camera device, a lighting device, a lock device, and a thermostat device.

[0429] The plurality of display elements may include display elements comprising a representation of a floor plan layout of the premises, wherein the floor plan layout includes representations of the plurality of components.

[0430] The floor plan layout may visually and separately indicate a location and a state of the plurality of components, wherein the state includes current state and historical state.

[0431] The floor plan layout may include a three-dimensional representation of the floor plan.

[0432] The floor plan layout may include a two-dimensional representation of the floor plan.

[0433] The floor plan layout may include configuration data for each of the plurality of components.

[0434] Embodiments include a system comprising an automation network including a gateway at a premises. The gateway is coupled to a remote network. The gateway is configured to control a plurality of components at the premises including premises devices and a security system comprising security system components. The plurality of components includes at least one camera. The system includes a sensor user interface (SUI) coupled to the gateway and presented to a user via a plurality of remote client devices. The SUI includes a plurality of display elements for managing and receiving data of the plurality of components agnostically across the plurality of remote client devices. The plurality of display elements includes a timeline user interface comprising event data of the plurality of components positioned at a time corresponding to events.

[0435] Embodiments include a system comprising: an automation network comprising a gateway at a premises, wherein the gateway is coupled to a remote network, wherein the gateway is configured to control a plurality of components at the premises including premises devices and a security system comprising security system components, wherein the plurality of components include at least one camera; and a sensor user interface (SUI) coupled to the gateway and presented to a user via a plurality of remote client devices, wherein the SUI includes a plurality of display elements for managing and receiving data of the plurality of components agnostically across the plurality of remote client devices, wherein the plurality of display elements includes a timeline user interface comprising event data of the plurality of components positioned at a time corresponding to events.

[0436] The timeline user interface comprises a variable-length timeline.

[0437] A time scale of the timeline user interface can be dynamically changed.

[0438] The event data may comprise component state of the plurality of components presented in a timeline.

[0439] The event data of the plurality of components may include at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0440] The timeline user interface may include at least one icon corresponding to the at least one of live video, captured

clips, captured pictures, and motion events of the at least one camera.

[0441] The timeline user interface may include at least one thumbnail image corresponding to the at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0442] A captured clip may include continuous video recording for a period of time.

[0443] An event captured in at least one of the live video, captured clips and captured pictures may be depicted on the timeline user interface using icons.

[0444] The event data of the plurality of components may include live video of the at least one camera.

[0445] The event data of the plurality of components may include captured clips of the at least one camera.

[0446] The event data of the plurality of components may include captured pictures of the at least one camera.

[0447] The event data of the plurality of components may include motion events of the at least one camera.

[0448] The timeline user interface may be configured to control navigation between live video, captured clips and captured pictures of the at least one camera.

[0449] A tap detected at a position on the timeline user interface may cause the timeline user interface to snap to and display one of a captured clip and captured picture nearest the position.

[0450] The timeline user interface may be configured to display concurrent ones of the captured clip and captured picture nearest the position.

[0451] When continuous video recording is available at the position, the continuous video recording may be presented instead of concurrent ones of the captured clip and captured picture nearest the position.

[0452] The system may include a dedicated coupling between a processor of the gateway and a controller of the security system, wherein the controller is coupled to the security system components.

[0453] The controlling of the plurality of components at the premises may include controlling interoperability among the plurality of components.

[0454] The gateway may be configured using data of the plurality of components.

[0455] At least one of the gateway and the plurality of remote devices may be configured to perform a synchronization to associate the plurality of remote devices with the plurality of components.

[0456] The plurality of remote devices may include applications that receive the data from and transmit control instructions to the plurality of components via the gateway.

[0457] The gateway may be coupled to the security system via a first network.

[0458] The first network may be a dedicated network.

[0459] The gateway may be coupled to the premises devices via a second network.

[0460] The plurality of remote client devices may include one or more of a smart phone, a mobile phone, a cellular phone, a tablet computer, a personal computer, and a touchscreen device.

[0461] The plurality of display elements may include an icon that visually indicates a state of the plurality of components.

[0462] The icon may be configured to control the plurality of components.

[0463] The plurality of display elements may include at least one warning that is an informational warning of the plurality of components.

[0464] The at least one warning may correspond to at least one of a camera device, a lighting device, a lock device, and a thermostat device.

[0465] The plurality of display elements may include display elements comprising a representation of a floor plan layout of the premises, wherein the floor plan layout includes representations of the plurality of components.

[0466] The floor plan layout may visually and separately indicate a location and a state of the plurality of components, wherein the state includes current state and historical state.

[0467] The floor plan layout may include a three-dimensional representation of the floor plan.

[0468] The floor plan layout may include a two-dimensional representation of the floor plan.

[0469] The floor plan layout may include configuration data for each of the plurality of components.

[0470] Embodiments include a method comprising configuring an automation network to include a gateway at a premises, wherein the gateway is coupled to a remote network, configuring the gateway to control a plurality of components at the premises including premises devices and a security system comprising security system components, wherein the plurality of components include at least one camera, configuring a sensor user interface (SUI) to include a plurality of display elements for managing and receiving data of the plurality of components agnostically across the plurality of remote client devices, wherein the SUI is coupled to the gateway and presented to a user via a plurality of remote client devices, wherein the plurality of display elements includes a timeline user interface comprising event data of the plurality of components positioned at a time corresponding to events.

[0471] The event data may comprise component state of the plurality of components presented in a timeline.

[0472] The event data of the plurality of components may include at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0473] The method may include configuring the timeline user interface to include at least one icon corresponding to the at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0474] The method may include configuring the timeline user interface to include at least one thumbnail image corresponding to the at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0475] A captured clip may include continuous video recording for a period of time.

[0476] The method may include configuring the timeline user interface to depict an event captured in at least one of the live video, captured clips and captured pictures using icons.

[0477] The event data of the plurality of components may include live video of the at least one camera.

[0478] The event data of the plurality of components may include captured clips of the at least one camera.

[0479] The event data of the plurality of components may include captured pictures of the at least one camera.

[0480] The event data of the plurality of components may include motion events of the at least one camera.

[0481] The method may include configuring the timeline user interface to control navigation between live video, captured clips and captured pictures of the at least one camera.

[0482] A tap detected at a position on the timeline user interface may cause the timeline user interface to snap to and display one of a captured clip and captured picture nearest the position.

[0483] The method may include configuring the timeline user interface to display concurrent ones of the captured clip and captured picture nearest the position.

[0484] When continuous video recording is available at the position, the continuous video recording may be presented instead of concurrent ones of the captured clip and captured picture nearest the position.

[0485] The method may include a dedicated coupling between a processor of the gateway and a controller of the security system, wherein the controller is coupled to the security system components.

[0486] The controlling of the plurality of components at the premises may include controlling interoperability among the plurality of components.

[0487] The method may include configuring the gateway using data of the plurality of components.

[0488] The method may include configuring at least one of the gateway and the plurality of remote devices to perform a synchronization to associate the plurality of remote devices with the plurality of components.

[0489] The plurality of remote devices may include applications that receive the data from and transmit control instructions to the plurality of components via the gateway.

[0490] The gateway may be coupled to the security system via a first network, and is coupled to the premises devices via a second network.

[0491] The method may include configuring the plurality of display elements to include a representation of a floor plan layout of the premises, wherein the floor plan layout includes representations of the plurality of components.

[0492] The floor plan layout may visually and separately indicate a location and a state of the plurality of components, wherein the state includes current state and historical state.

[0493] The floor plan layout may include a three-dimensional representation of the floor plan.

[0494] Embodiments include a method comprising configuring an automation network to include a gateway at a premises. The gateway is coupled to a remote network. The method includes configuring the gateway to control a plurality of components at the premises including premises devices and a security system comprising security system components. The plurality of components includes at least one camera. The method includes configuring a sensor user interface (SUI) to include a plurality of display elements for managing and receiving data of the plurality of components agnostically across the plurality of remote client devices. The SUI is coupled to the gateway and presented to a user via a plurality of remote client devices. The plurality of display elements includes a timeline user interface comprising event data of the plurality of components positioned at a time corresponding to events.

[0495] Embodiments include a method comprising: configuring an automation network to include a gateway at a premises, wherein the gateway is coupled to a remote network; configuring the gateway to control a plurality of components at the premises including premises devices and a security system comprising security system components, wherein the plurality of components include at least one camera; configuring a sensor user interface (SUI) to include a plurality of display elements for managing and receiving data of the plurality of components agnostically across the plurality of remote client devices, wherein the SUI is coupled to the gateway and presented to a user via a plurality of remote client devices, wherein the plurality of display elements includes a timeline user interface comprising event data of the plurality of components positioned at a time corresponding to events.

[0496] The event data may comprise component state of the plurality of components presented in a timeline.

[0497] The event data of the plurality of components may include at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0498] The method may include configuring the timeline user interface to include at least one icon corresponding to the at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0499] The method may include configuring the timeline user interface to include at least one thumbnail image corresponding to the at least one of live video, captured clips, captured pictures, and motion events of the at least one camera.

[0500] A captured clip may include continuous video recording for a period of time.

[0501] The method may include configuring the timeline user interface to depict an event captured in at least one of

the live video, captured clips and captured pictures using icons.

[0502] The event data of the plurality of components may include live video of the at least one camera.

[0503] The event data of the plurality of components may include captured clips of the at least one camera.

[0504] The event data of the plurality of components may include captured pictures of the at least one camera.

[0505] The event data of the plurality of components may include motion events of the at least one camera.

[0506] The method may include configuring the timeline user interface to control navigation between live video, captured clips and captured pictures of the at least one camera.

[0507] A tap detected at a position on the timeline user interface may cause the timeline user interface to snap to and display one of a captured clip and captured picture nearest the position.

[0508] The method may include configuring the timeline user interface to display concurrent ones of the captured clip and captured picture nearest the position.

[0509] When continuous video recording is available at the position, the continuous video recording may be presented instead of concurrent ones of the captured clip and captured picture nearest the position.

[0510] The method may include a dedicated coupling between a processor of the gateway and a controller of the security system, wherein the controller is coupled to the security system components.

[0511] The controlling of the plurality of components at the premises may include controlling interoperability among the plurality of components.

[0512] The method may include configuring the gateway using data of the plurality of components.

[0513] The method may include configuring at least one of the gateway and the plurality of remote devices to perform a synchronization to associate the plurality of remote devices with the plurality of components.

[0514] The plurality of remote devices may include applications that receive the data from and transmit control instructions to the plurality of components via the gateway.

[0515] The gateway may be coupled to the security system via a first network, and is coupled to the premises devices via a second network.

[0516] The method may include configuring the plurality of display elements to include a representation of a floor plan layout of the premises, wherein the floor plan layout includes representations of the plurality of components.

[0517] The floor plan layout may visually and separately indicate a location and a state of the plurality of components, wherein the state includes current state and historical state.

[0518] The floor plan layout may include a three-dimensional representation of the floor plan.

[0519] As described above, computer networks suitable for use with the embodiments described herein include local area networks (LAN), wide area networks (WAN), Internet, or other connection services and network variations such as the world wide web, the public internet, a private internet, a private computer network, a public network, a mobile network, a cellular network, a value-added network, and the like. Computing devices coupled or connected to the network may be any microprocessor controlled device that permits access to the network, including terminal devices, such as personal computers, workstations, servers, mini computers, main-frame computers, laptop computers, mobile computers, palm top computers, hand held computers, mobile phones, TV set-top boxes, or combinations thereof. The computer network may include one of more LANs, WANs, Internets, and computers. The computers may serve as servers, clients, or a combination thereof.

[0520] The integrated security system can be a component of a single system, multiple systems, and/or geographically separate systems. The integrated security system can also be a subcomponent or subsystem of a single system, multiple systems, and/or geographically separate systems. The integrated security system can be coupled to one or more other components (not shown) of a host system or a system coupled to the host system.

[0521] One or more components of the integrated security system and/or a corresponding system or application to which the integrated security system is coupled or connected includes and/or runs under and/or in association with a processing system. The processing system includes any collection of processor-based devices or computing devices operating together, or components of processing systems or devices, as is known in the art. For example, the processing system can include one or more of a portable computer, portable communication device operating in a communication network, and/or a network server. The portable computer can be any of a number and/or combination of devices selected from among personal computers, personal digital assistants, portable computing devices, and portable communication devices, but is not so limited. The processing system can include components within a larger computer system.

[0522] The processing system of an embodiment includes at least one processor and at least one memory device or subsystem. The processing system can also include or be coupled to at least one database. The term "processor" as generally used herein refers to any logic processing unit, such as one or more central processing units (CPUs), digital signal processors (DSPs), application-specific integrated circuits (ASIC), etc. The processor and memory can be monolithically integrated onto a single chip, distributed among a number of chips or components, and/or provided by some combination of algorithms. The methods described herein can be implemented in one or more of software algorithm(s), programs, firmware, hardware, components, circuitry, in any combination.

[0523] The components of any system that includes the integrated security system can be located together or in

separate locations. Communication paths couple the components and include any medium for communicating or transferring files among the components. The communication paths include wireless connections, wired connections, and hybrid wireless/wired connections. The communication paths also include couplings or connections to networks including local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), proprietary networks, interoffice or backend networks, and the Internet. Furthermore, the communication paths include removable fixed mediums like floppy disks, hard disk drives, and CD-ROM disks, as well as flash RAM, Universal Serial Bus (USB) connections, RS-232 connections, telephone lines, buses, and electronic mail messages.

[0524] Aspects of the integrated security system and corresponding systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including programmable logic devices (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects of the integrated security system and corresponding systems and methods include: microcontrollers with memory (such as electronically erasable programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the integrated security system and corresponding systems and methods may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

[0525] It should be noted that any system, method, and/or other components disclosed herein may be described using computer aided design tools and expressed (or represented), as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, nonvolatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., HTTP, FTP, SMTP, etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of the above described components may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

[0526] Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of "including, but not limited to." Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words "herein," "hereunder," "above," "below," and words of similar import, when used in this application, refer to this application as a whole and not to any particular portions of this application. When the word "or" is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

[0527] The above description of embodiments of the integrated security system and corresponding systems and methods is not intended to be exhaustive or to limit the systems and methods to the precise forms disclosed. While specific embodiments of, and examples for, the integrated security system and corresponding systems and methods are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the systems and methods, as those skilled in the relevant art will recognize. The teachings of the integrated security system and corresponding systems and methods provided herein can be applied to other systems and methods, not only for the systems and methods described above.

[0528] The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the integrated security system and corresponding systems and methods in light of the above detailed description.

Claims

1. A method comprising:

receiving, from a camera of a system located at a premises, event data;
displaying a user interface associated with the system, wherein the user interface comprises:

a timeline comprising a time period indicator corresponding, at least in part, to a time period represented by the event data; and
an icon at a location on the timeline, wherein the location is indicative of a time point within the time period, wherein the icon is associated with a portion of the event data, wherein the portion of the event data is selected based at least on the time point; and

causing, responsive to an activation of the icon, the user interface to display the portion of the event data associated with the icon.

2. The method of claim 1, wherein the event data comprises at least one of live video, a captured clip, a still image, and an indication of a motion event from the camera.

3. The method of claim 1 or 2, wherein the event data comprises at least one of concurrent data or continuous data for the time period.

4. The method of claim 1, 2, or 3, wherein the activation of the icon is based at least on a tapping or a dragging via the user interface.

5. The method of one of claims 1-4, wherein the event data comprises an image and a video captured, concurrently, by the camera.

6. The method of one of claims 1-5, wherein the method further comprises transmitting the event data to at least one remote device.

7. The method of one of claims 1-6, wherein the timeline comprises a variable-length timeline.

8. The method of one of claims 1-7, wherein the timeline comprises a scale, and wherein the scale can be dynamically changed.

9. The method of one of claims 1-8, wherein the method further comprises displaying, via the user interface, an indication of movement detected by the camera.

10. The method of one of claims 1-9, wherein the portion of the event data associated with the icon comprises an indication of an event associated with the time point.

11. The method of claim 10, wherein the portion of the event data is selected based at least on the event.

12. The method of one of claims 1-11, wherein the event data comprises portions of data, wherein each of portions of data is associated with a respective time interval.

13. The method of claim 12, wherein the portion of the event data associated with the icon comprises at least one of the portions of data, and wherein the at least one of the portions of data is selected based at least on the respective time interval of the at least one of the portions of data being near the time point associated with the icon on the timeline.

14. An apparatus configured to implement the method of any one of claims 1-13.

15. A device comprising:

one or more processors; and
memory storing instructions that, when executed by the one or more processors, cause the device to perform the method of any one of claims 1-13.

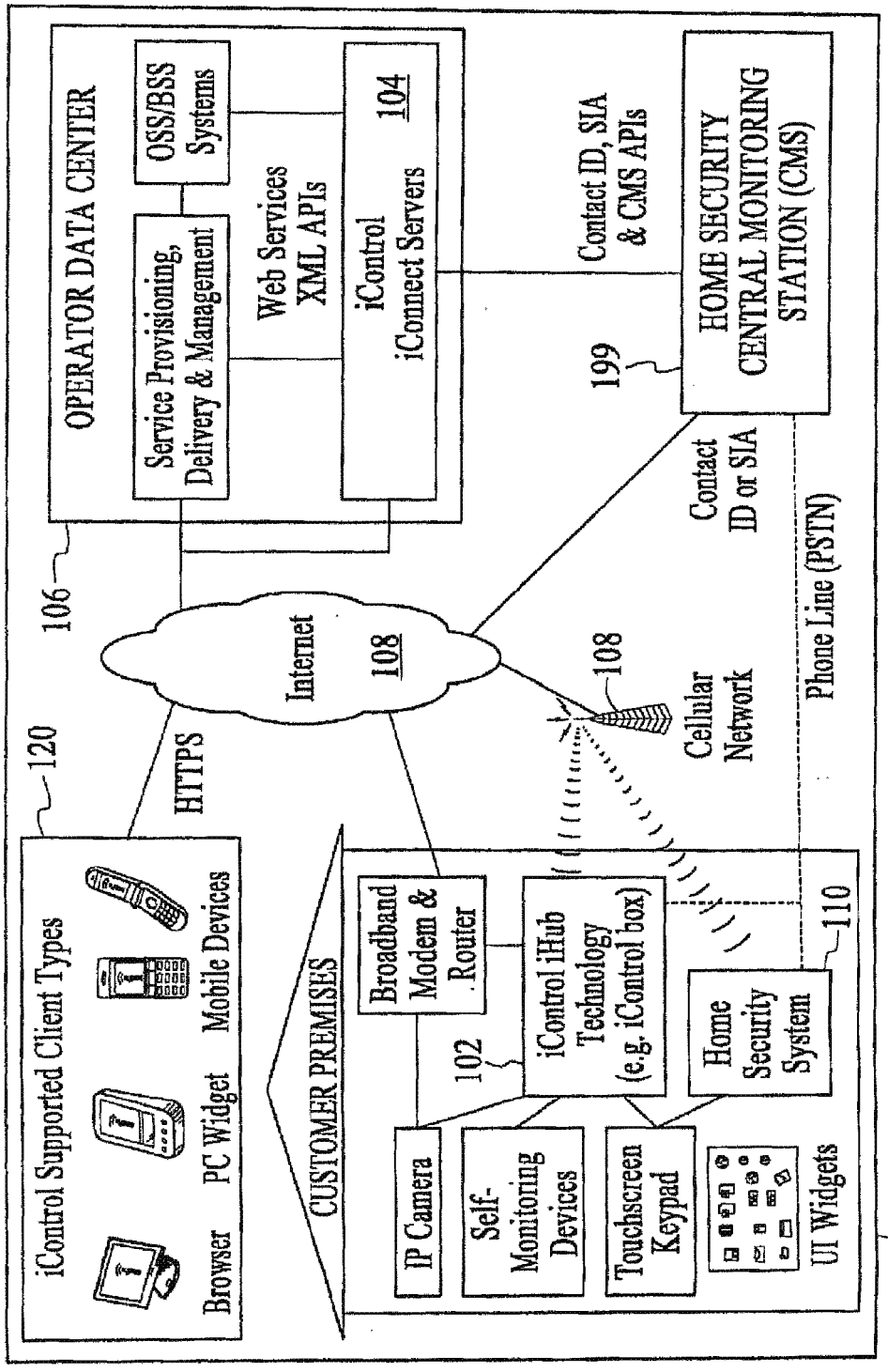

OPERATOR DATA CENTER
OSS/BSS Systems
Service Provisioning, Delivery & Management
Web Services XML APIs
iControl iConnect Servers
104
106
Contact ID, SIA & CMS APIs
199
HOME SECURITY CENTRAL MONITORING STATION (CMS)
Internet
108
Contact ID or SIA
Cellular Network
108
Phone Line (PSTN)
HTTPS
120
iControl Supported Client Types
Browser
PC Widget
Mobile Devices
CUSTOMER PREMISES
Broadband Modem & Router
iControl iHub Technology (e.g. iControl box)
102
IP Camera
Self-Monitoring Devices
Touchscreen Keypad
Home Security System
110
UI Widgets
100

FIG.1

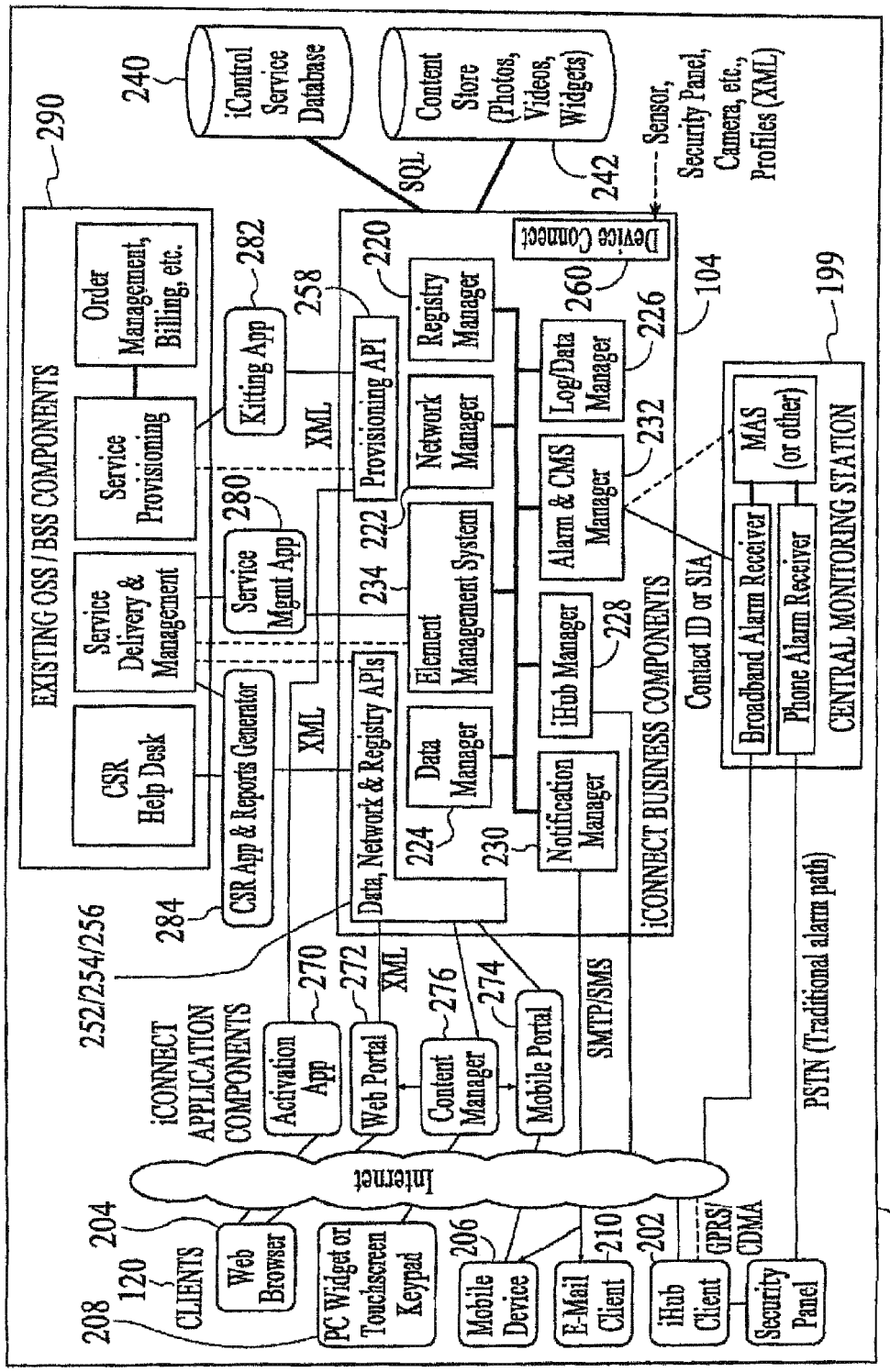

EXISTING OSS / BSS COMPONENTS
290
CSR Help Desk
Service Delivery & Management
Service Provisioning
Order Management, Billing, etc.
CSR App & Reports Generator
284
Service Mgmt App
280
Kitting App
282
iControl Service Database
240
Content Store (Photos, Videos, Widgets)
242
SQL
Sensor, Security Panel, Camera, etc., Profiles (XML)
XML
258
220
Provisioning API
Registry Manager
Network Manager
Element Management System
222
234
Device Connect
260
Log/Data Manager
226
104
Alarm & CMS Manager
232
iHub Manager
228
Data Manager
224
230
Notification Manager
Data, Network & Registry APIs
iCONNECT BUSINESS COMPONENTS
Contact ID or SIA
Broadband Alarm Receiver
Phone Alarm Receiver
MAS (or other)
CENTRAL MONITORING STATION
199
252/254/256
iCONNECT APPLICATION COMPONENTS
Activation App
270
Web Portal
272
Content Manager
276
Mobile Portal
274
XML
SMTP/SMS
PSTN (Traditional alarm path)
Internet
204
208
120
CLIENTS
Web Browser
PC Widget or Touchscreen Keypad
206
Mobile Device
210
E-Mail Client
202
iHub Client
GPRS/ CDMA
Security Panel
100

FIG.2

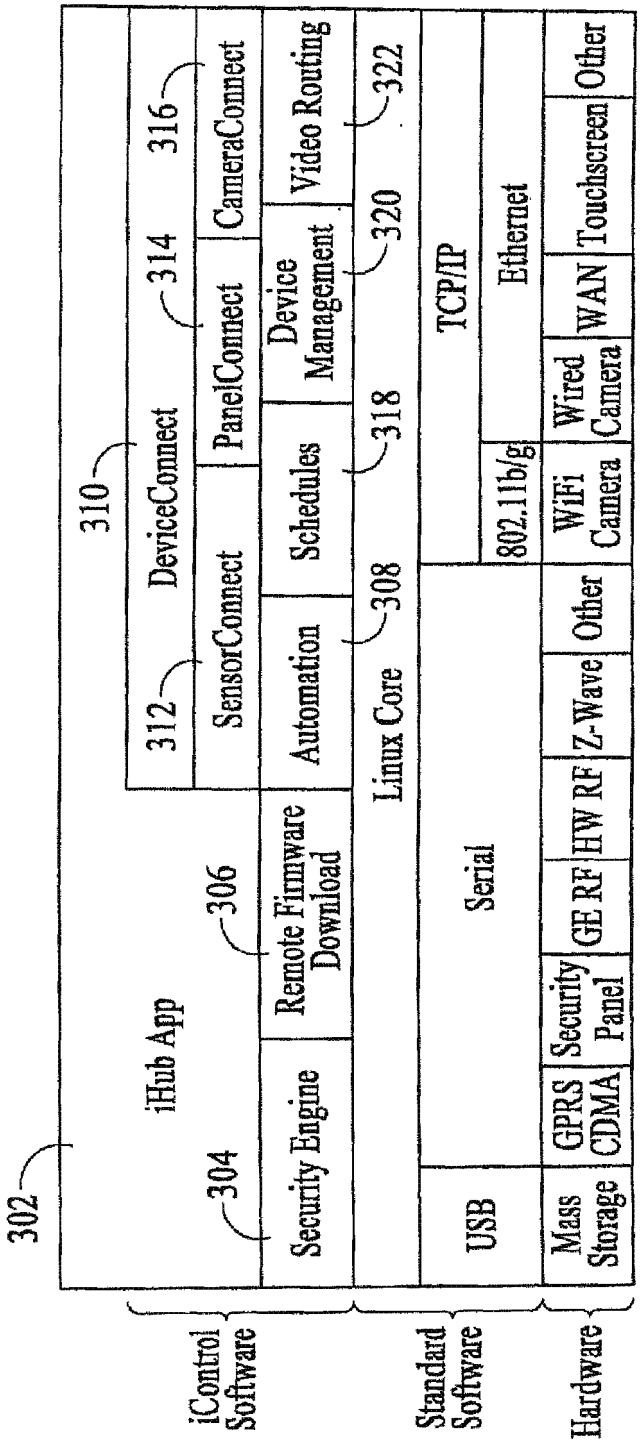

102
302
iHub App
310
312
DeviceConnect
314
316
304
306
SensorConnect
PanelConnect
CameraConnect
Security Engine
Remote Firmware Download
Automation
Schedules
Device Management
Video Routing
Linux Core
308
318
320
322
USB
Serial
TCP/IP
802.11b/g
Ethernet
Mass Storage
GPRS CDMA
Security Panel
GE RF
HW RF
Z-Wave
Other
WiFi Camera
Wired Camera
WAN
Touchscreen
Other
iControl Software
Standard Software
Hardware

FIG.3

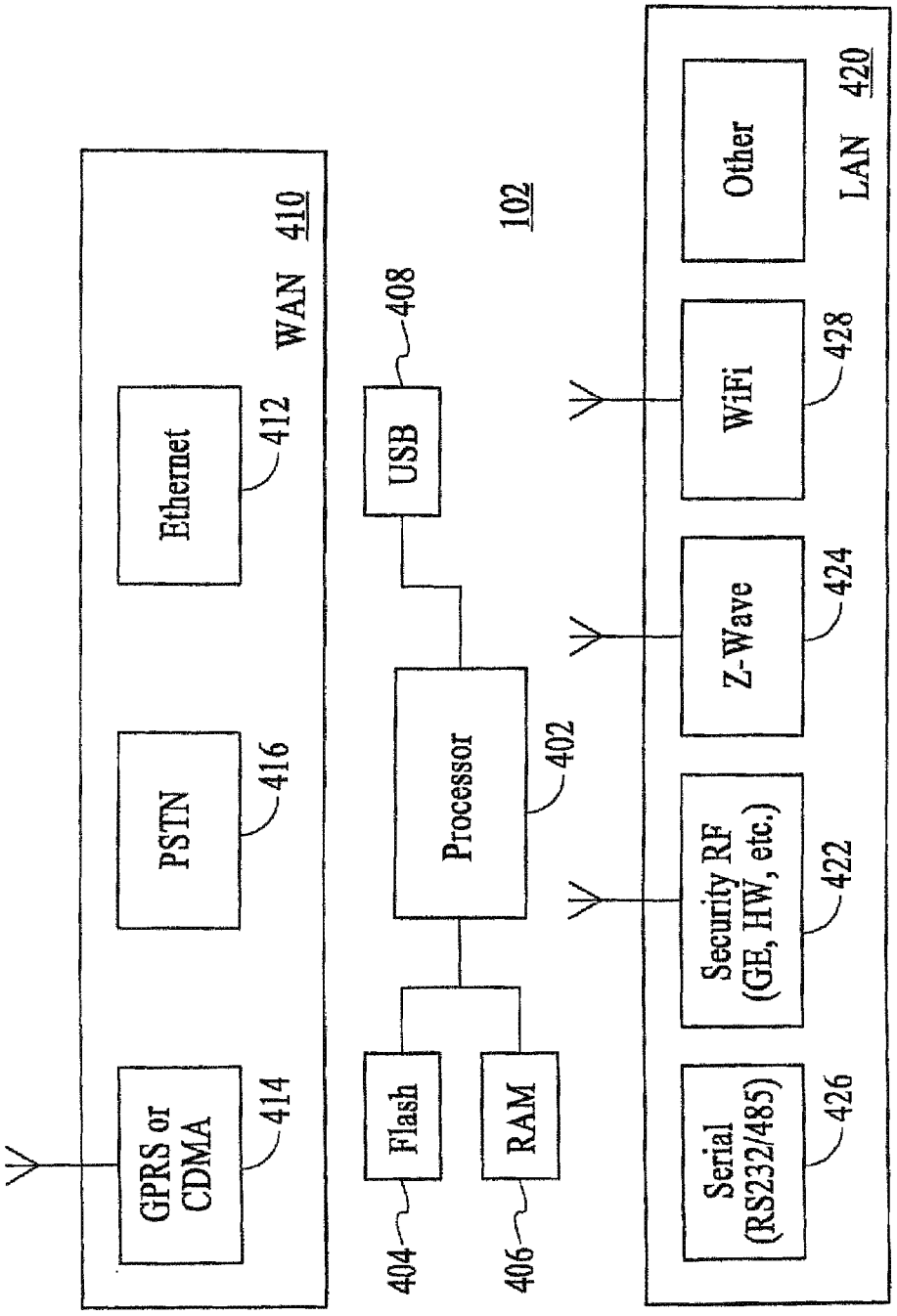

WAN 410
Ethernet
412
PSTN
416
GPRS or CDMA
414
102
USB
408
Processor
402
Flash
404
RAM
406
LAN 420
Other
WiFi
428
Z-Wave
424
Security RF (GE, HW, etc.)
422
Serial (RS232/485)
426

FIG.4

4001 4002

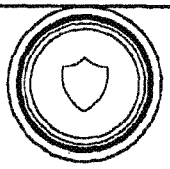
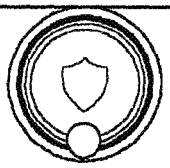
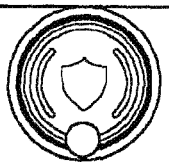
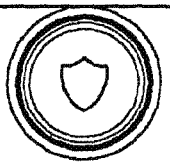
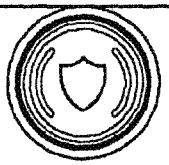
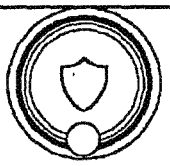
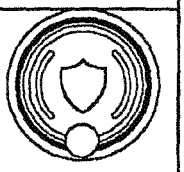
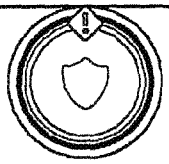
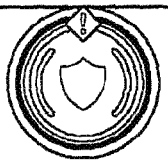
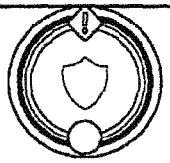
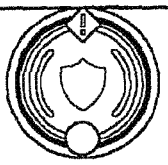
	All Quiet	Motion	Open	Open & Motion
Disarmed. OR Subdisarmed.	 Disarmed. All Quiet. 4010	 Disarmed. Motion. 4011	 Disarmed. [# sensors open] Sensor(s) Open. 4012	 Disarmed. [# sensors open] Sensor(s) Open. 4013
Armed [D&W, Stay, Away, All, Night Stay, Instant, Motion, Maximum].	 Armed Doors & Windows. All Quiet. 4014	 Armed Doors & Windows. Motion. 4015	 Armed Doors & Windows. [# sensors open] Sensor(s) Open. 4016	 Armed Doors & Windows. [# sensors open] Sensor(s) Open. 4017
Disarmed. OR Subdisarmed. Sensor AWOL, tripped, tampered, or low battery. Uncleared Alarm.	 Disarmed. Sensor Problem. 4018	 Disarmed. Sensor Problem. 4019	 Disarmed. Sensor Problem. 4020	 Disarmed. Sensor Problem. 4021

FIG. 5A

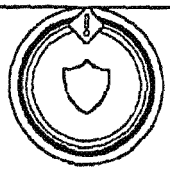
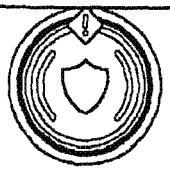
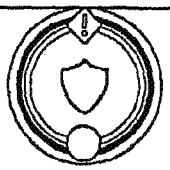
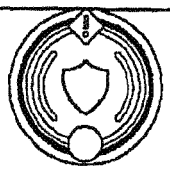
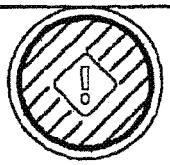
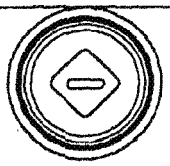
Armed [D&W, Stay, Away, All, Night Stay, Instant, Motion, Maximum]. Sensor AWOL, tripped, tampered, or low battery.	 Armed Doors & Windows. Sensor Problem. 4022	 Armed Doors & Windows. Sensor Problem. 4023	 Armed Doors & Windows. Sensor Problem. 4024	 Armed Doors & Windows. Sensor Problem. 4025
Alarm	 Armed Away/Stay. [ALARM TYPE] ALARM. 4026			
No iHub Connection (broadband offline, etc). No Security panel Connection.	 Status Unavailable. 4027			

FIG. 5B

Security State 4030		Sensor Status 4032
Armed Doors & Windows.		Uncleared Alarm.
Armed All.		Sensor Tripped.
Armed Stay.		Sensor Problem.
Armed Away.		Sensor(s) Bypassed.
Disarmed.		Motion.
Armed Maximum.		All Quiet.
Armed Night Stay.		
Armed Stay Instant.		[# of sensors open] Sensor(s) Open.
Armed Away Instant.		"1 Sensor Open."
Armed Motion.		OR
Subdisarmed.		"[# of sensors open] Sensors Open."

FIG. 6

System State	Icon	Warning Text
Primary connection is broadband. Broadband is down. Cellular being used.		Using cellular connection
Primary connection is broadband. Broadband and cellular are down.		No cellular connection
Primary connection is broadband. Broadband is down. No cellular backup installed.		Broadband connection unknown
Primary connection is cellular. Cellular is down.		No cellular connection
Security panel not connected to AC power		Security panel AC power loss
Security panel low battery		Security panel low battery
Security panel tampered		Security panel tampered
Sensor(s) bypassed	No Icon	Sensor(s) bypassed

FIG. 7

Sensor State / Sort Order	Icon	Sensor name	Status Text
1. Breached & any sensor state		[Sensor name] (Zone #)	ALARM, [Sensor state]
2. Tripped (Smoke, Water, Gas, Freeze, etc.)		[Sensor name] (Zone #)	Tripped
3. Tampered		[Sensor name] (Zone #)	Tampered, [Sensor state]
4. Low Battery		[Sensor name] (Zone #)	Low Battery, [Sensor state]
5. Offline / AWOL		[Sensor name] (Zone #)	Offline
*6. Unknown**		[Sensor name] (Zone #)	Unknown
7. Installing		[Sensor name] (Zone #)	Installing
8. Open		[Sensor name]	[Sensor state]
9. Motion		[Sensor name]	[Sensor state]
10. Bypassed		[Sensor name]	Bypassed, [Sensor state]
Quiet Sensors:			
Okay, Closed, No Motion		[Sensor name]	[Sensor state]

FIG. 8

EP 3 285 238 A2

 (red diamond bang) = tamper, offline, bypassed, installing, battery

 (yellow triangle) = open or triggered

 (wavy lines) = motion

FIG. 9

	Icon Description	Sensor State
	Green circle	Closed, No Motion, Okay

FIG. 10

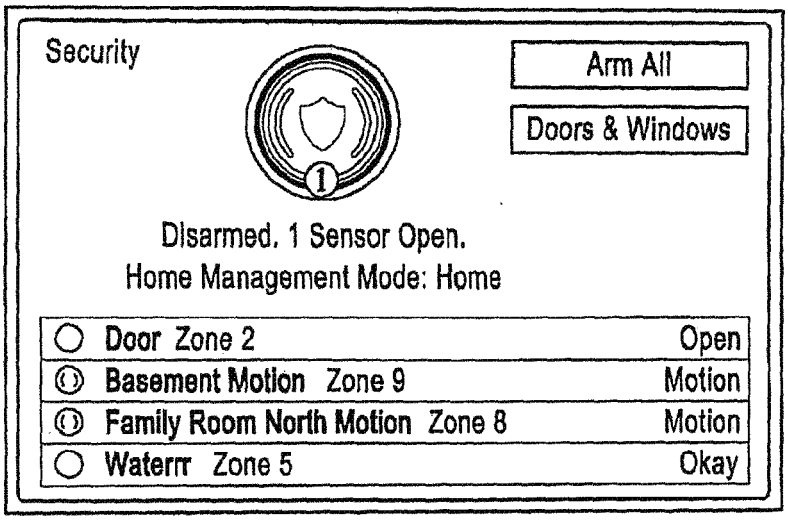

Security
Arm All
Doors & Windows
1
Disarmed. 1 Sensor Open.
Home Management Mode: Home
Door Zone 2
Open
Basement Motion Zone 9
Motion
Family Room North Motion Zone 8
Motion
Waterrr Zone 5
Okay

FIG. 11

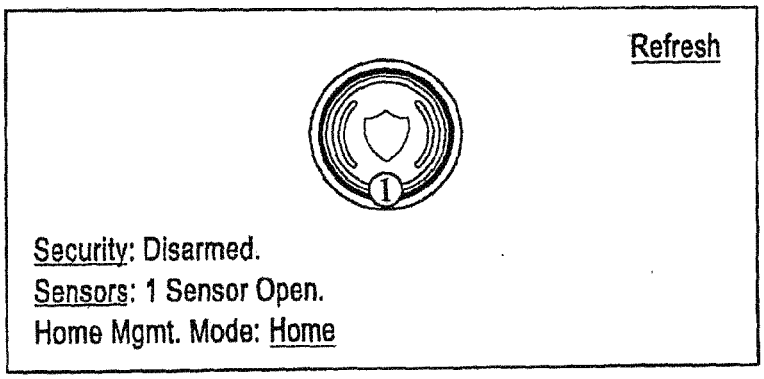

Refresh
1
Security: Disarmed.
Sensors: 1 Sensor Open.
Home Mgmt. Mode: Home

FIG. 12

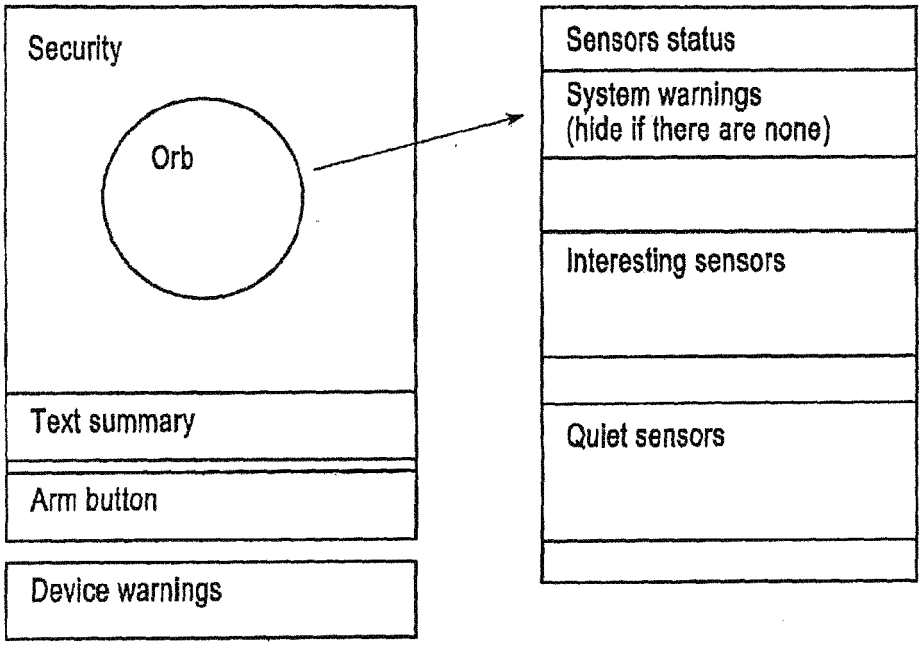

Security
Orb
Text summary
Arm button
Device warnings
Sensors status
System warnings
(hide if there are none)
Interesting sensors
Quiet sensors

FIG. 13

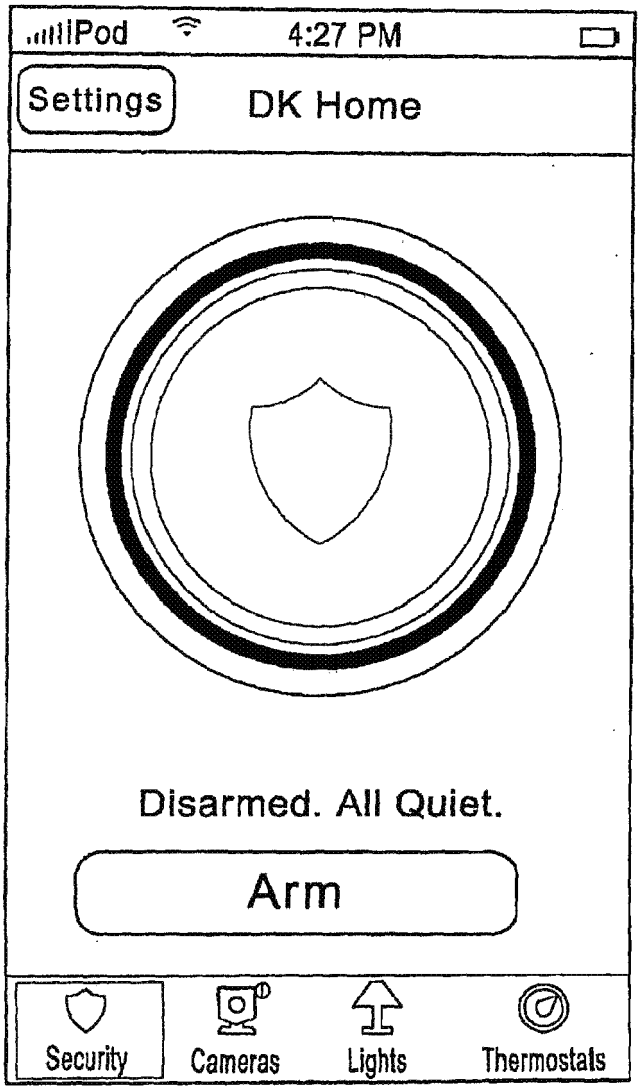

iPod
4:27 PM
Settings
DK Home
Disarmed. All Quiet.
Arm
Security
Cameras
Lights
Thermostats

FIG. 14

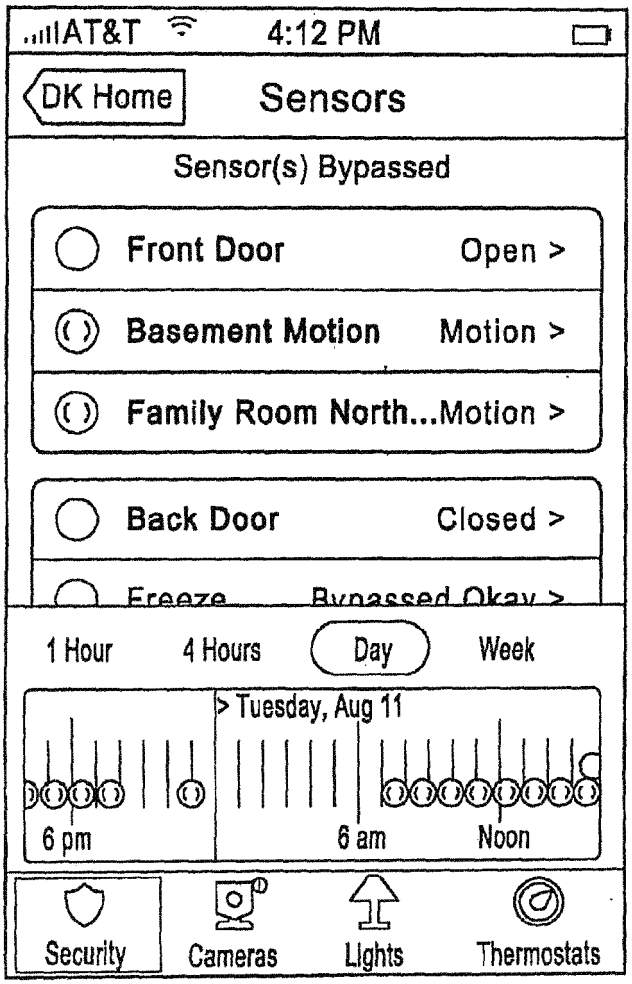

AT&T
4:12 PM
DK Home
Sensors
Sensor(s) Bypassed
Front Door
Open >
Basement Motion
Motion >
Family Room North...
Motion >
Back Door
Closed >
1 Hour
4 Hours
Day
Week
> Tuesday, Aug 11
6 pm
6 am
Noon
Security
Cameras
Lights
Thermostats

FIG. 15

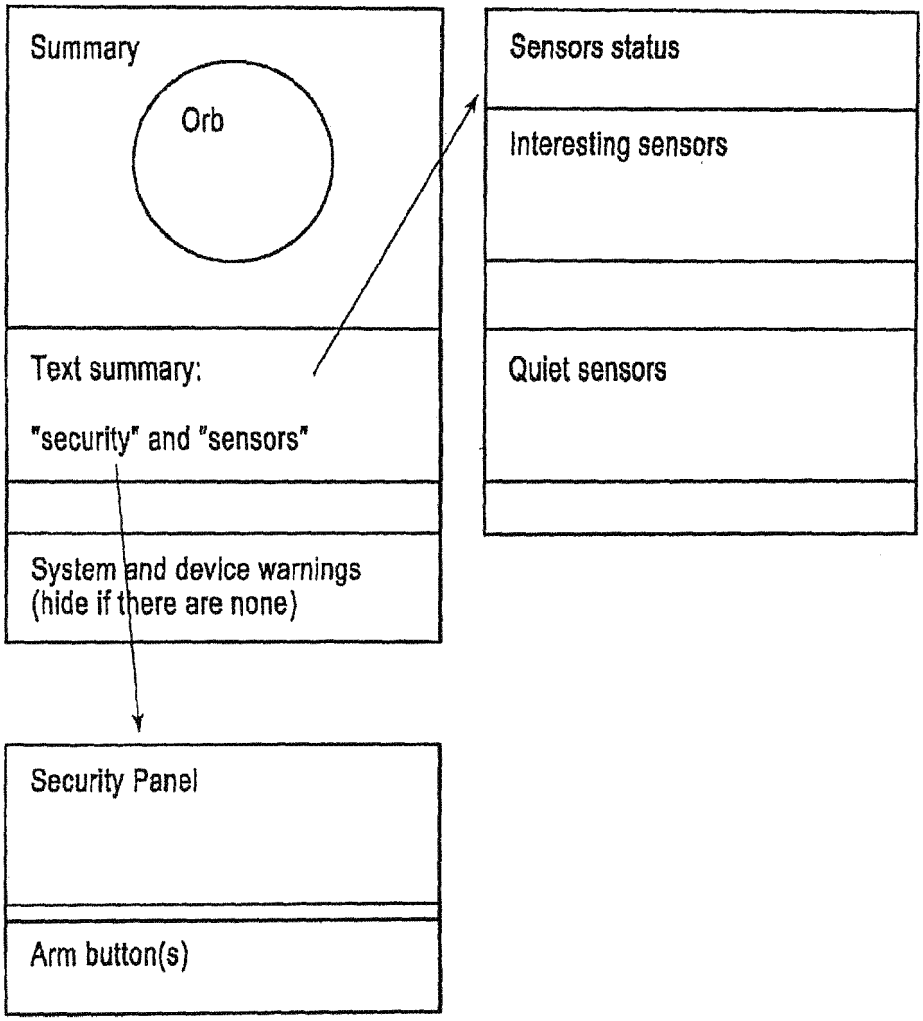

Summary
Orb
Text summary:
"security" and "sensors"
System and device warnings
(hide if there are none)
Sensors status
Interesting sensors
Quiet sensors
Security Panel
Arm button(s)

FIG. 16

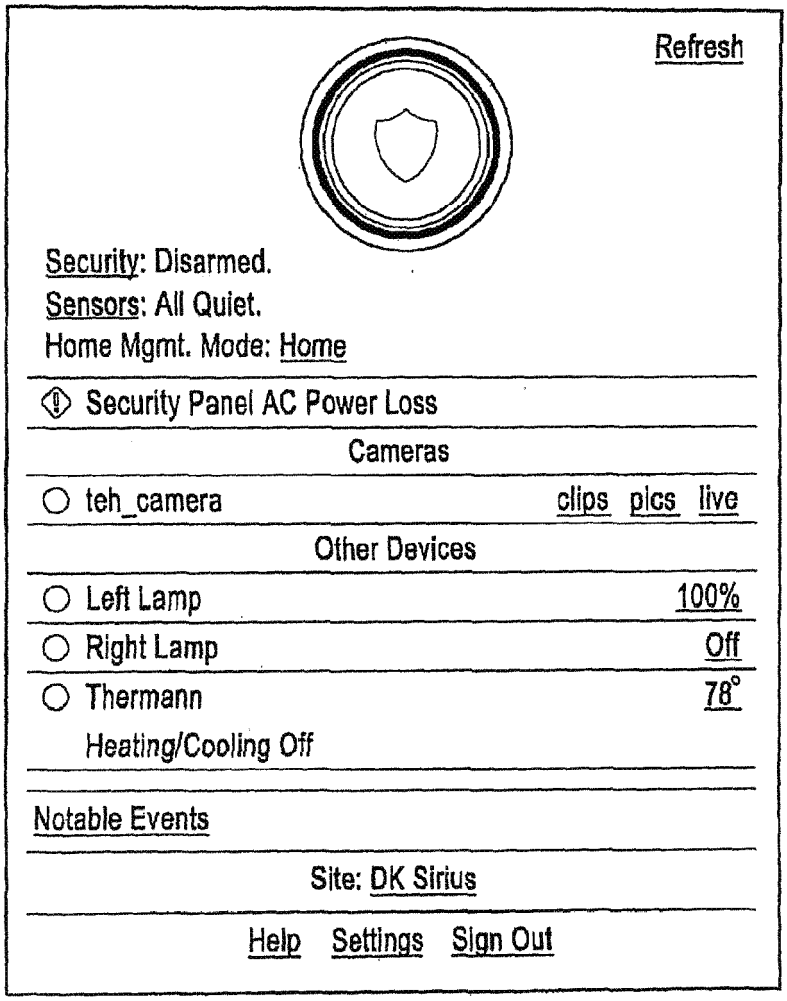

Refresh
Security: Disarmed.
Sensors: All Quiet.
Home Mgmt. Mode: Home
Security Panel AC Power Loss
Cameras
teh_camera
clips pics live
Other Devices
Left Lamp
100%
Right Lamp
Off
Thermann
78°
Heating/Cooling Off
Notable Events
Site: DK Sirius
Help Settings Sign Out

FIG. 17

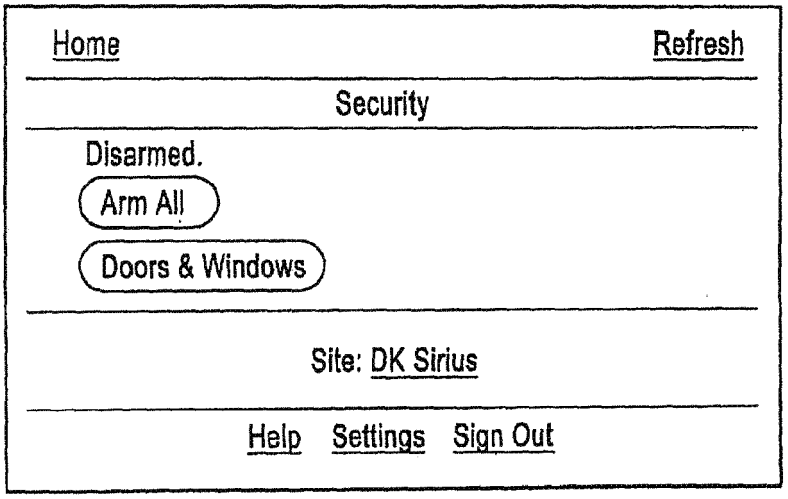

Home
Refresh
Security
Disarmed.
Arm All
Doors & Windows
Site: DK Sirius
Help
Settings
Sign Out

FIG. 18

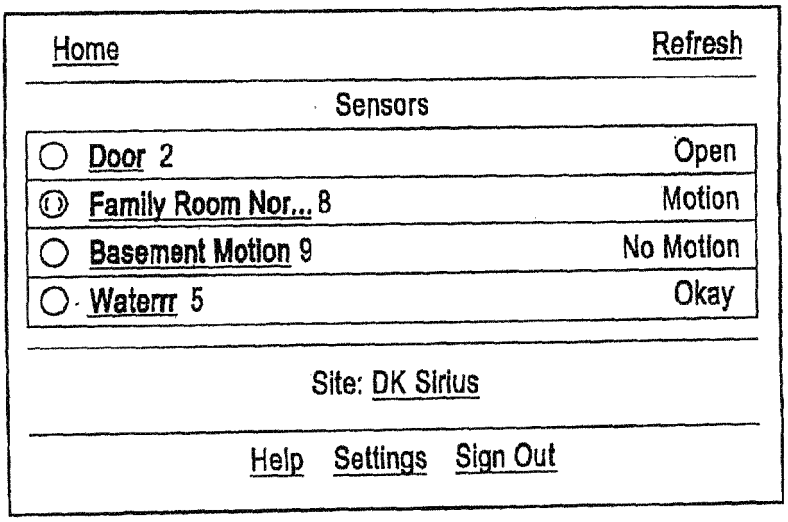

Home
Refresh
Sensors
Door 2
Open
Family Room Nor... 8
Motion
Basement Motion 9
No Motion
Waterrr 5
Okay
Site: DK Sirius
Help
Settings
Sign Out

FIG. 19

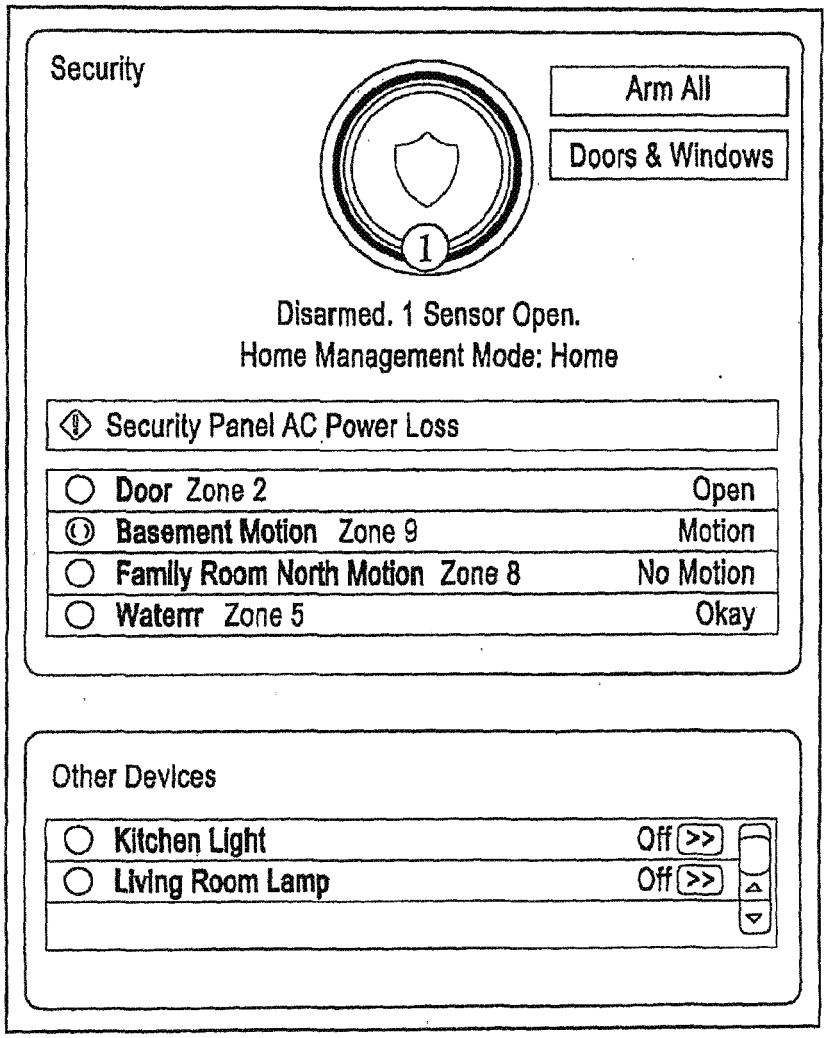

Security
Arm All
Doors & Windows
1
Disarmed. 1 Sensor Open.
Home Management Mode: Home
Security Panel AC Power Loss
Door Zone 2
Open
Basement Motion Zone 9
Motion
Family Room North Motion Zone 8
No Motion
Waterrr Zone 5
Okay
Other Devices
Kitchen Light
Off
Living Room Lamp
Off

FIG. 20

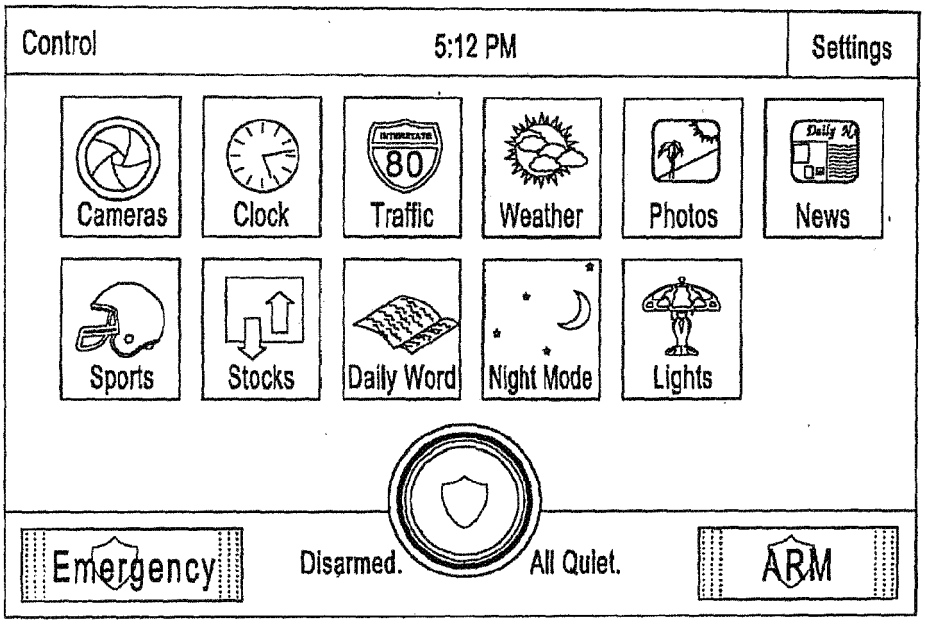

Control
5:12 PM
Settings
Cameras
Clock
Traffic
Weather
Photos
News
Sports
Stocks
Daily Word
Night Mode
Lights
Emergency
Disarmed.
All Quiet.
ARM

FIG. 21

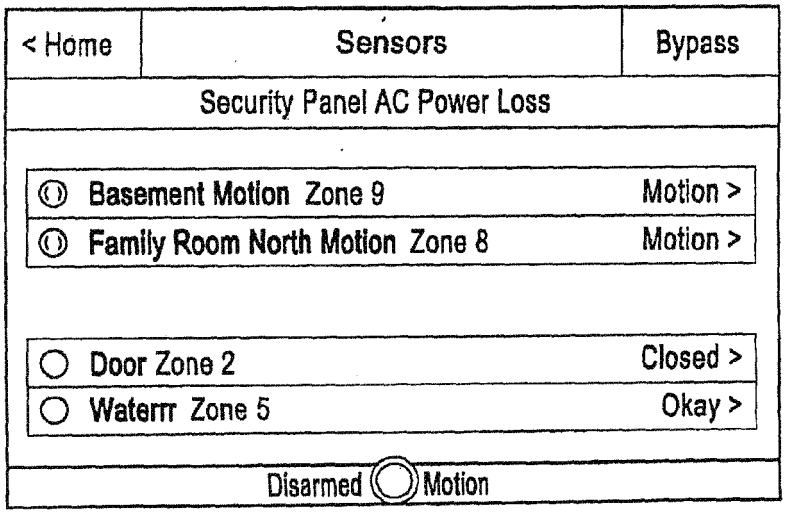

< Home
Sensors
Bypass
Security Panel AC Power Loss
Basement Motion Zone 9
Motion >
Family Room North Motion Zone 8
Motion >
Door Zone 2
Closed >
Waterrr Zone 5
Okay >
Disarmed
Motion

FIG. 22

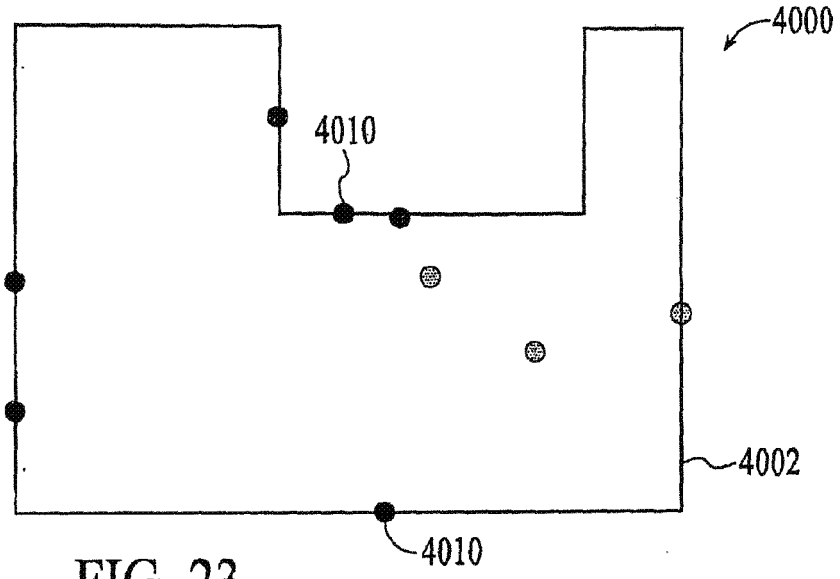


FIG. 23

Sensor State	Icon
Alarmed, tripped, or tampered sensors	
Low Battery	
Offline / AWOL	
Unknown	
Installing	
Open door / window sensor	
Motion sensor active	
Quiet Sensors:	
Okay, Closed, No Motion	

FIG. 24

FIG. 25

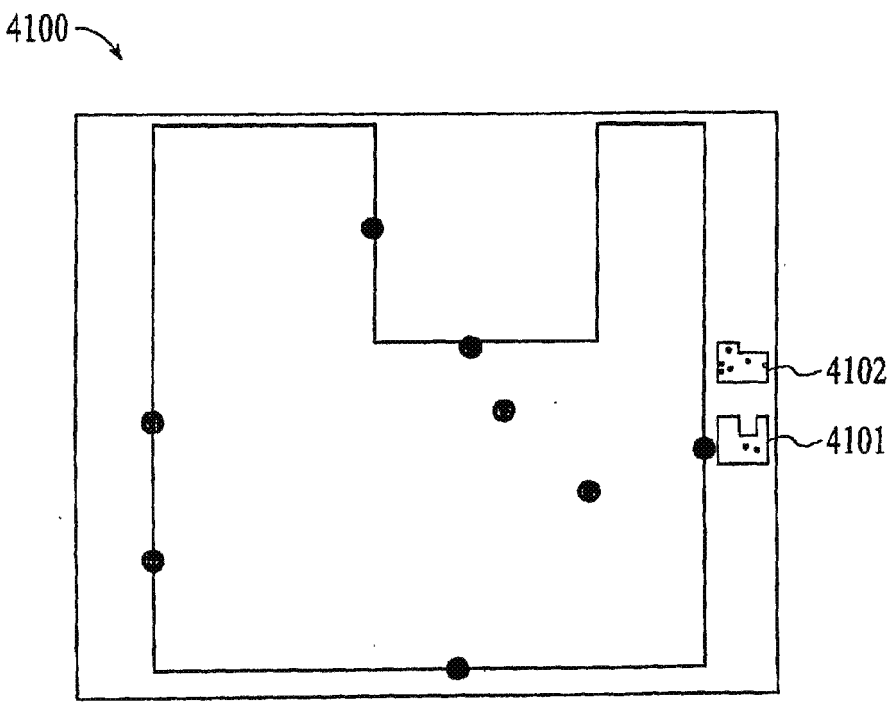


FIG. 26

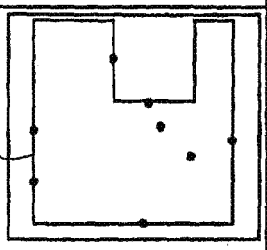
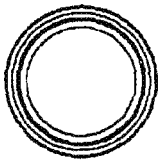
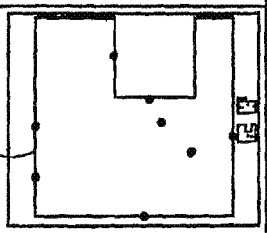
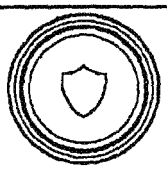
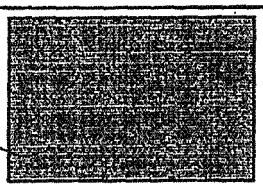
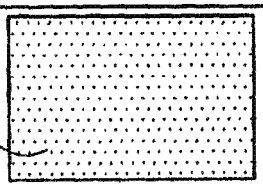
System State	Home View	System Icon
Disarmed or Subdisarmed 4202		
Armed (any type) 4204		
Alarm 4206	 TBD: Red with black diagonal stripes	
Offline (iHub or panel) 4208	 TBD: gray bgnd, all sensors are unknown icon	

FIG. 27

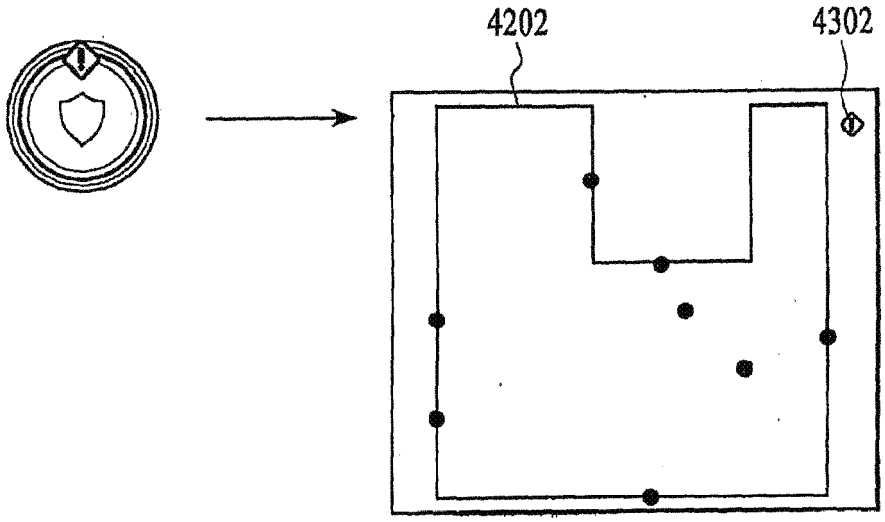


FIG. 28

FIG. 29

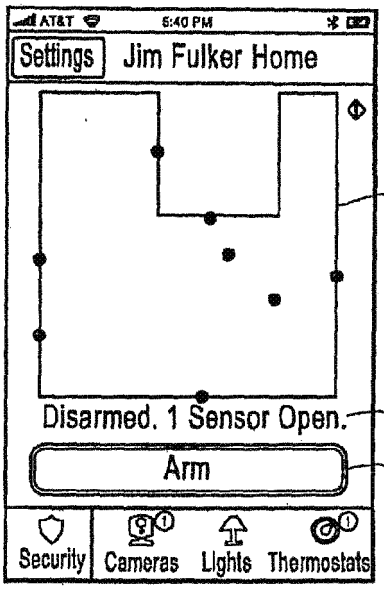
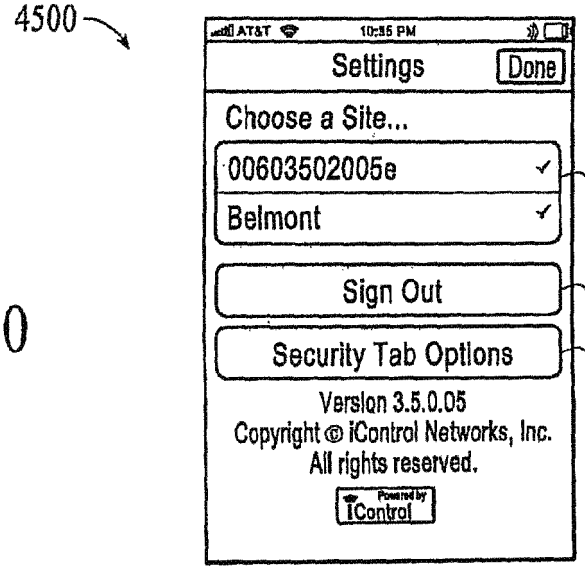

AT&T
5:40 PM
Settings
Jim Fulker Home
4402
Disarmed. 1 Sensor Open.
4404
Arm
4406
Security
Cameras
Lights
Thermostats

FIG. 30


4500
AT&T
10:35 PM
Settings
Done
Choose a Site...
00603502005e
Belmont
4502
Sign Out
4504
Security Tab Options
4506
Version 3.5.0.05
Copyright © iControl Networks, Inc.
All rights reserved.
Powered by iControl

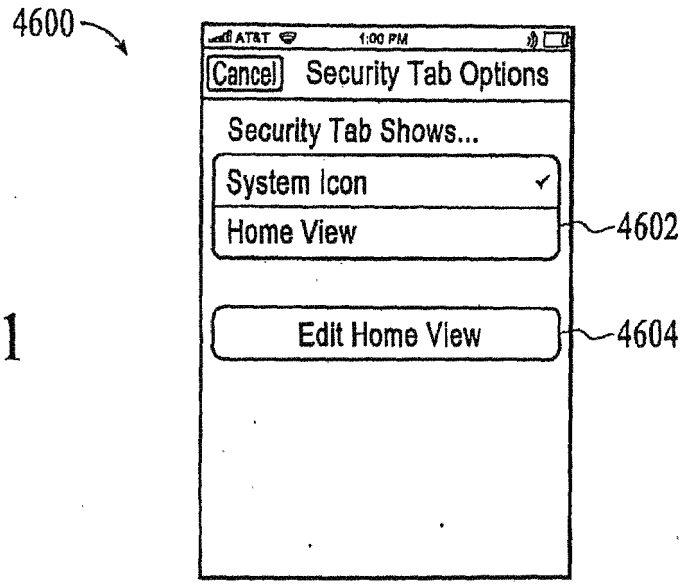

4600
AT&T
1:00 PM
Cancel
Security Tab Options
Security Tab Shows...
System Icon
Home View
4602
Edit Home View
4604

FIG. 31

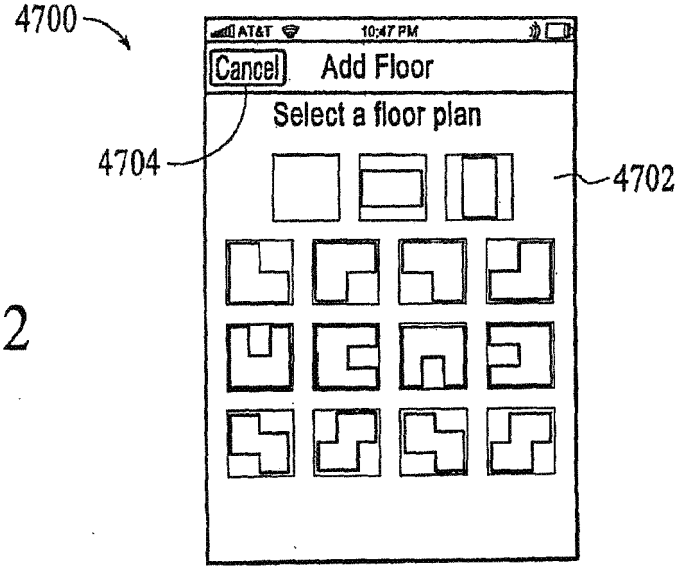

4700
AT&T
10:47 PM
Cancel
Add Floor
Select a floor plan
4704
4702

FIG. 32

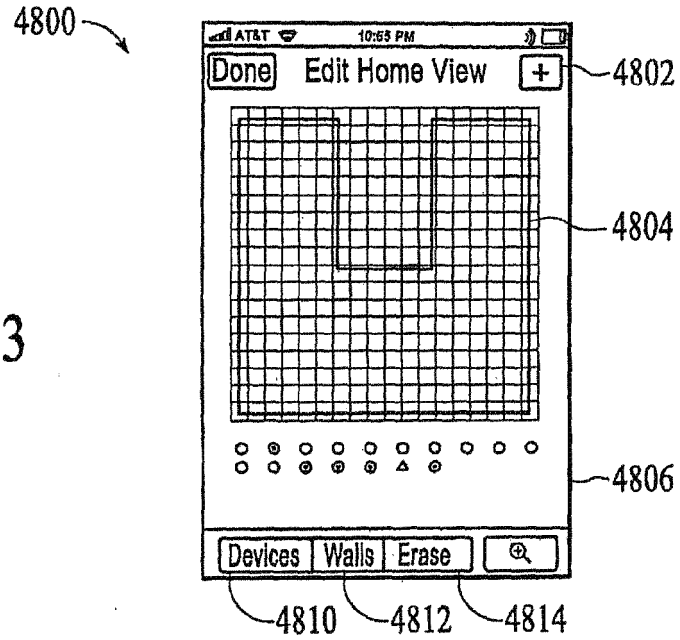

4800
AT&T
10:55 PM
Done
Edit Home View
+
4802
4804
4806
Devices
Walls
Erase
4810
4812
4814

FIG. 33

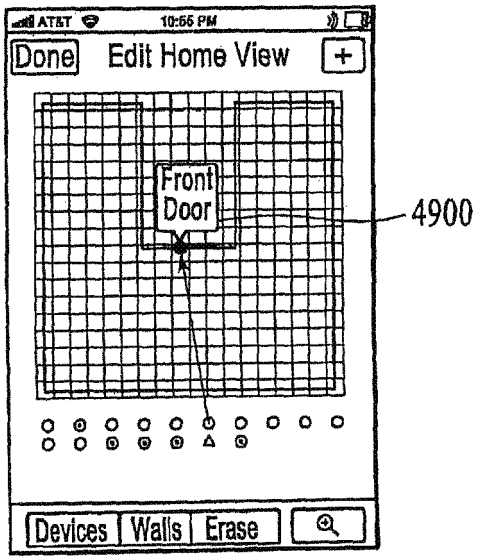

AT&T
10:56 PM
Done
Edit Home View
+
Front Door
4900
Devices
Walls
Erase

FIG. 34

FIG. 35

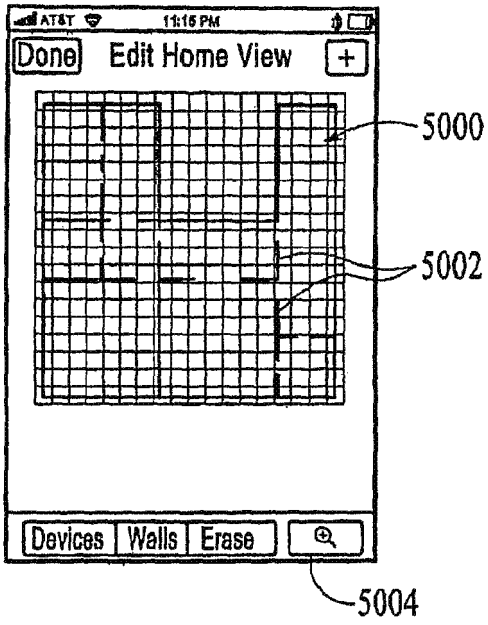
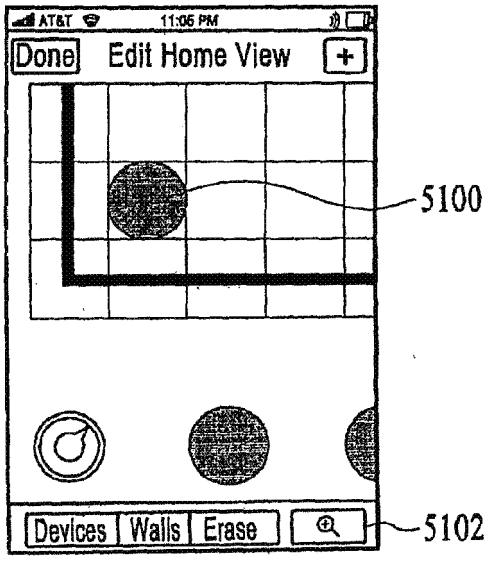

AT&T
11:16 PM
Done
Edit Home View
+
5000
5002
Devices
Walls
Erase
5004

FIG. 36


AT&T
11:06 PM
Done
Edit Home View
+
5100
Devices
Walls
Erase
5102

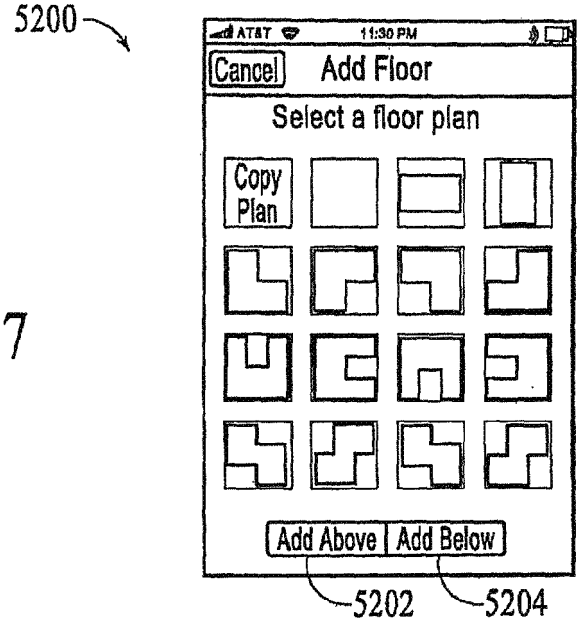

5200
AT&T
11:30 PM
Cancel
Add Floor
Select a floor plan
Copy Plan
Add Above
Add Below
5202
5204

FIG. 37

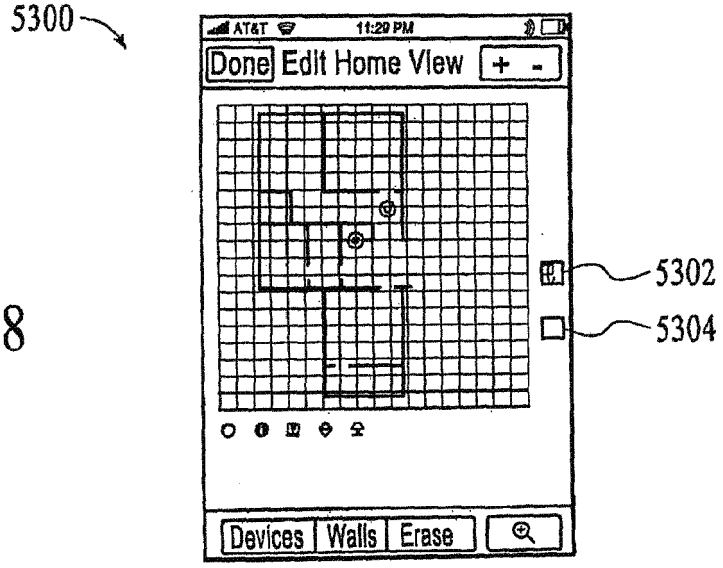

5300
AT&T
11:29 PM
Done
Edit Home View
+
-
5302
5304
Devices
Walls
Erase

FIG. 38

FIG. 39

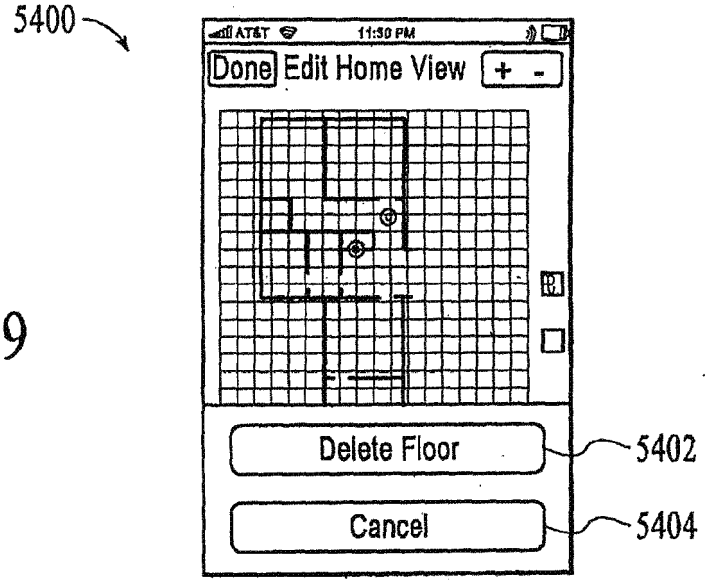
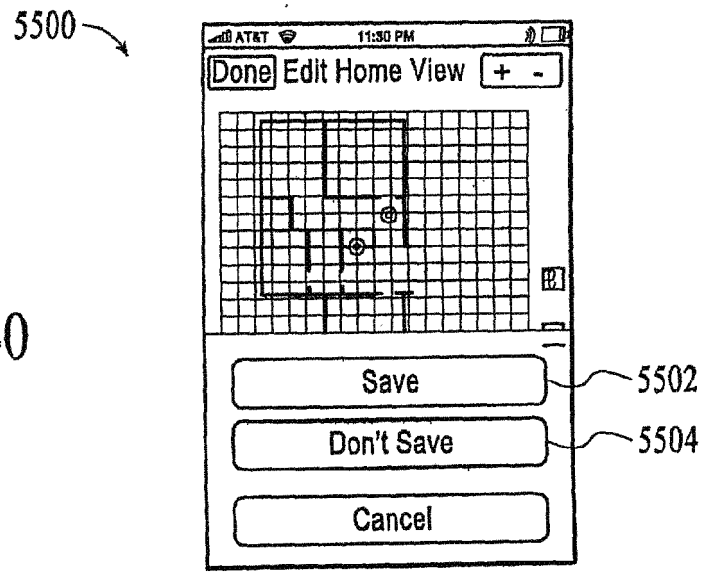

5400
AT&T
11:30 PM
Done
Edit Home View
+
-
Delete Floor
5402
Cancel
5404

FIG. 40


5500
AT&T
11:30 PM
Done
Edit Home View
+
-
Save
5502
Don't Save
5504
Cancel

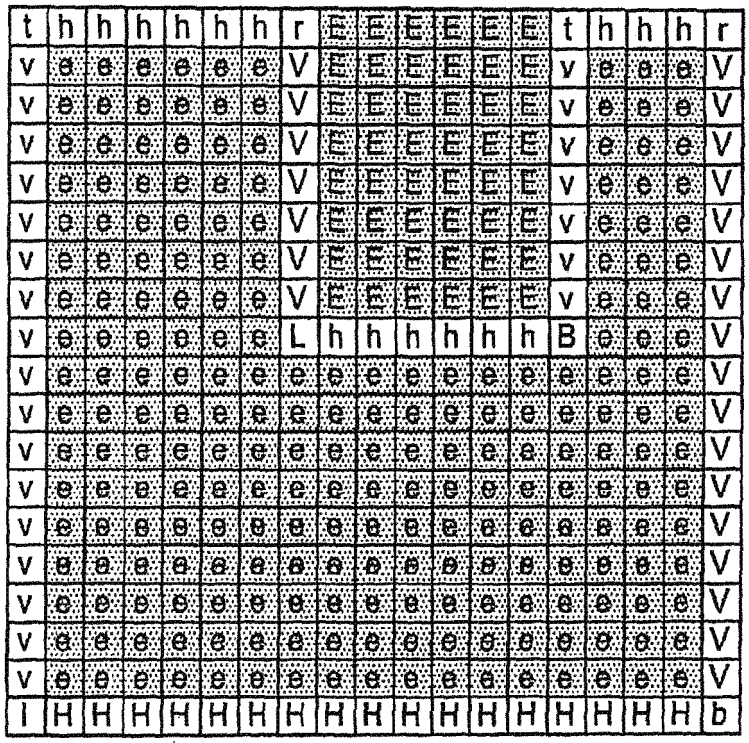


FIG. 41

tile number (from 0)	device type	device identifier
0	zone	3
238	zone	1
341	camera	Courtyard Cam
552	thermo	Upstairs Thermostat

FIG. 42

FIG. 43

homeViewLayouts="
thhhhhhrEEEEEEEthhhr
veeeeeeVEEEEEEEveeeV
veeeeeeVEEEEEEEveeeV
veeeeeeVEEEEEEEveeeV
veeeeeeVEEEEEEEveeeV
veeeeeeVEEEEEEEveeeV
veeeeeeVEEEEEEEveeeV
veeeeeeVEEEEEEEveeeV
veeeeeeLhhhhhhBeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
veeeeeeeeeeeeeeeeeV
1HHHHHHHHHHHHHHHHHb"

Tile Shape	Simple / filled
empty	 e
horizontal wall	 h
vertical wall	 v
top left corner	 t
top right corner	 r
bottom left corner	 l
bottom right corner	 b
T-shape down	 p
T-shape right	 f
T-shape up	 n
T-shape left	 j
4 corner shape	 x

FIG. 44

Tile Shape	Simple / filled	Fill bottom / right	Fill top / left	Empty exterior
empty	e			E
horizontal wall	h	i	I	H
vertical wall	v	w	W	V
top left corner	t	u	U	T
top right corner	r	s	S	R
bottom left corner	l	m	M	L
bottom right corner	b	c	C	B

Tile Shape	Fill all	Fill 1	Fill 2	Fill 3	Fill 4	Fill 5	Fill 6	Ext
T-shape down	p	P	q	Q	=	0	1	a
T-shape right	f	F	g	G	2	3	4	A
T-shape up	n	N	o	O	5	6	7	d
T-shape left	j	J	k	K	8	9	$	D

Tile Shape	Fill all	Fill 1	Fill 2	Fill 3	Fill 4	Exterior
4 corner shape	x + [	X ^]	y _ (underscore) {	Y - (dash) }	z , (comma)	Z ' (single quote)

FIG. 45

Let's take a simple room for example:

In this example, there are two perimeter versions of the top-right corner tile "f". One filled on the bottom right (tile "u"):

and one filled on the top left (tile "U"):

FIG. 46

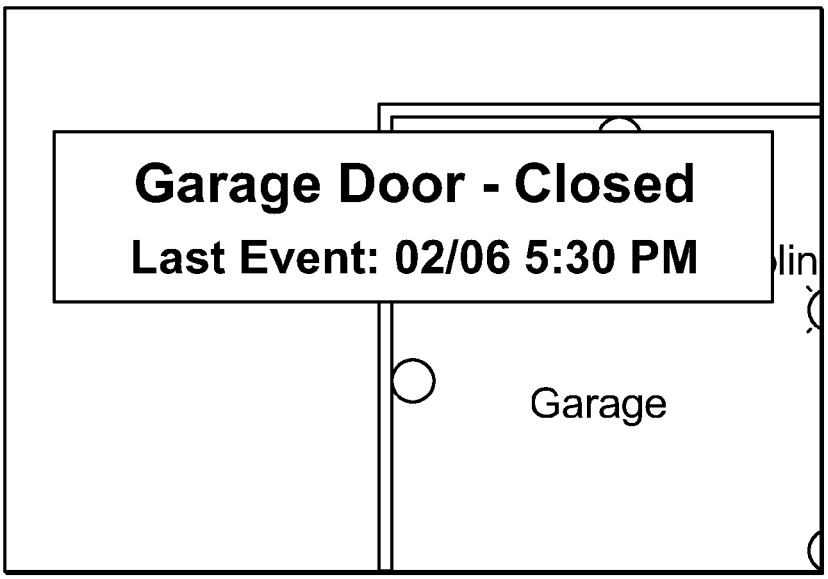


FIG. 47

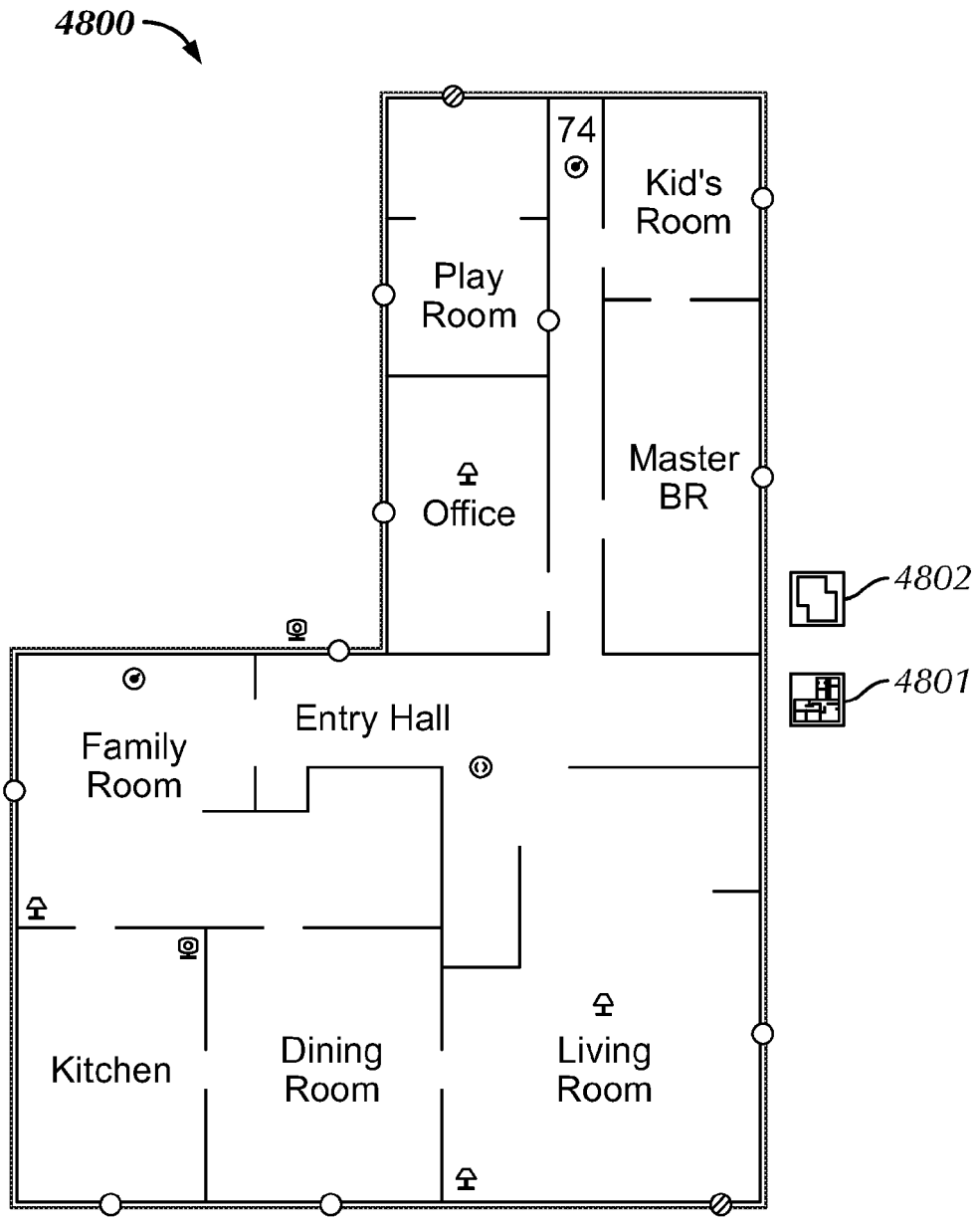

4800
74
Kid's Room
Play Room
Office
Master BR
4802
4801
Entry Hall
Family Room
Kitchen
Dining Room
Living Room

FIG. 48

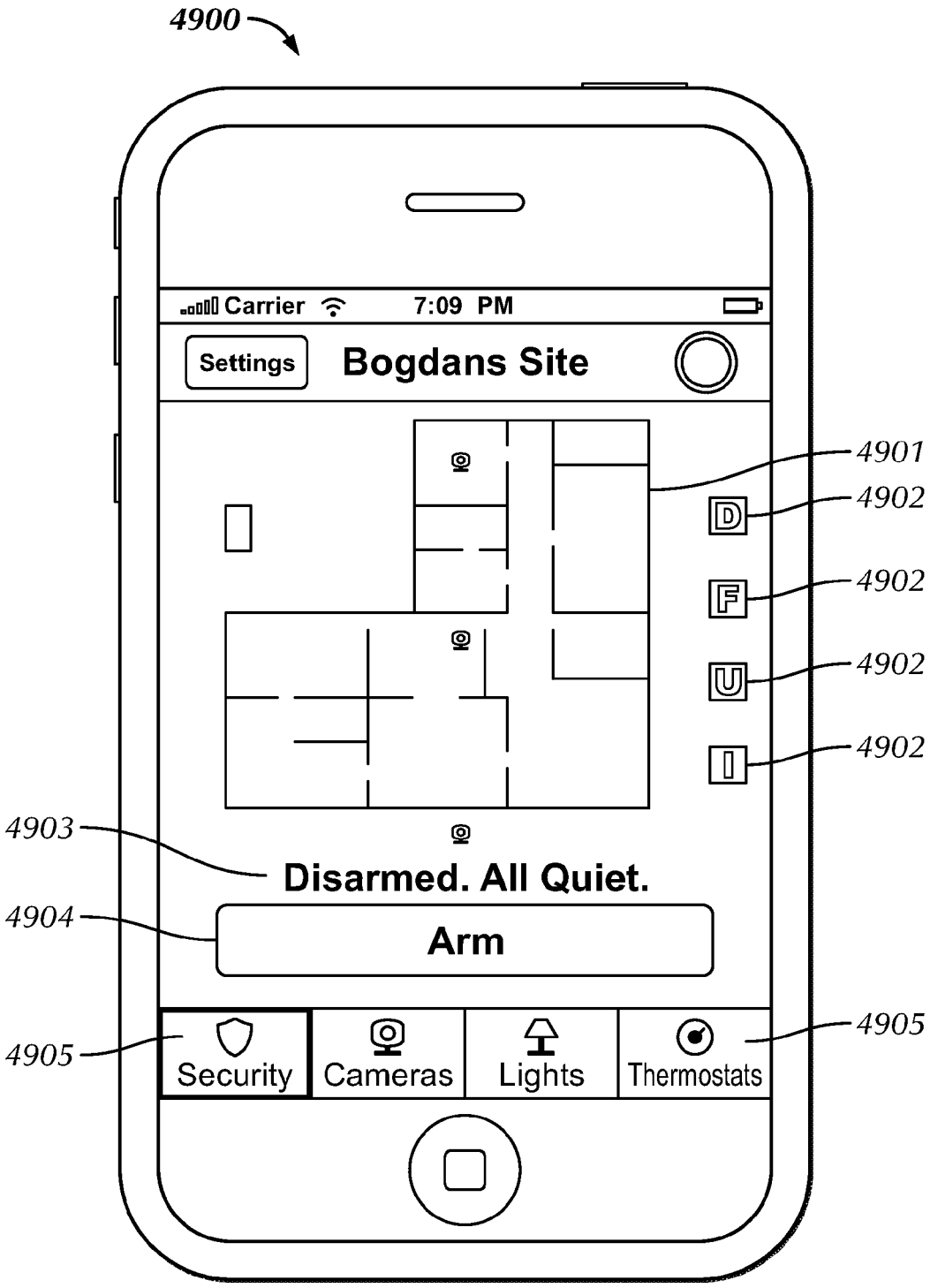

4900
Carrier
7:09 PM
Settings
Bogdans Site
4901
4902
D
4902
F
4902
U
4902
I
4903
Disarmed. All Quiet.
4904
Arm
4905
Security
Cameras
Lights
Thermostats
4905

FIG. 49

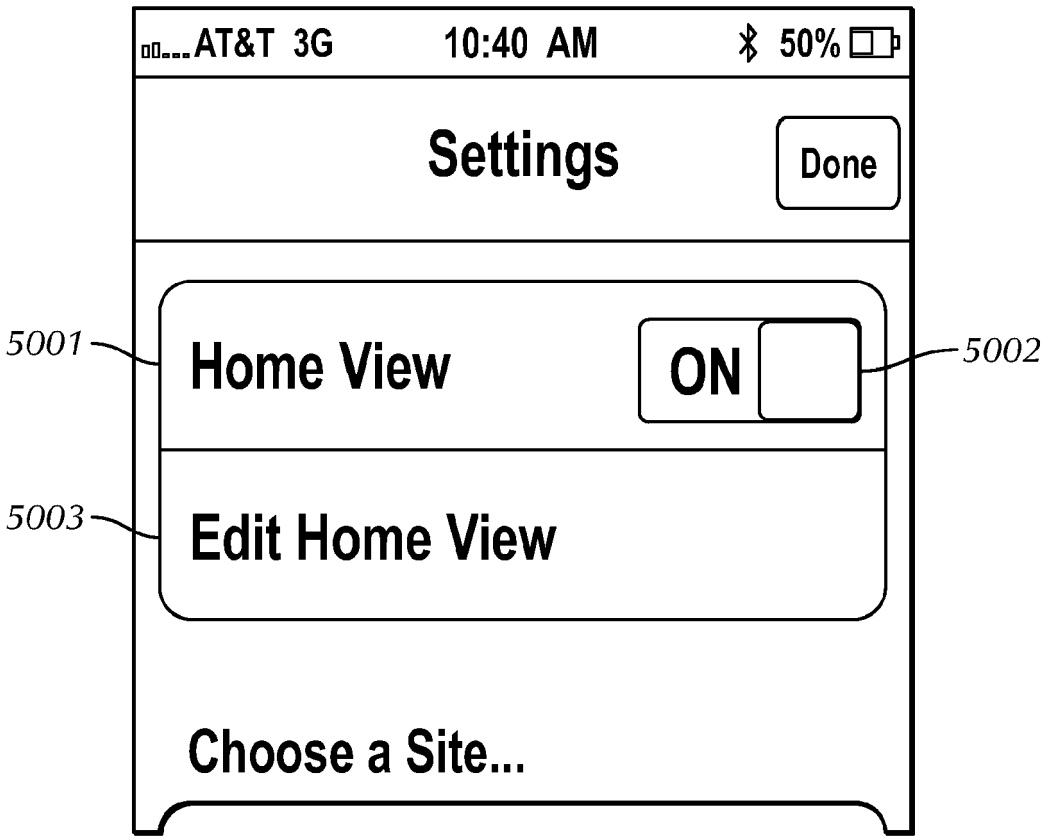

AT&T 3G
10:40 AM
50%
Settings
Done
5001
Home View
ON
5002
5003
Edit Home View
Choose a Site...

FIG. 50

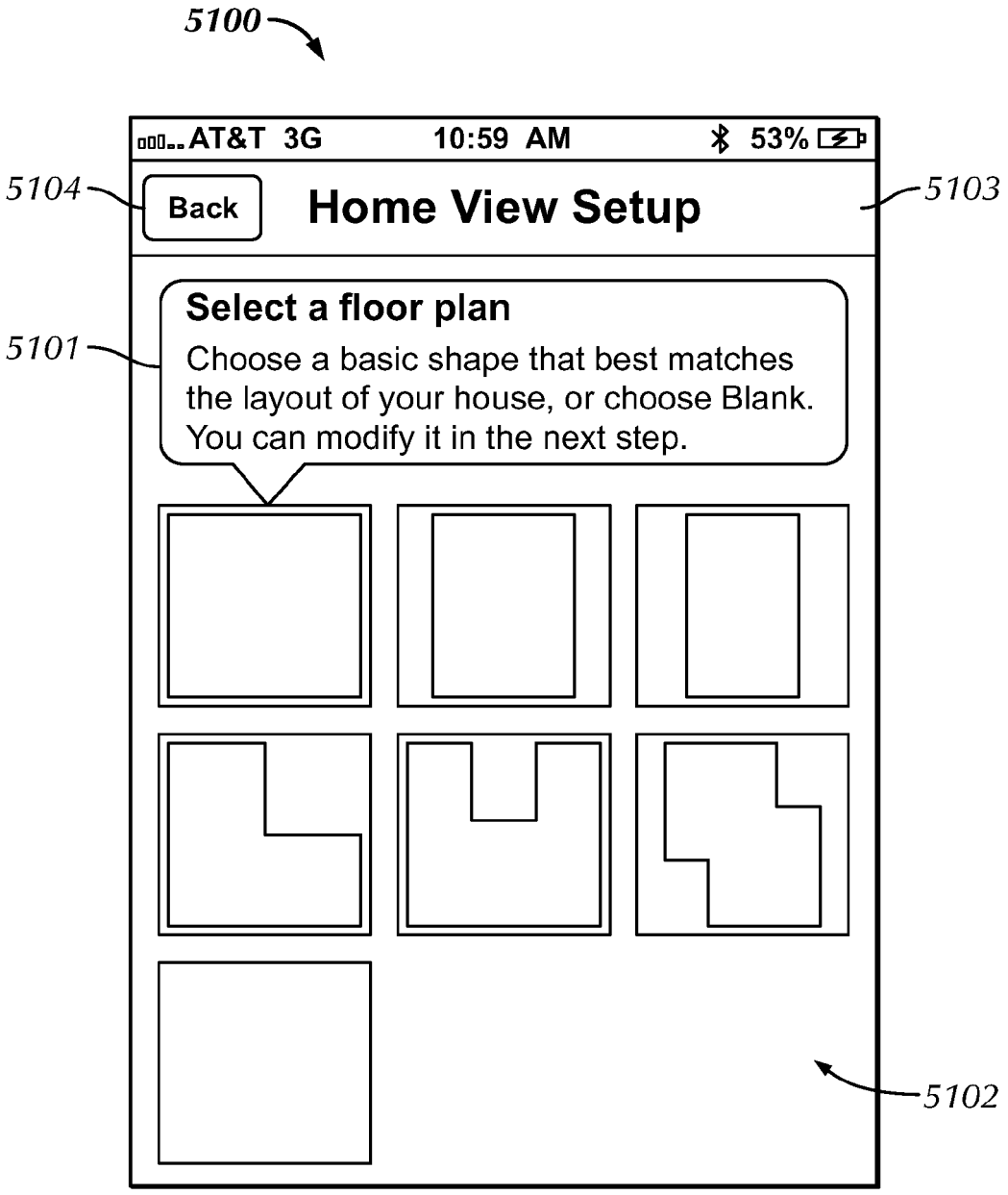

5100
AT&T 3G
10:59 AM
53%
5104
Back
Home View Setup
5103
5101
Select a floor plan
Choose a basic shape that best matches the layout of your house, or choose Blank. You can modify it in the next step.
5102

FIG. 51

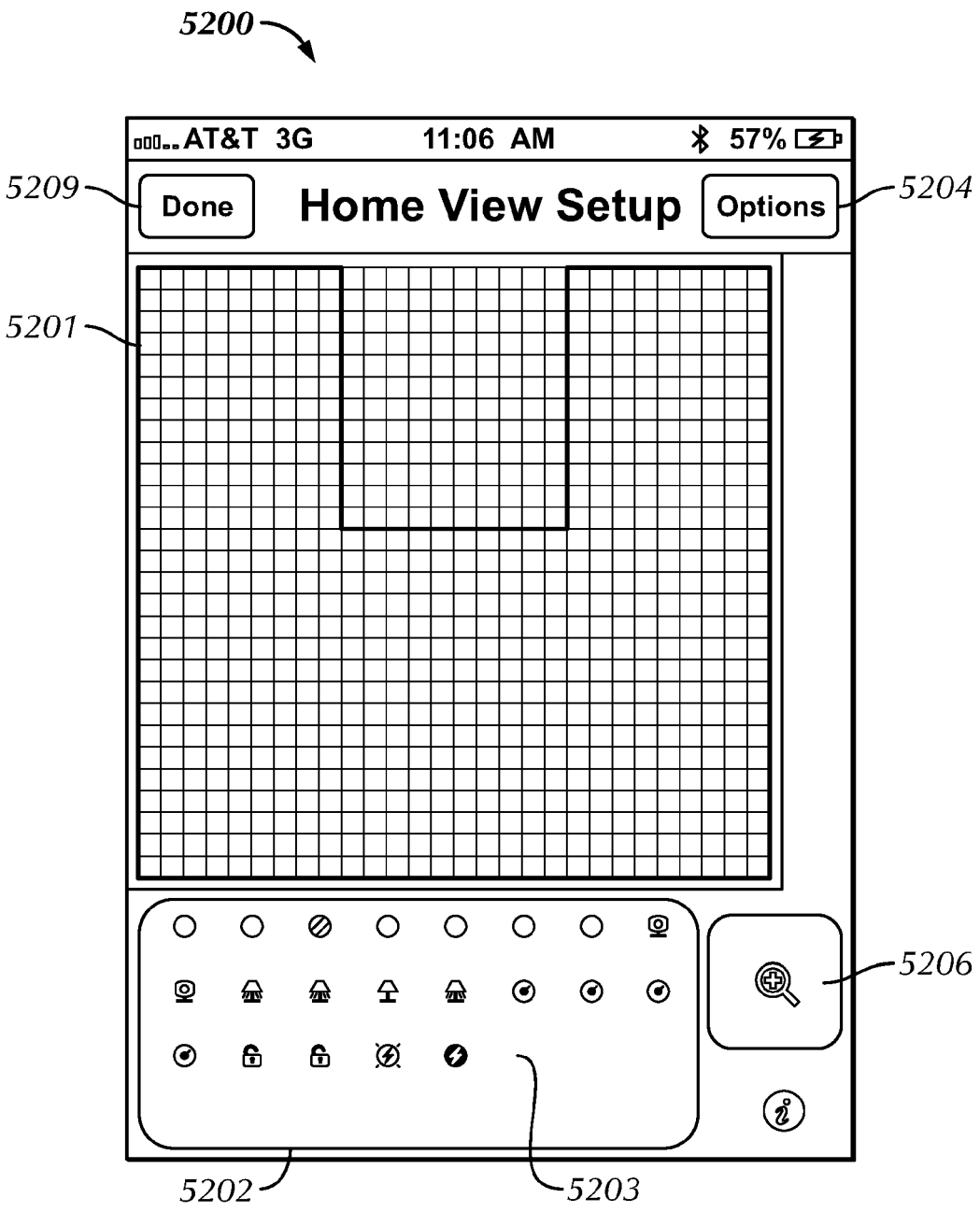

5200
AT&T 3G
11:06 AM
57%
5209
Done
Home View Setup
Options
5204
5201
5206
5202
5203

FIG. 52

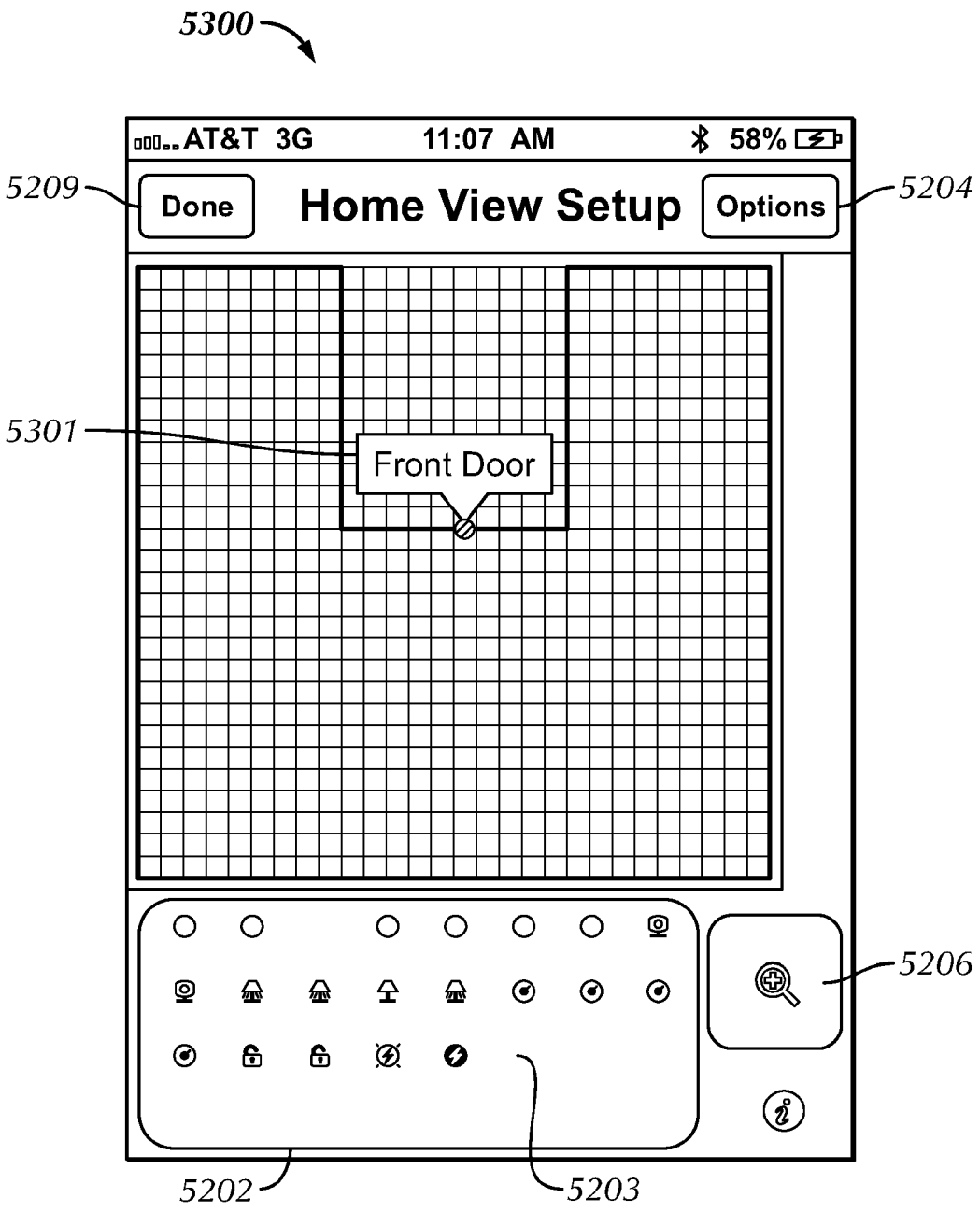

5300
AT&T 3G
11:07 AM
58%
5209
Done
Home View Setup
Options
5204
5301
Front Door
5206
5202
5203

FIG. 53

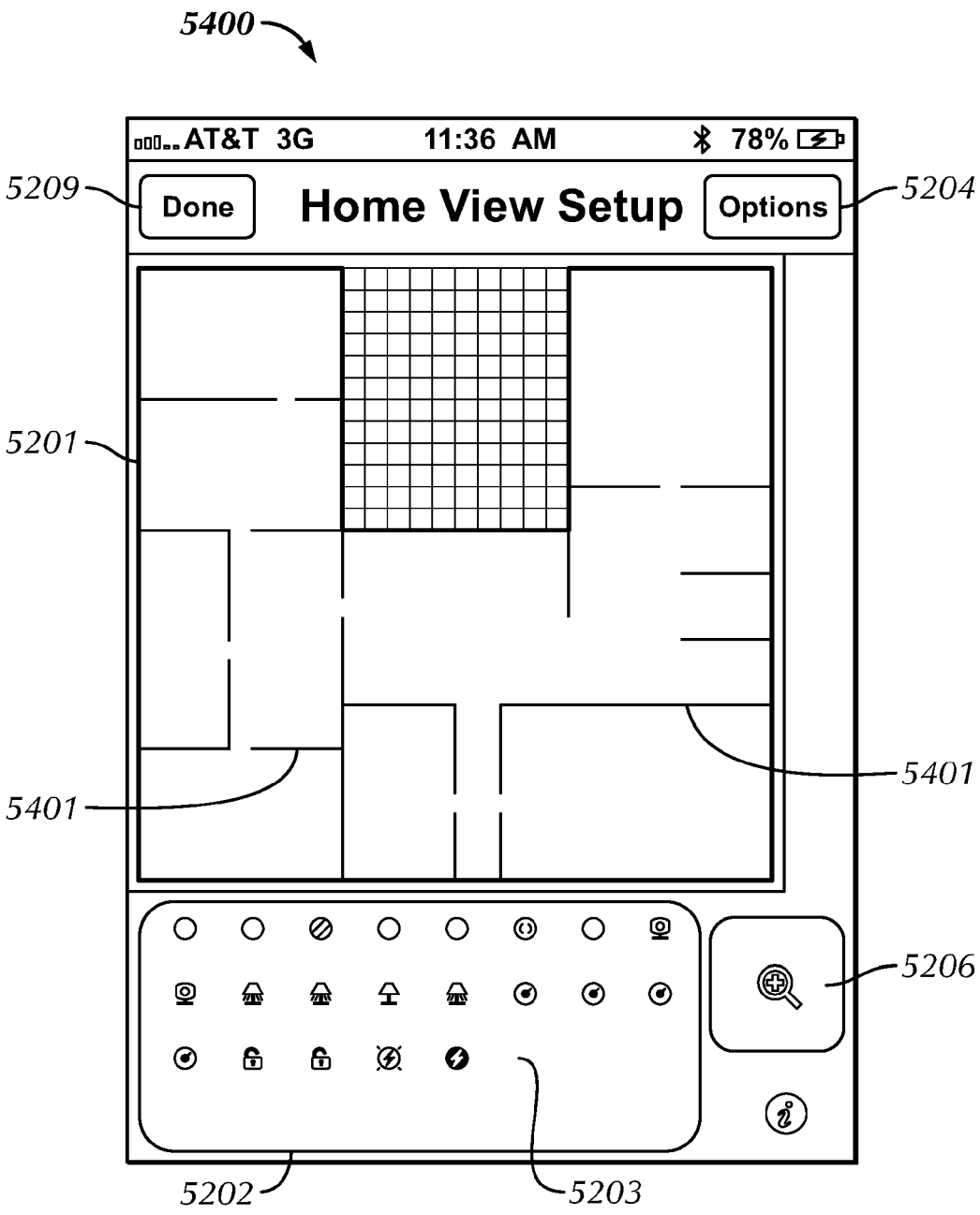

5400
AT&T 3G
11:36 AM
78%
Done
Home View Setup
Options
5209
5204
5201
5401
5401
5206
5202
5203

FIG. 54

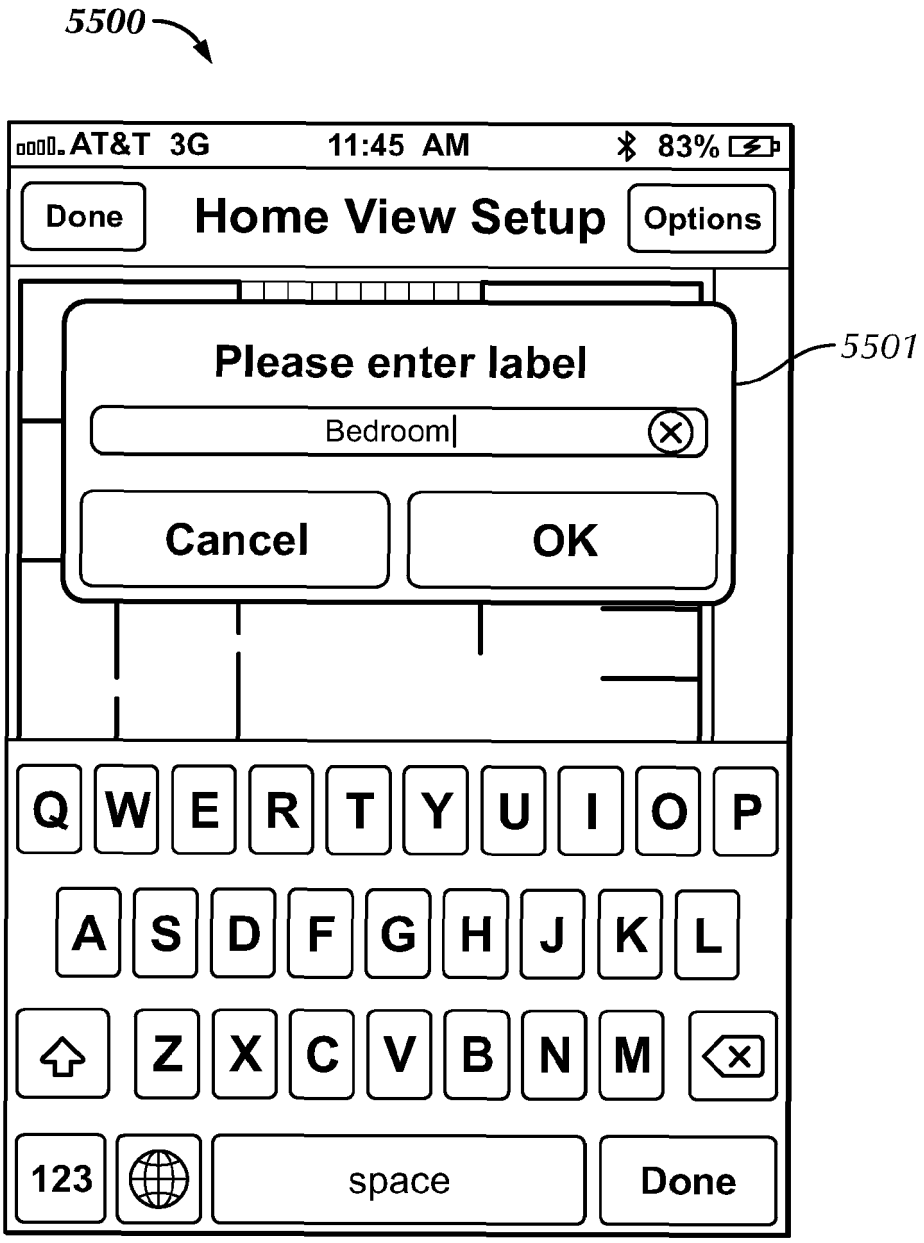

5500
AT&T 3G
11:45 AM
83%
Done
Home View Setup
Options
Please enter label
5501
Bedroom
Cancel
OK
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
Done

FIG. 55

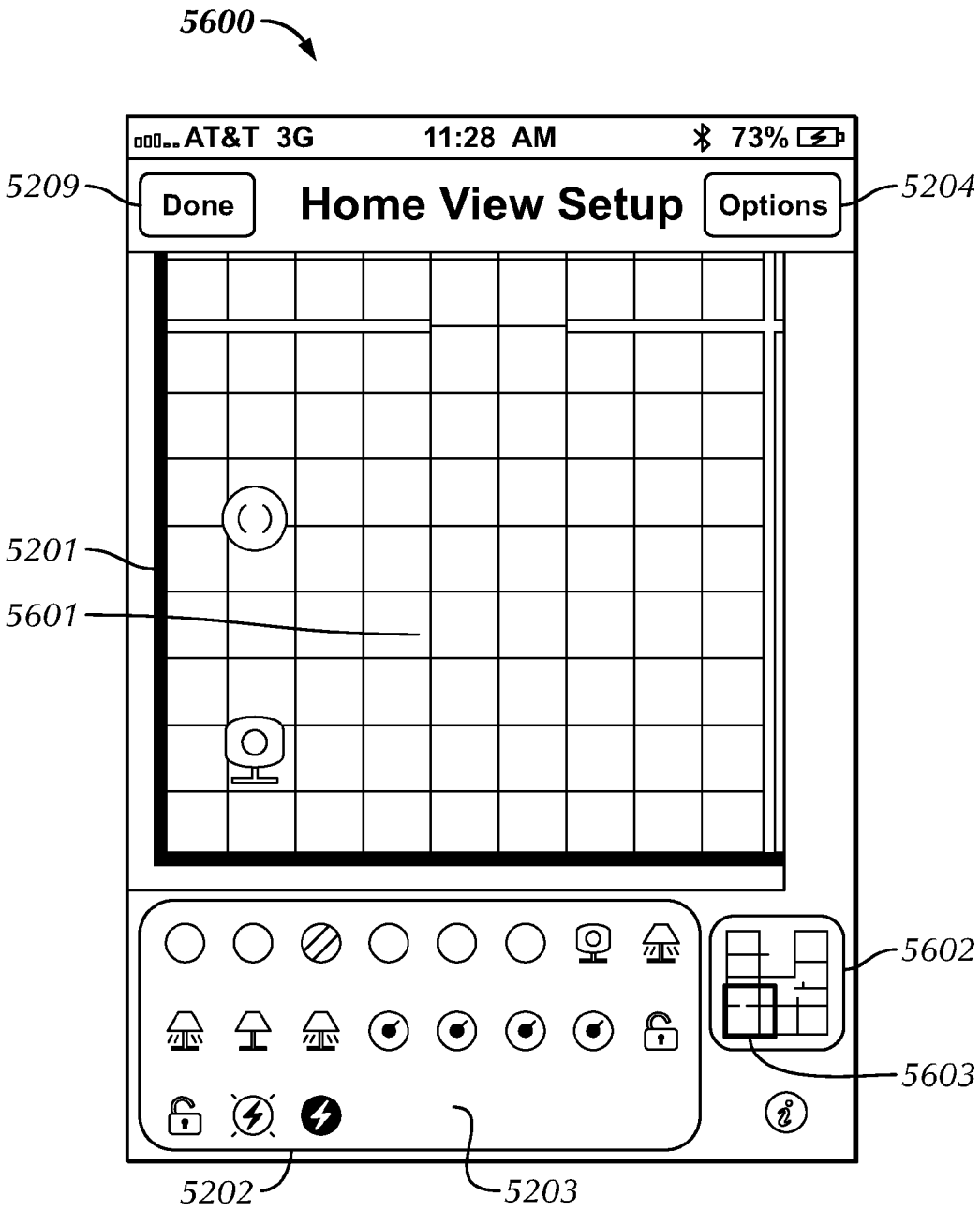

5600
AT&T 3G
11:28 AM
73%
Done
Home View Setup
Options
5209
5204
5201
5601
5602
5603
5202
5203

FIG. 56

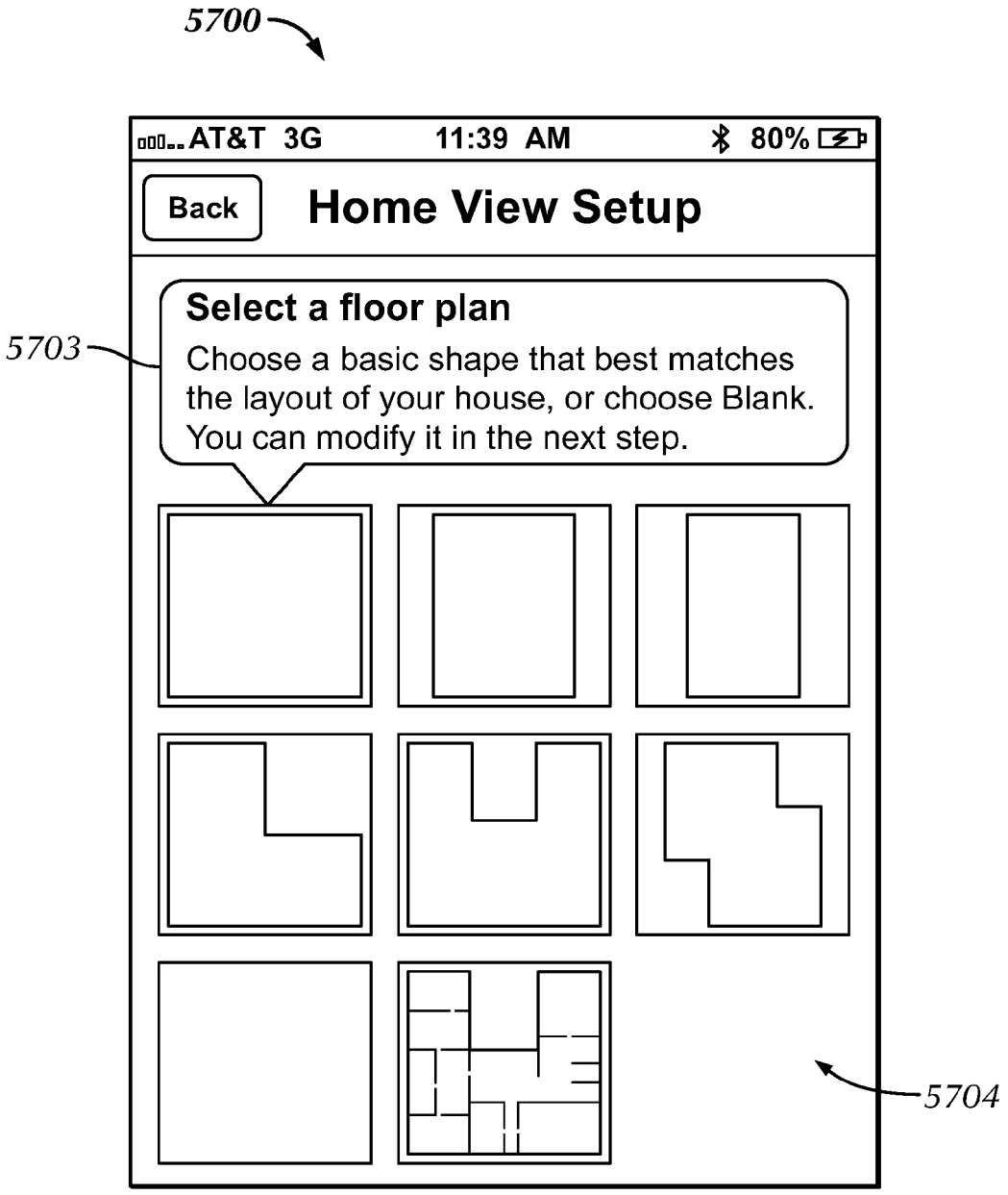

5700
AT&T 3G
11:39 AM
80%
Back
Home View Setup
5703
Select a floor plan
Choose a basic shape that best matches the layout of your house, or choose Blank. You can modify it in the next step.
5704

FIG. 57

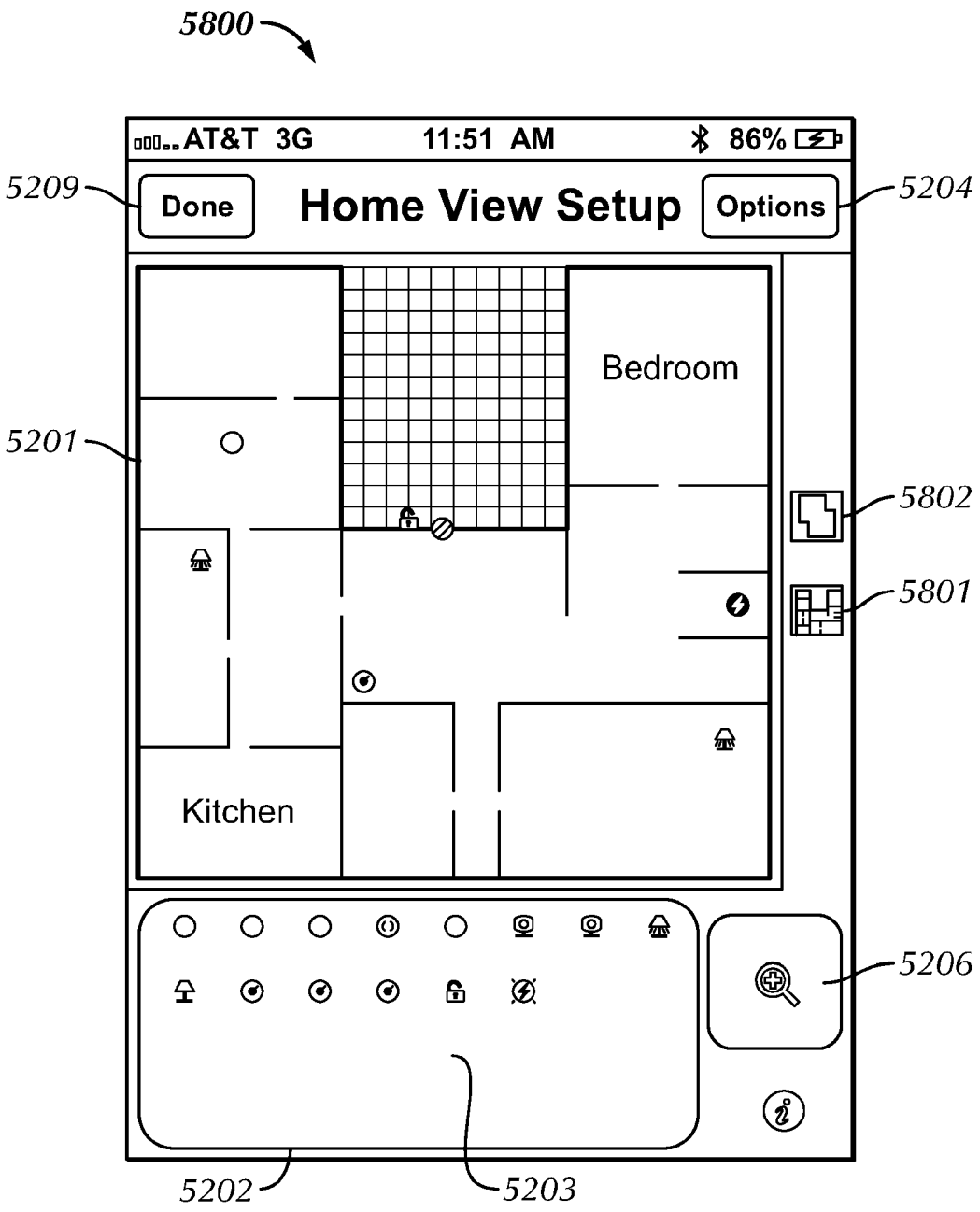

5800
AT&T 3G
11:51 AM
86%
5209
Done
Home View Setup
Options
5204
Bedroom
5201
5802
5801
Kitchen
5206
5202
5203

FIG. 58

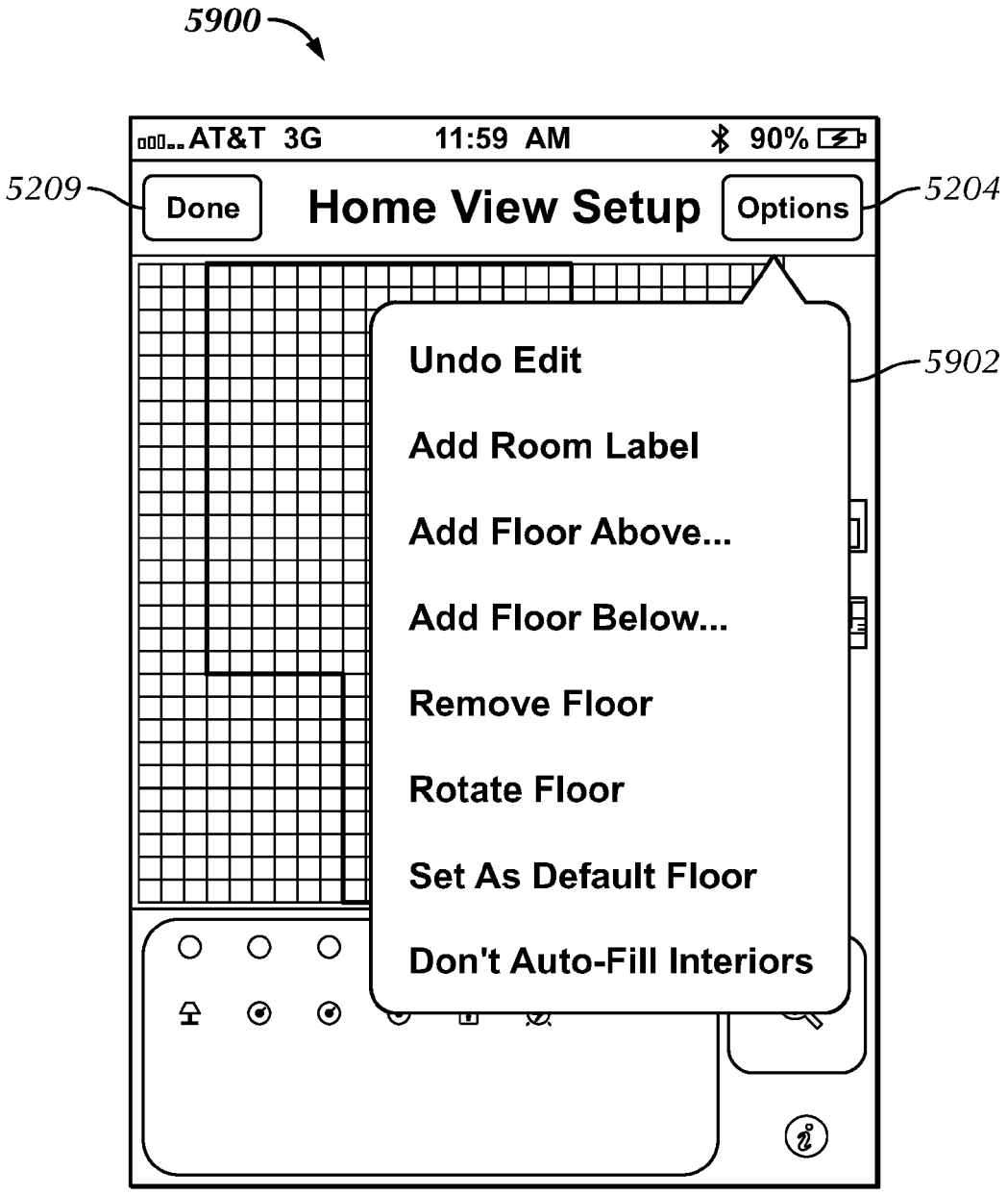

5900
AT&T 3G
11:59 AM
90%
5209
Done
Home View Setup
Options
5204
5902
Undo Edit
Add Room Label
Add Floor Above...
Add Floor Below...
Remove Floor
Rotate Floor
Set As Default Floor
Don't Auto-Fill Interiors

FIG. 59

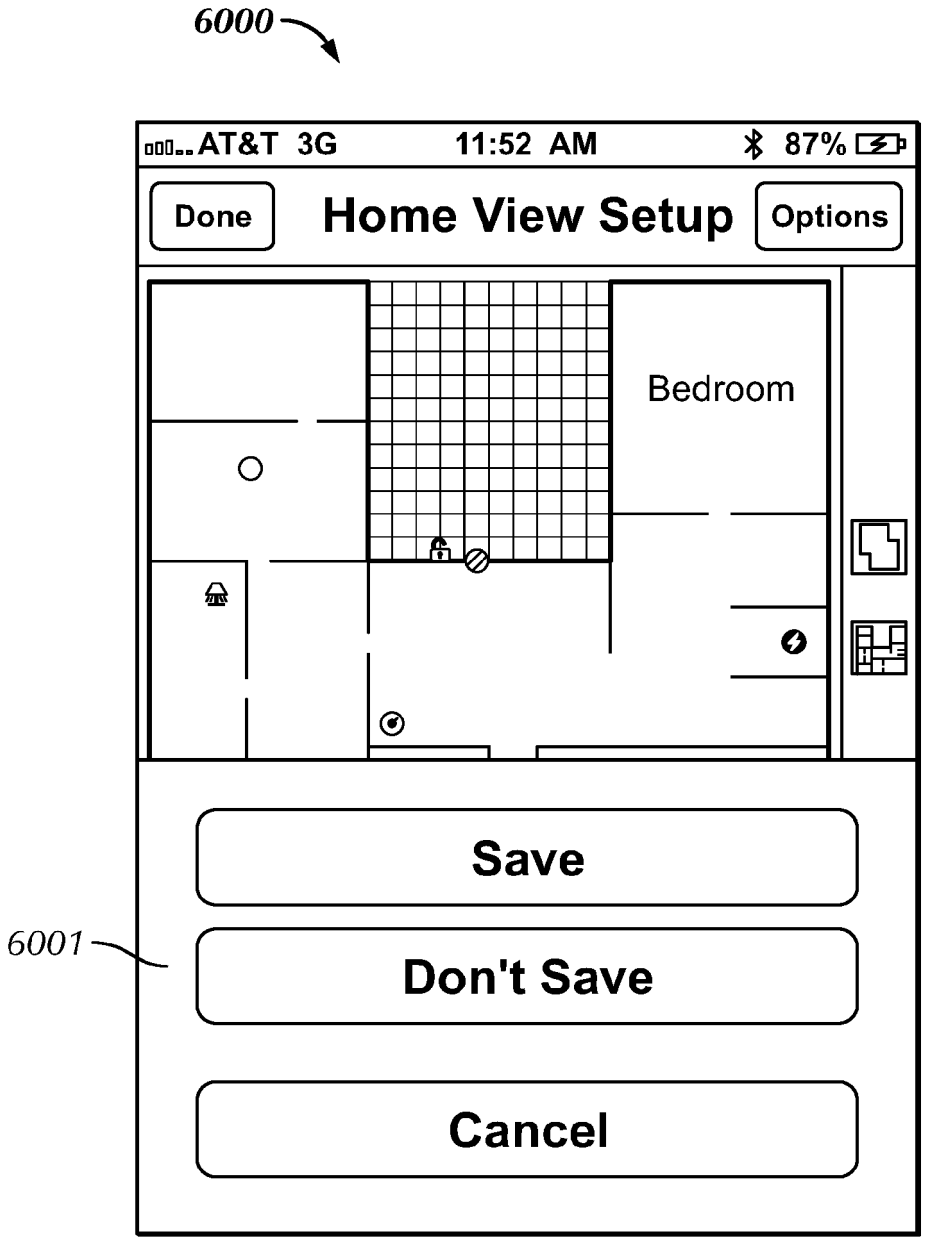

6000
AT&T 3G
11:52 AM
87%
Done
Home View Setup
Options
Bedroom
Save
6001
Don't Save
Cancel

FIG. 60

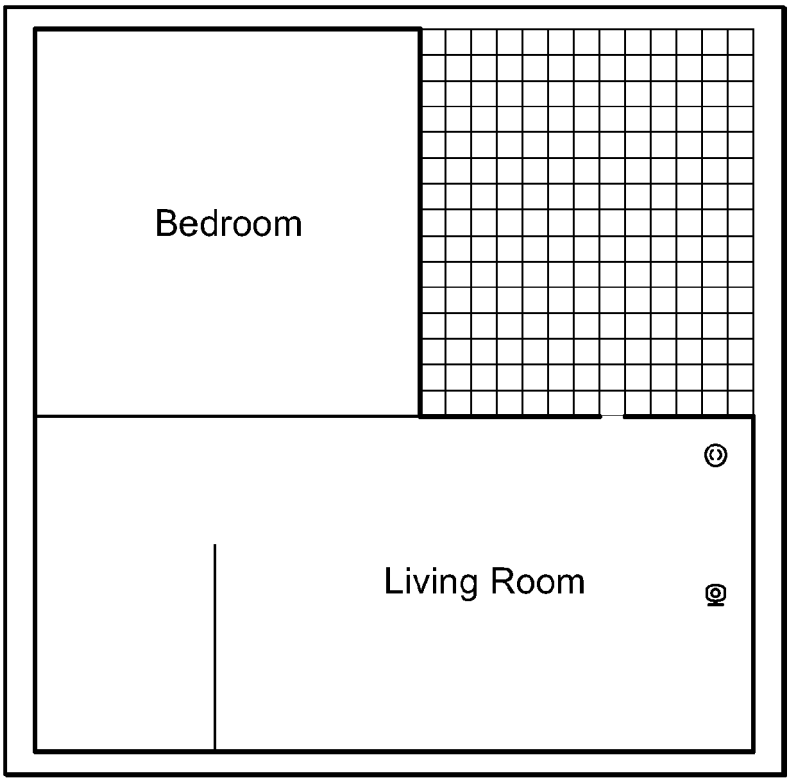


FIG. 61

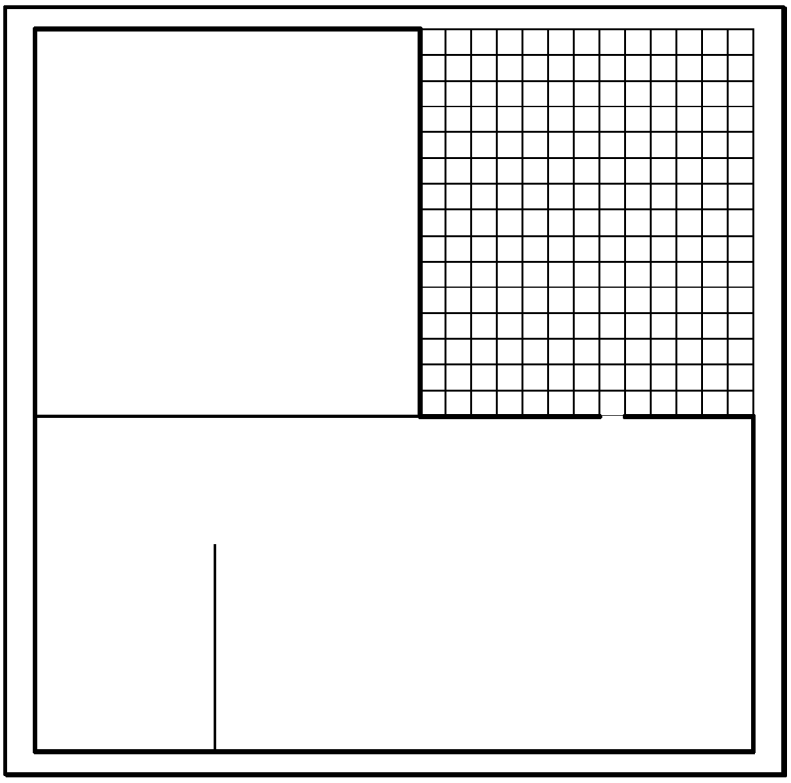


FIG. 62

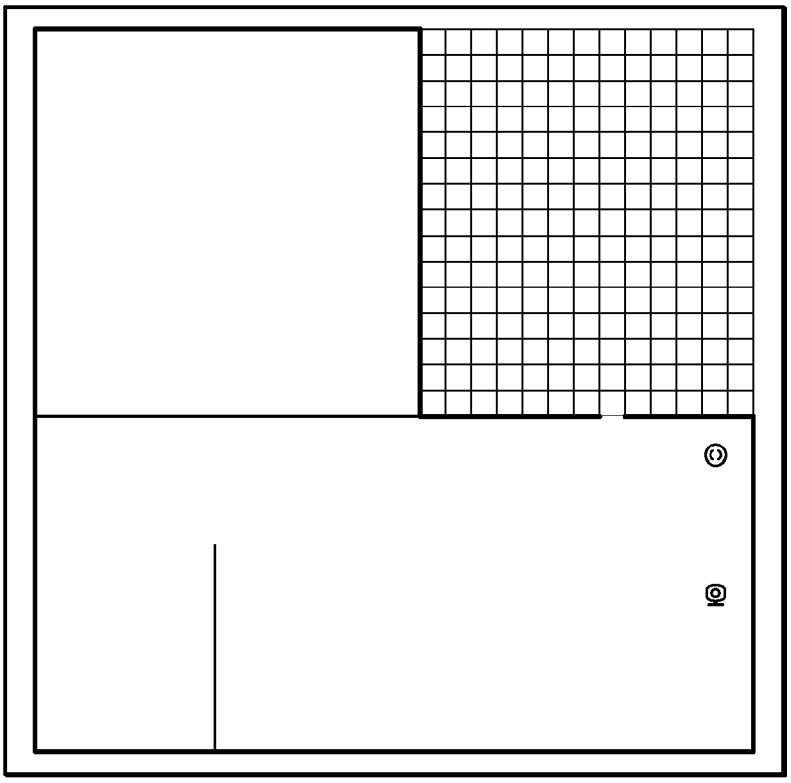


FIG. 63

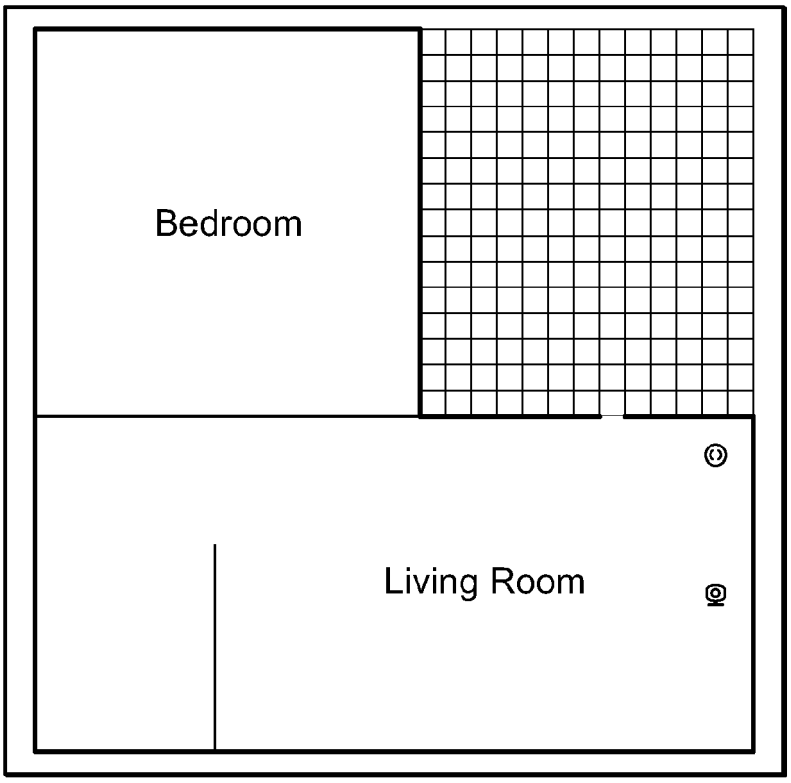


FIG. 64

FIG. 65

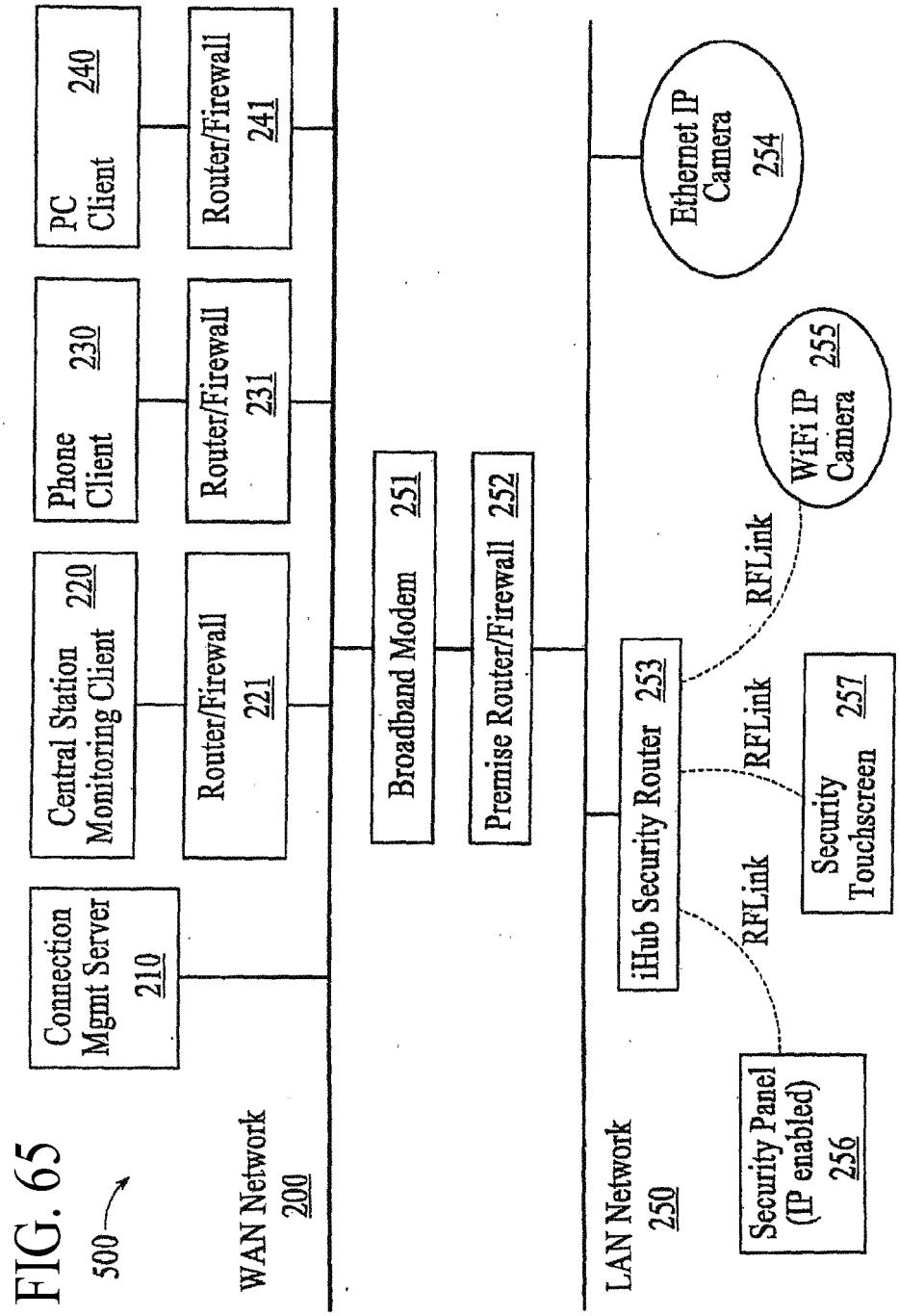
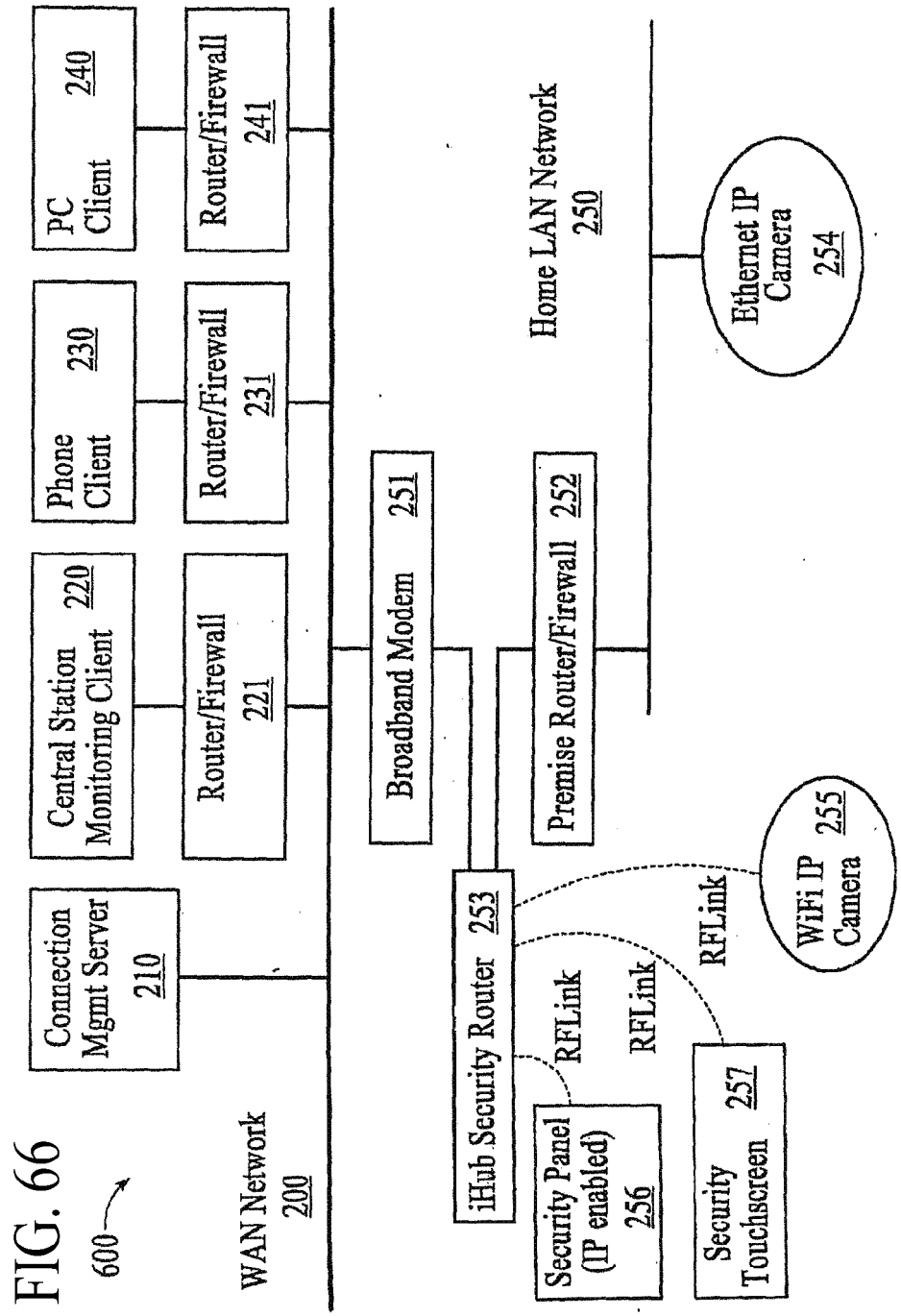

500
WAN Network 200
LAN Network 250
Connection Mgmt Server 210
Central Station Monitoring Client 220
Phone Client 230
PC Client 240
Router/Firewall 221
Router/Firewall 231
Router/Firewall 241
Broadband Modem 251
Premise Router/Firewall 252
iHub Security Router 253
Ethernet IP Camera 254
WiFi IP Camera 255
Security Panel (IP enabled) 256
Security Touchscreen 257
RFLink
RFLink
RFLink

FIG. 66


600
WAN Network 200
Connection Mgmt Server 210
Central Station Monitoring Client 220
Phone Client 230
PC Client 240
Router/Firewall 221
Router/Firewall 231
Router/Firewall 241
Broadband Modem 251
iHub Security Router 253
Premise Router/Firewall 252
Home LAN Network 250
Ethernet IP Camera 254
WiFi IP Camera 255
RFLink
RFLink
RFLink
Security Panel (IP enabled) 256
Security Touchscreen 257

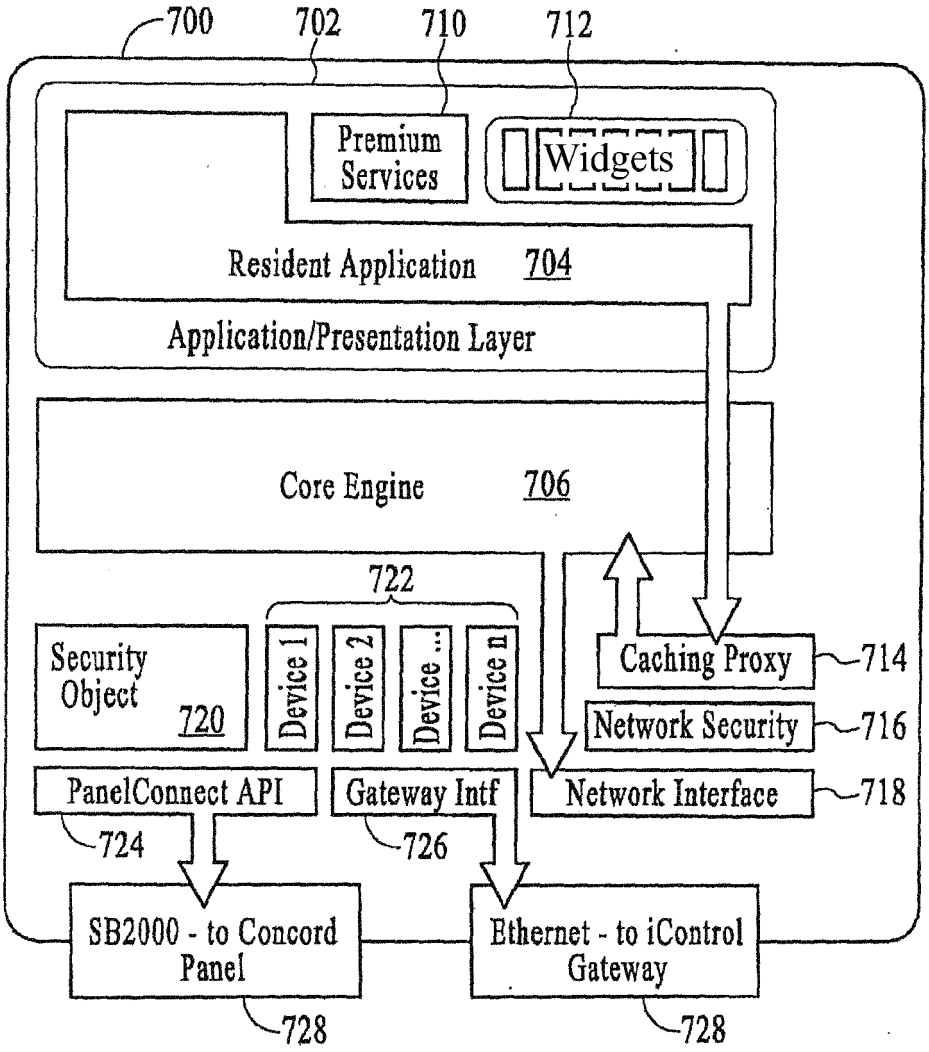

700
702
710
712
Premium Services
Widgets
Resident Application 704
Application/Presentation Layer
Core Engine 706
722
Security Object 720
Device 1
Device 2
Device ...
Device n
Caching Proxy
714
Network Security
716
PanelConnect API
Gateway Intf
Network Interface
718
724
726
SB2000 - to Concord Panel
Ethernet - to iControl Gateway
728
728

FIG. 67

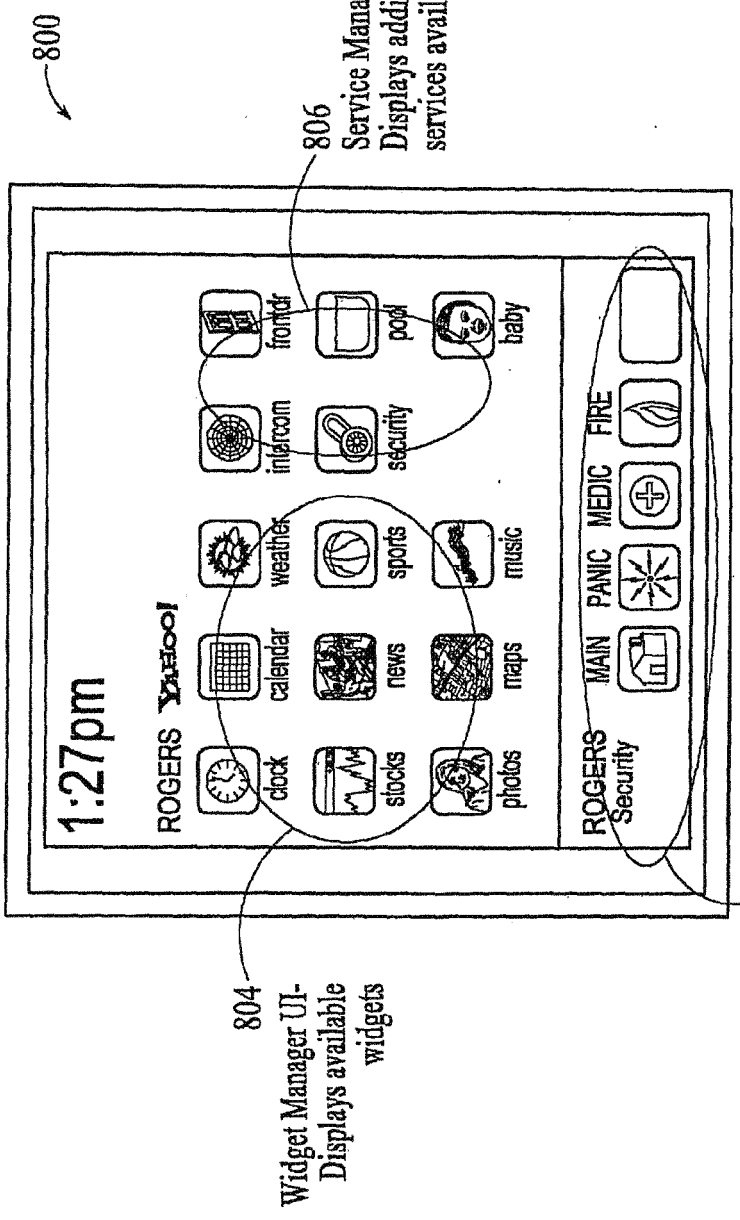

800
806
Service Manager UI-
Displays additional
services available
1:27pm
ROGERS
clock
calendar
weather
intercom
security
pool
baby
stocks
news
sports
music
photos
maps
ROGERS
Security
MAIN
PANIC
MEDIC
FIRE
804
Widget Manager UI-
Displays available
widgets
802
Resident application UI-
Core security functionality,
always available

FIG. 68

FIG. 69

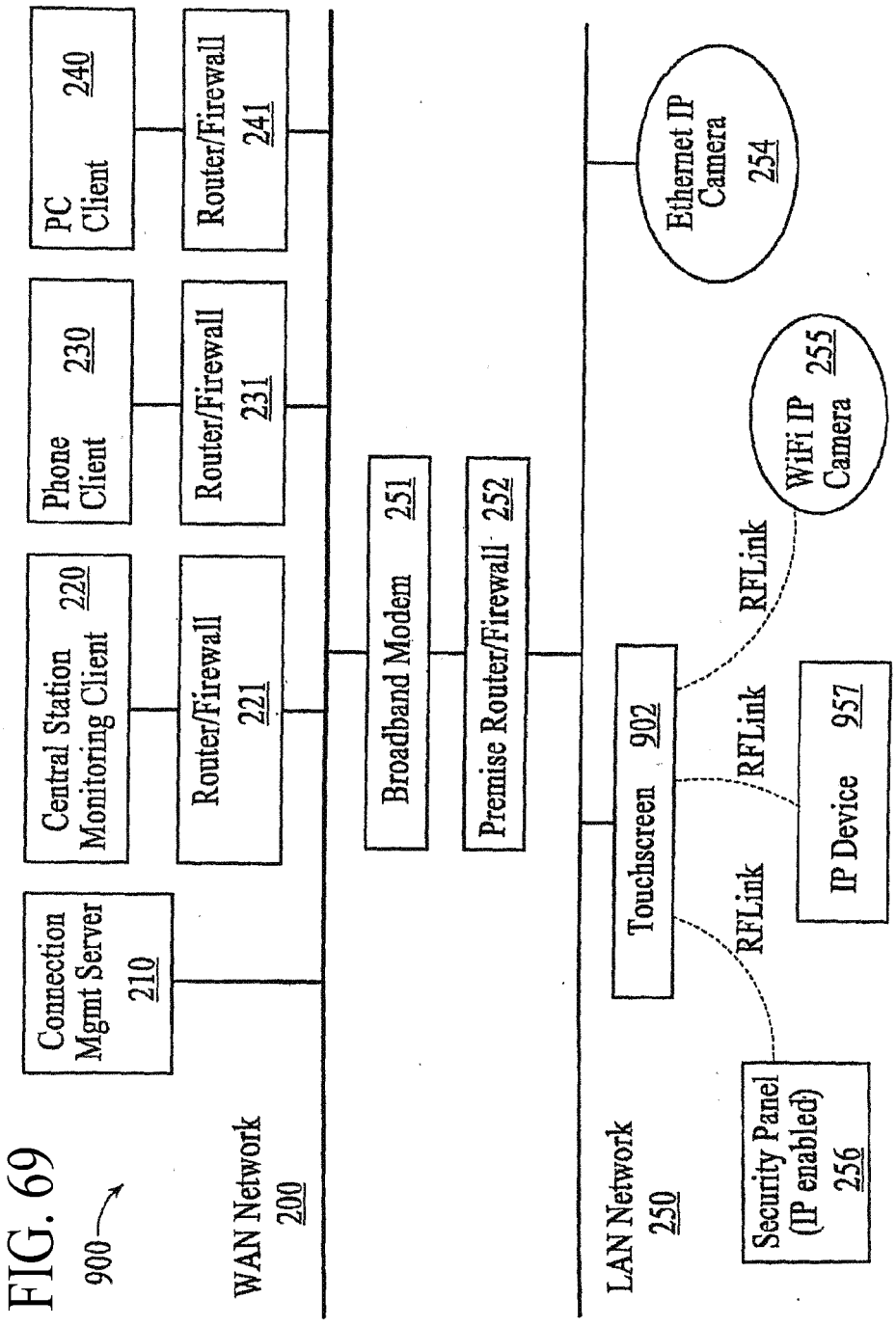
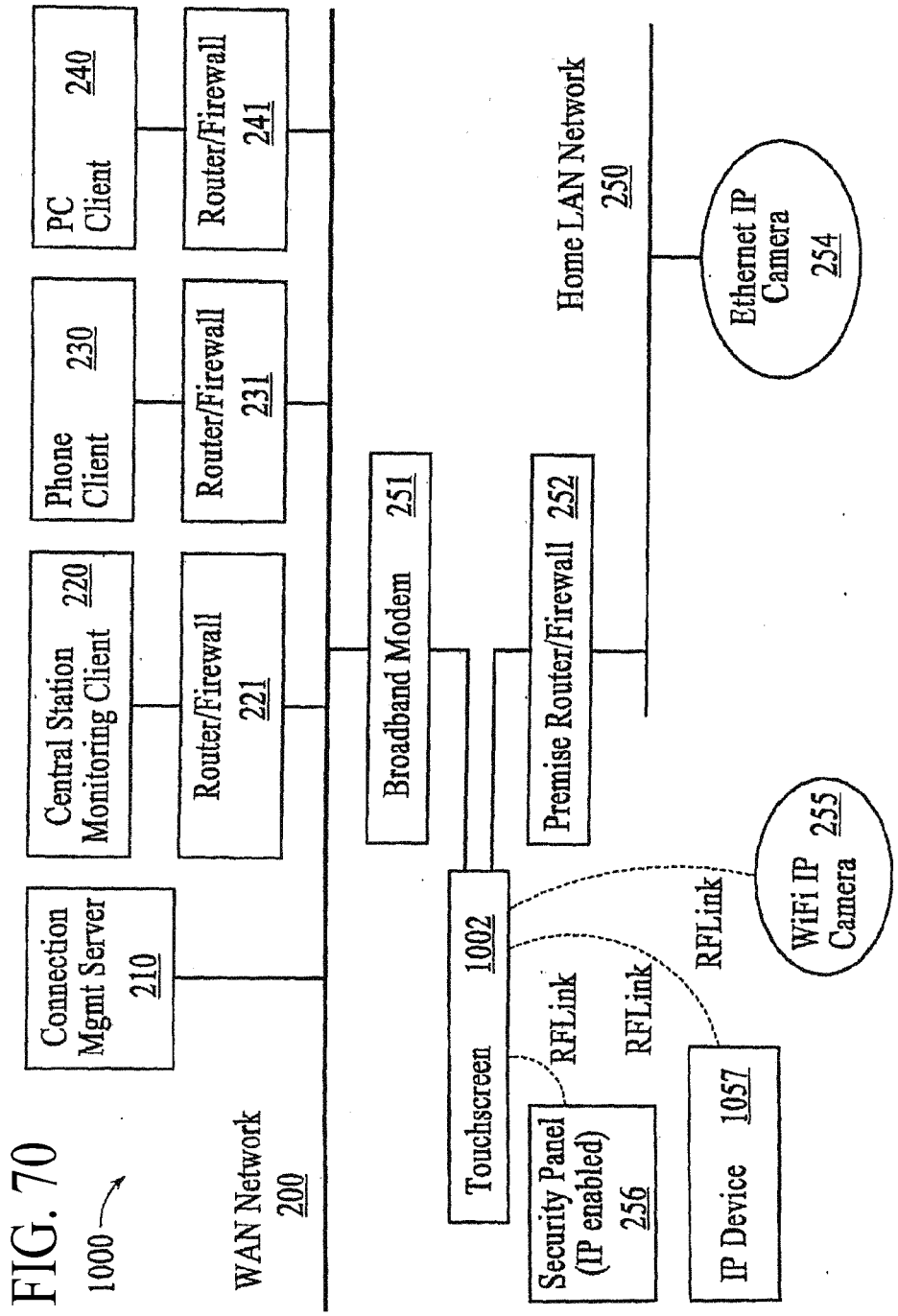

900
WAN Network 200
LAN Network 250
Connection Mgmt Server 210
Central Station Monitoring Client 220
Router/Firewall 221
Phone Client 230
Router/Firewall 231
PC Client 240
Router/Firewall 241
Broadband Modem 251
Premise Router/Firewall 252
Touchscreen 902
Ethernet IP Camera 254
WiFi IP Camera 255
IP Device 957
Security Panel (IP enabled) 256
RFLink
RFLink
RFLink

FIG. 70


1000
WAN Network 200
Connection Mgmt Server 210
Central Station Monitoring Client 220
Phone Client 230
PC Client 240
Router/Firewall 221
Router/Firewall 231
Router/Firewall 241
Broadband Modem 251
Premise Router/Firewall 252
Home LAN Network 250
Ethernet IP Camera 254
Touchscreen 1002
Security Panel (IP enabled) 256
IP Device 1057
WiFi IP Camera 255
RFLink
RFLink
RFLink

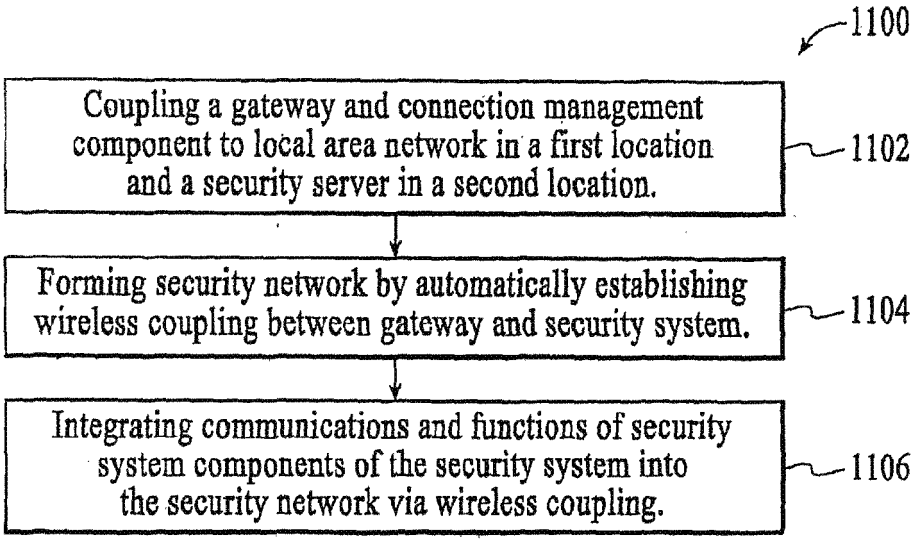

1100
Coupling a gateway and connection management component to local area network in a first location and a security server in a second location.
1102
Forming security network by automatically establishing wireless coupling between gateway and security system.
1104
Integrating communications and functions of security system components of the security system into the security network via wireless coupling.
1106

FIG. 71

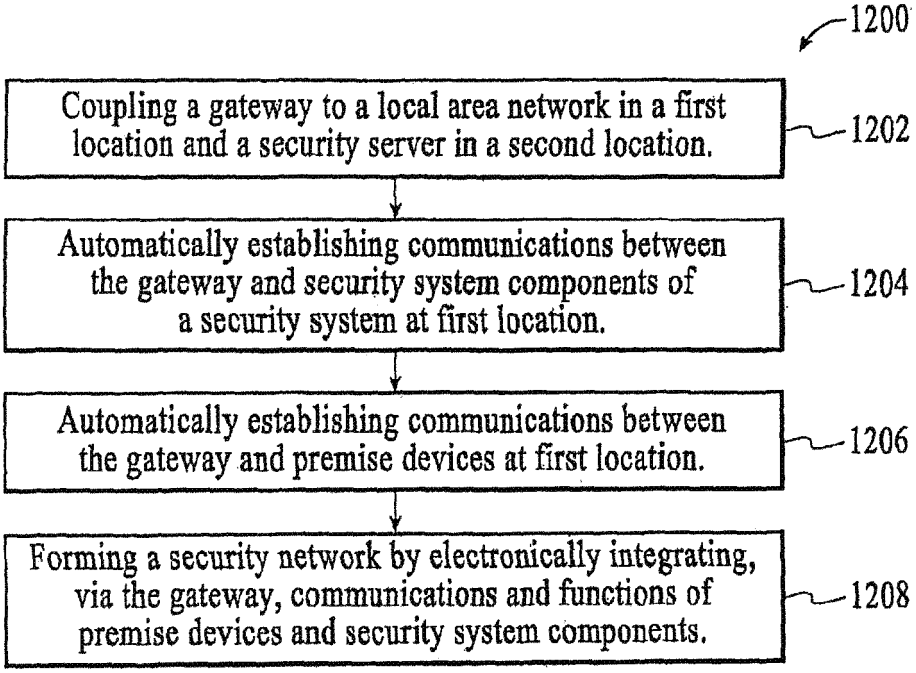

1200
Coupling a gateway to a local area network in a first location and a security server in a second location.
1202
Automatically establishing communications between the gateway and security system components of a security system at first location.
1204
Automatically establishing communications between the gateway and premise devices at first location.
1206
Forming a security network by electronically integrating, via the gateway, communications and functions of premise devices and security system components.
1208

FIG. 72

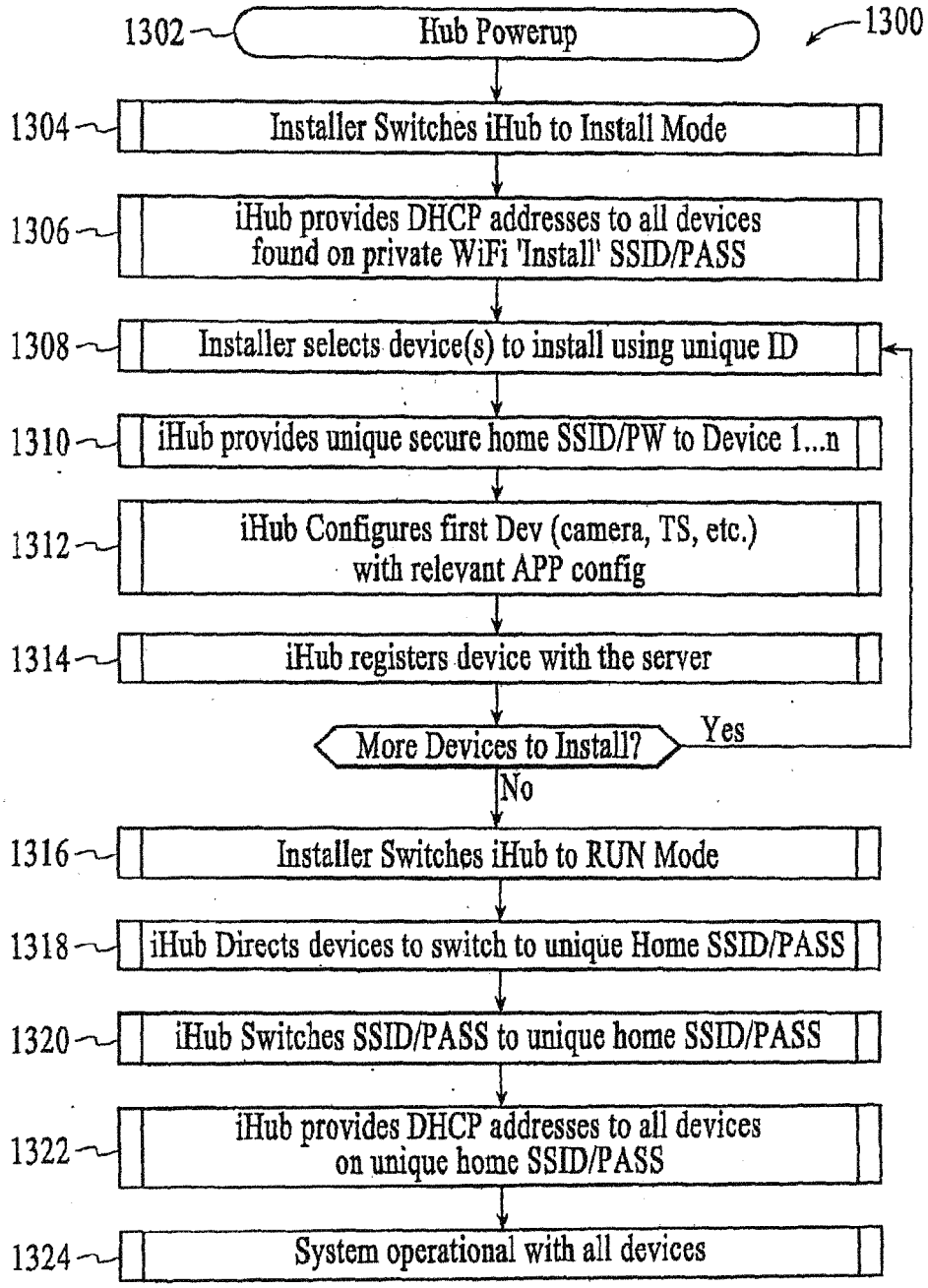

1302
Hub Powerup
1300
1304
Installer Switches iHub to Install Mode
1306
iHub provides DHCP addresses to all devices found on private WiFi 'Install' SSID/PASS
1308
Installer selects device(s) to install using unique ID
1310
iHub provides unique secure home SSID/PW to Device 1...n
1312
iHub Configures first Dev (camera, TS, etc.) with relevant APP config
1314
iHub registers device with the server
More Devices to Install?
Yes
No
1316
Installer Switches iHub to RUN Mode
1318
iHub Directs devices to switch to unique Home SSID/PASS
1320
iHub Switches SSID/PASS to unique home SSID/PASS
1322
iHub provides DHCP addresses to all devices on unique home SSID/PASS
1324
System operational with all devices

FIG. 73

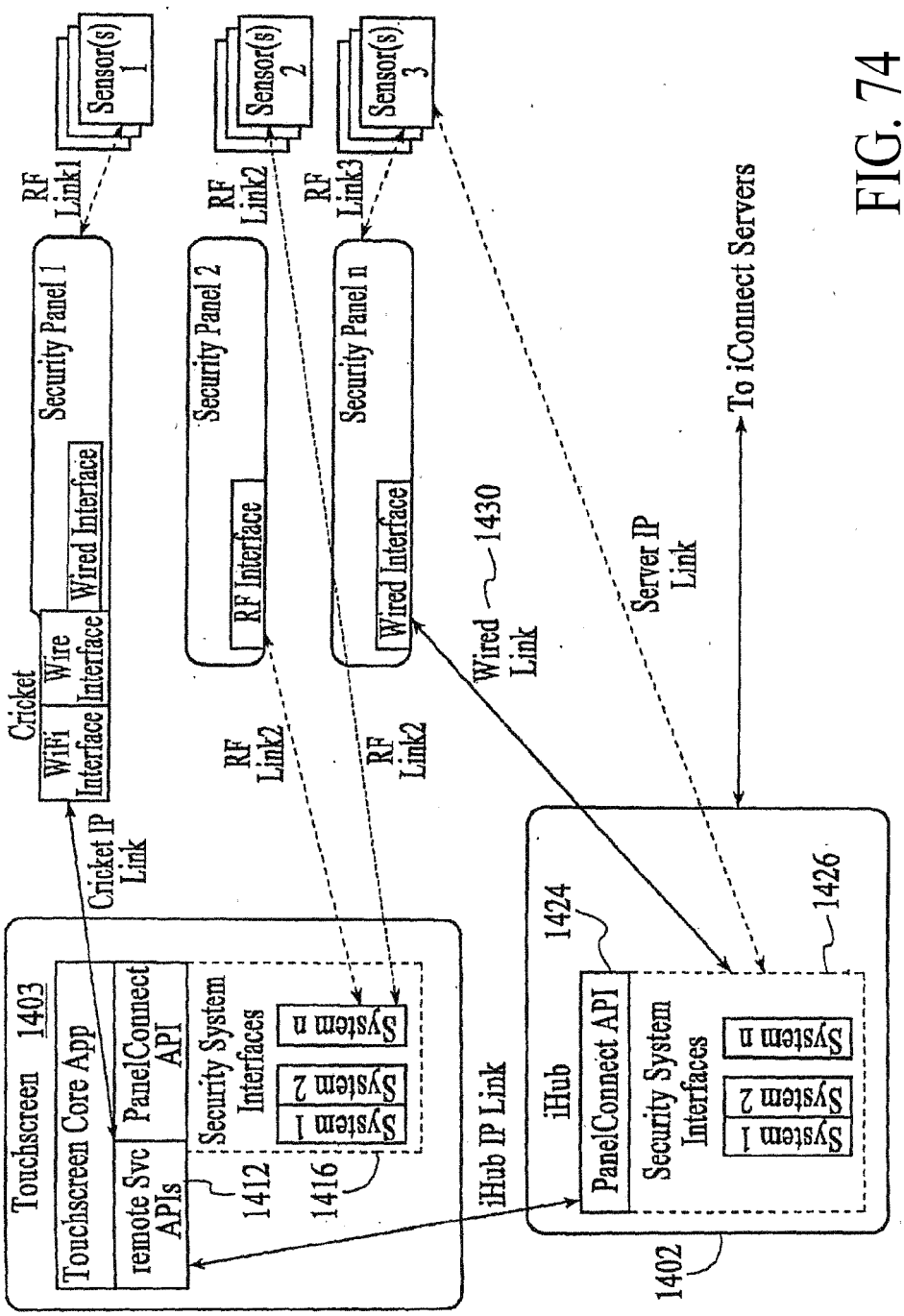

Sensor(s) 1
Sensor(s) 2
Sensor(s) 3
RF Link1
RF Link2
RF Link3
Security Panel 1
Security Panel 2
Security Panel n
Wired Interface
RF Interface
Wired Interface
Cricket
WiFi Interface
Wire Interface
Cricket IP Link
RF Link2
RF Link2
Wired Link
1430
Server IP Link
To iConnect Servers
Touchscreen 1403
Touchscreen Core App
remote Svc APIs
PanelConnect API
Security System Interfaces
System 1
System 2
System n
1412
1416
iHub IP Link
iHub
1424
PanelConnect API
Security System Interfaces
System 1
System 2
System n
1426
1402

FIG. 74

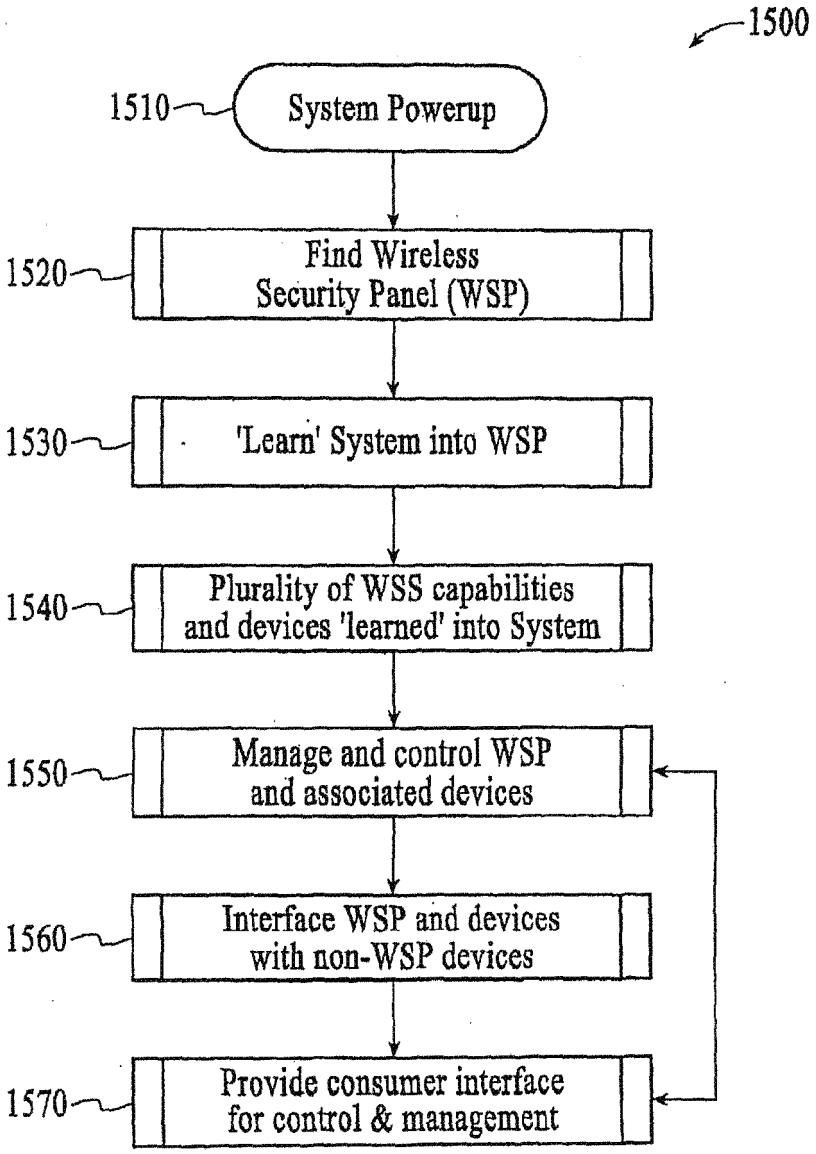

1500
1510
System Powerup
1520
Find Wireless Security Panel (WSP)
1530
'Learn' System into WSP
1540
Plurality of WSS capabilities and devices 'learned' into System
1550
Manage and control WSP and associated devices
1560
Interface WSP and devices with non-WSP devices
1570
Provide consumer interface for control & management

FIG. 75

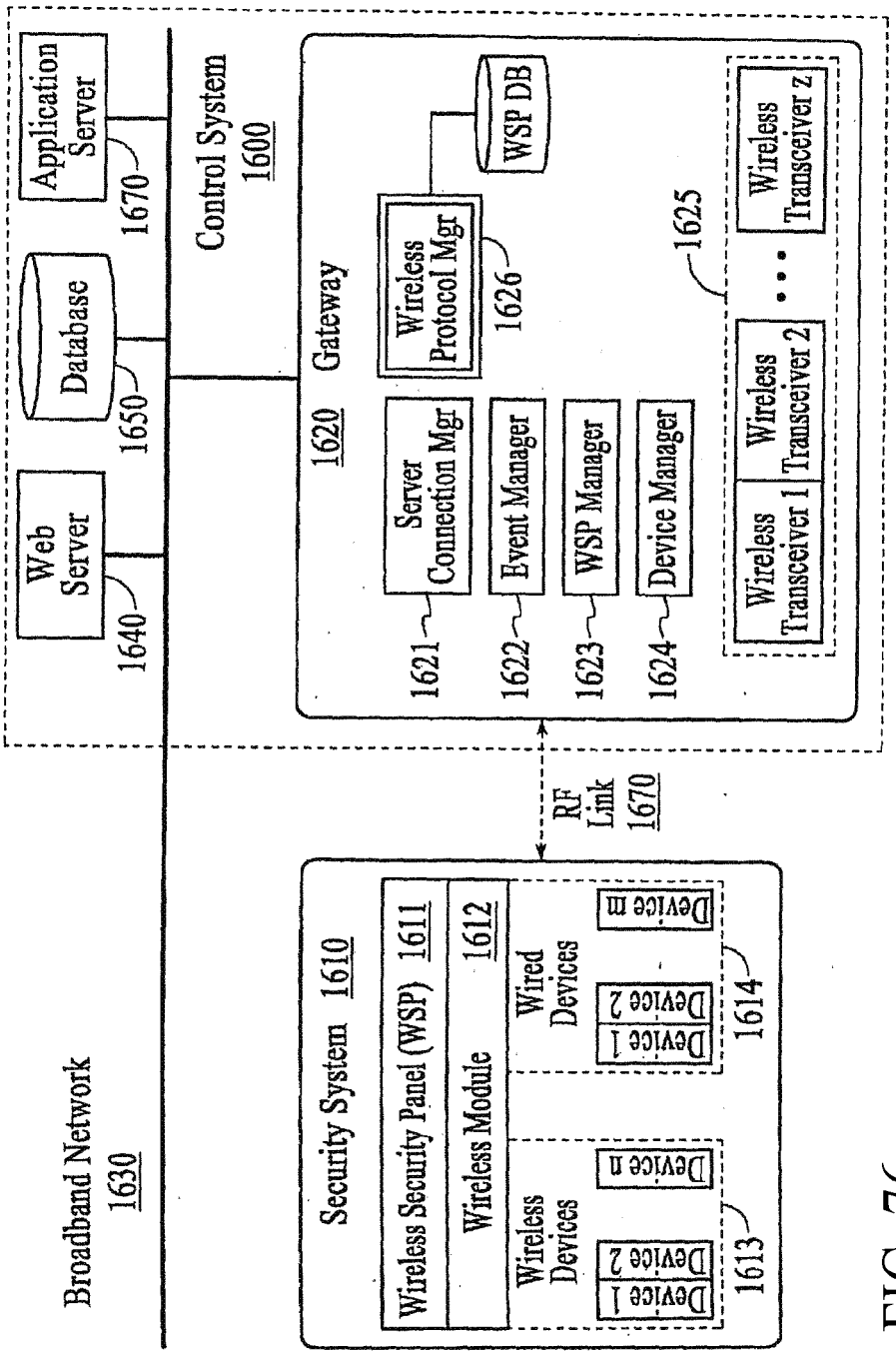

Broadband Network
1630
Web Server
1640
Database
1650
Application Server
1670
Control System
1600
Gateway
1620
Server Connection Mgr
1621
Event Manager
1622
WSP Manager
1623
Device Manager
1624
Wireless Protocol Mgr
1626
WSP DB
1625
Wireless Transceiver 1
Wireless Transceiver 2
Wireless Transceiver z
RF Link
1670
Security System 1610
Wireless Security Panel (WSP) 1611
Wireless Module 1612
Wireless Devices
Device 1
Device 2
Device n
1613
Wired Devices
Device 1
Device 2
Device m
1614

FIG. 76

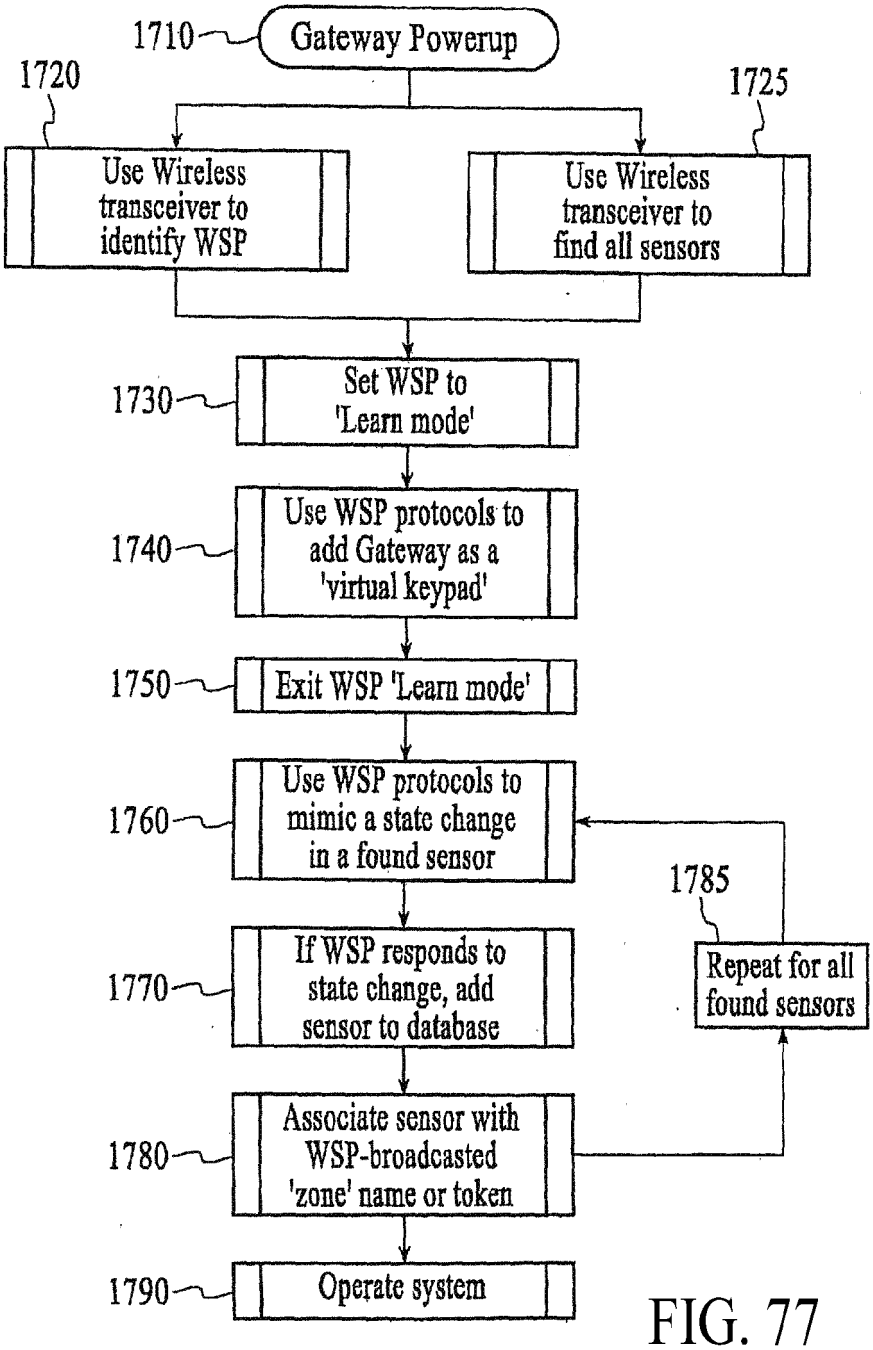

1710
Gateway Powerup
1720
1725
Use Wireless transceiver to identify WSP
Use Wireless transceiver to find all sensors
1730
Set WSP to 'Learn mode'
1740
Use WSP protocols to add Gateway as a 'virtual keypad'
1750
Exit WSP 'Learn mode'
1760
Use WSP protocols to mimic a state change in a found sensor
1785
Repeat for all found sensors
1770
If WSP responds to state change, add sensor to database
1780
Associate sensor with WSP-broadcasted 'zone' name or token
1790
Operate system

FIG. 77

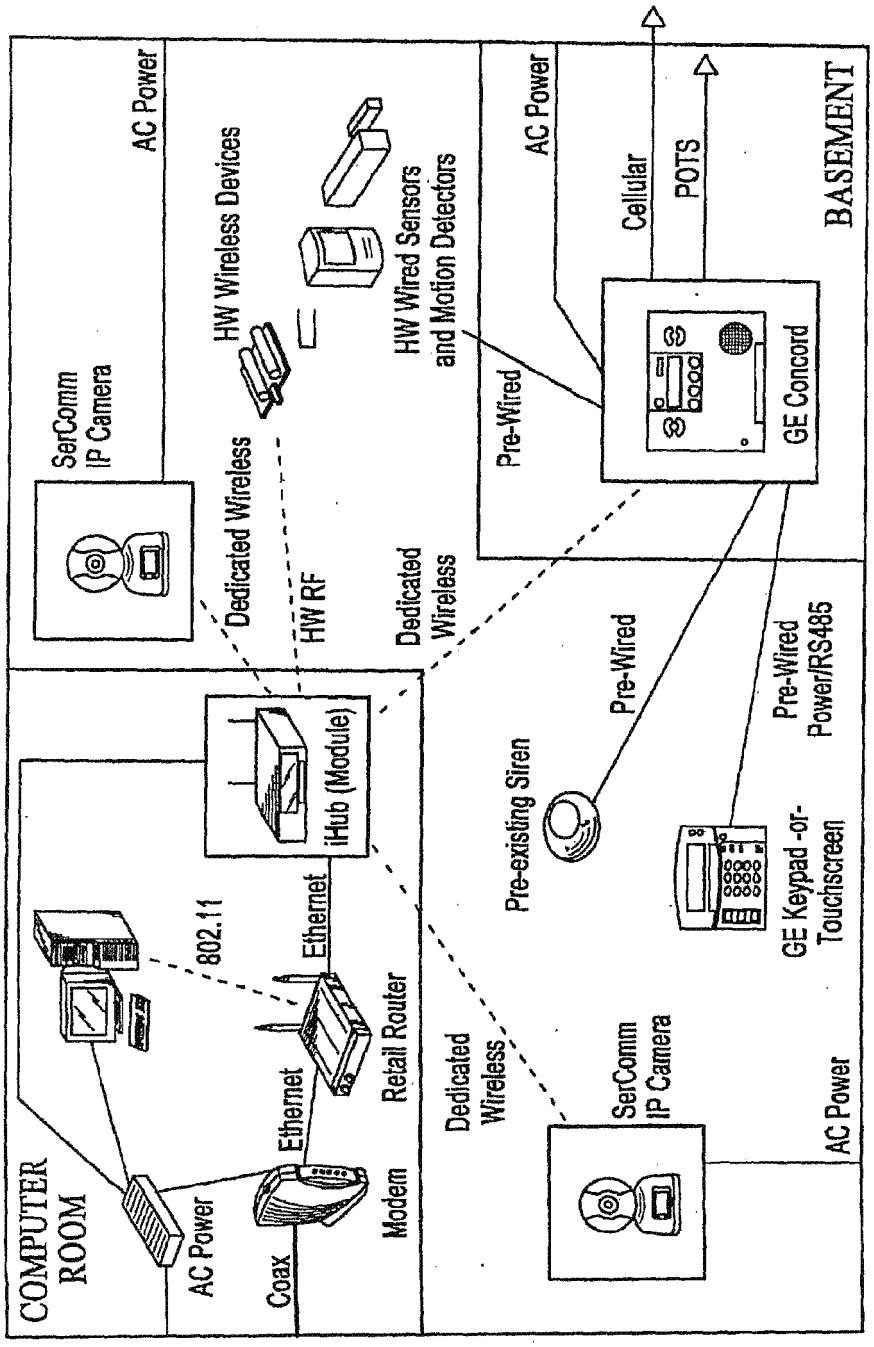

COMPUTER ROOM
AC Power
Coax
Modem
Ethernet
Retail Router
802.11
Ethernet
iHub (Module)
Dedicated Wireless
HW RF
Dedicated Wireless
SerComm IP Camera
AC Power
HW Wireless Devices
HW Wired Sensors and Motion Detectors
Pre-existing Siren
Pre-Wired
Dedicated Wireless
SerComm IP Camera
AC Power
GE Keypad -or- Touchscreen
Pre-Wired Power/RS485
Pre-Wired
AC Power
Cellular
POTS
GE Concord
BASEMENT

FIG. 78

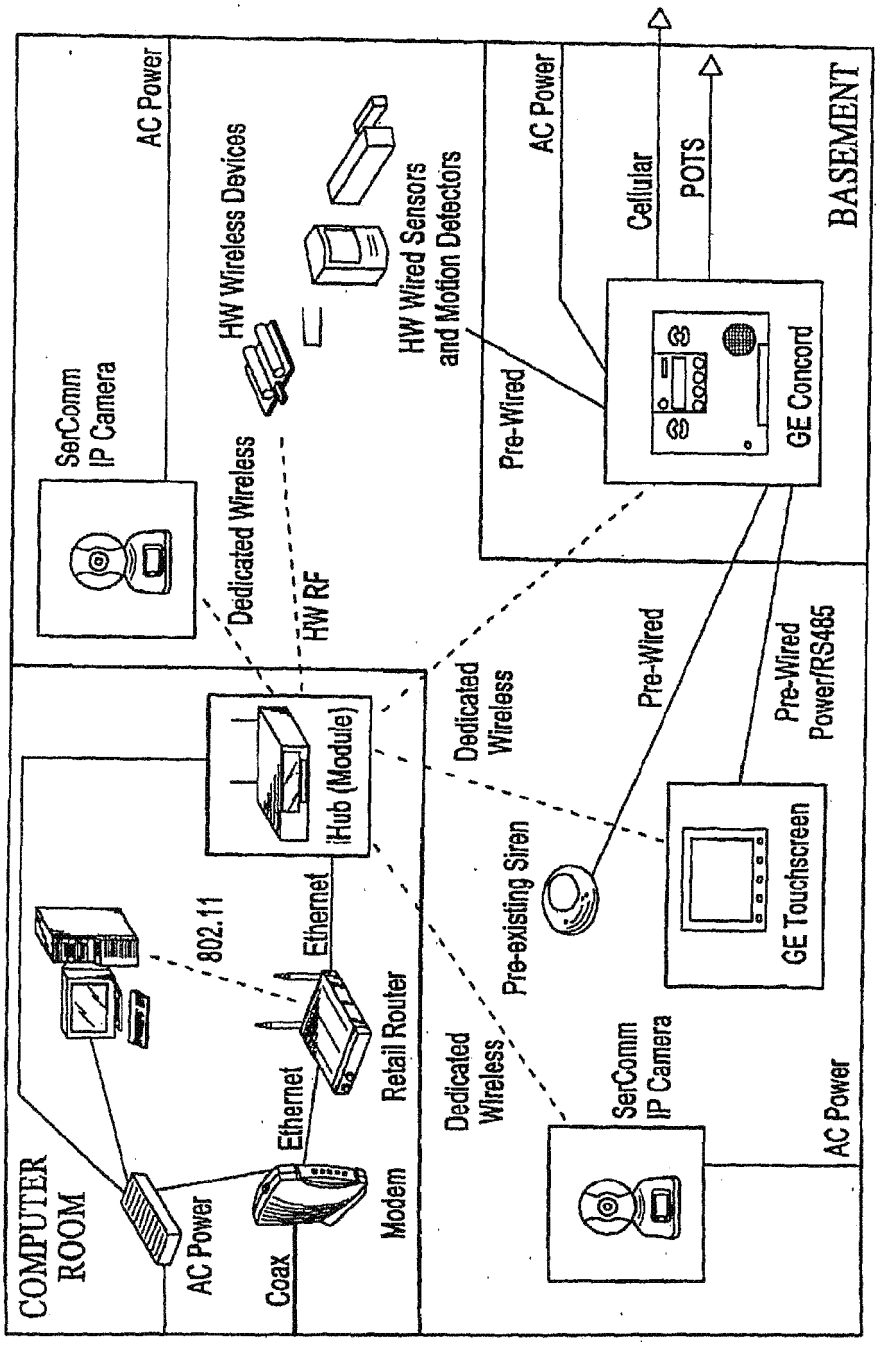

COMPUTER ROOM
AC Power
Coax
Modem
Ethernet
Retail Router
802.11
Ethernet
iHub (Module)
Dedicated Wireless
HW RF
SerComm IP Camera
AC Power
HW Wireless Devices
HW Wired Sensors and Motion Detectors
Dedicated Wireless
Pre-existing Siren
Dedicated Wireless
SerComm IP Camera
AC Power
Pre-Wired
Pre-Wired
Pre-Wired Power/RS485
GE Touchscreen
AC Power
Pre-Wired
Cellular
POTS
GE Concord
BASEMENT

FIG. 79

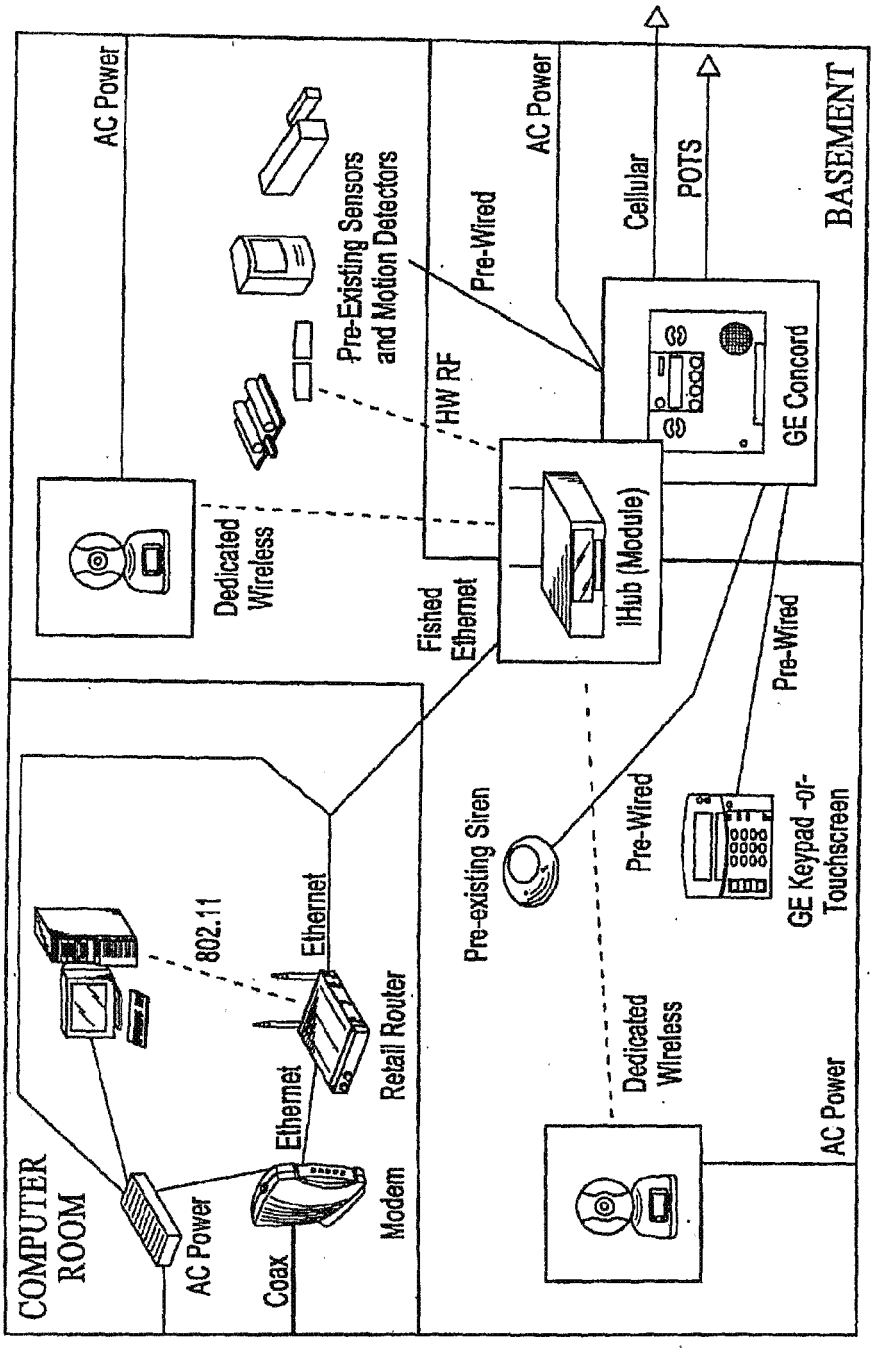

COMPUTER ROOM
AC Power
Coax
Modem
Ethernet
Retail Router
802.11
Ethernet
Dedicated Wireless
AC Power
Pre-existing Siren
Fished Ethernet
HW RF
Pre-Existing Sensors and Motion Detectors
Pre-Wired
iHub (Module)
Dedicated Wireless
Pre-Wired
GE Keypad -or- Touchscreen
AC Power
Pre-Wired
GE Concord
Cellular
POTS
BASEMENT

FIG. 80

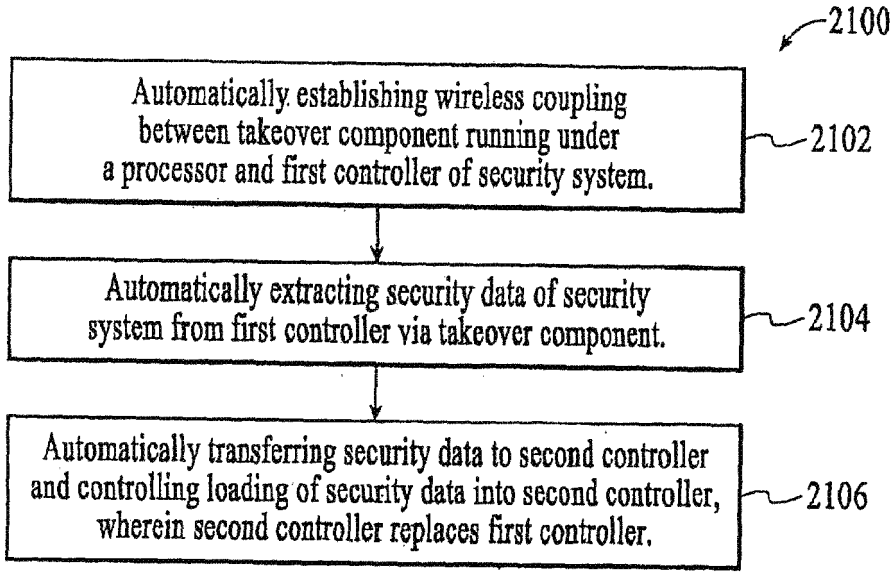

2100
Automatically establishing wireless coupling between takeover component running under a processor and first controller of security system.
2102
Automatically extracting security data of security system from first controller via takeover component.
2104
Automatically transferring security data to second controller and controlling loading of security data into second controller, wherein second controller replaces first controller.
2106

FIG. 81

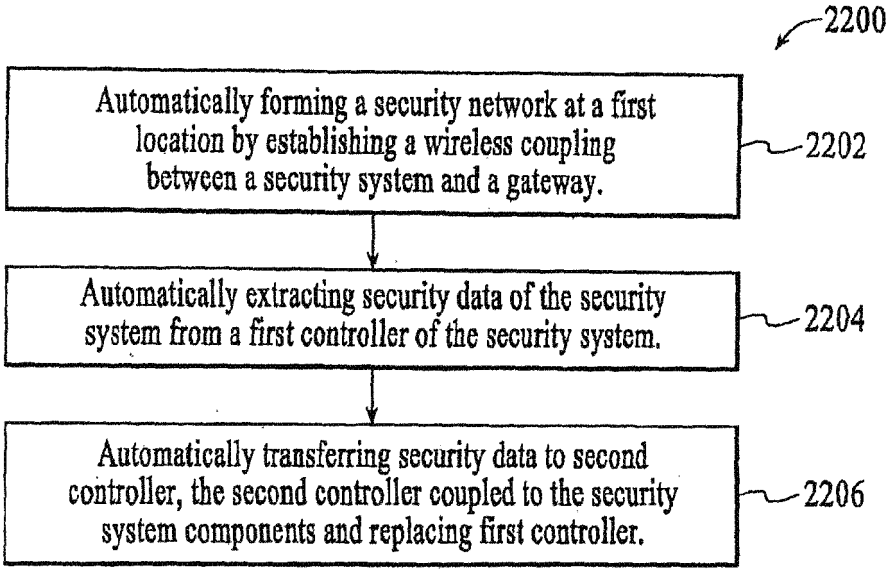

2200
Automatically forming a security network at a first location by establishing a wireless coupling between a security system and a gateway.
2202
Automatically extracting security data of the security system from a first controller of the security system.
2204
Automatically transferring security data to second controller, the second controller coupled to the security system components and replacing first controller.
2206

FIG. 82

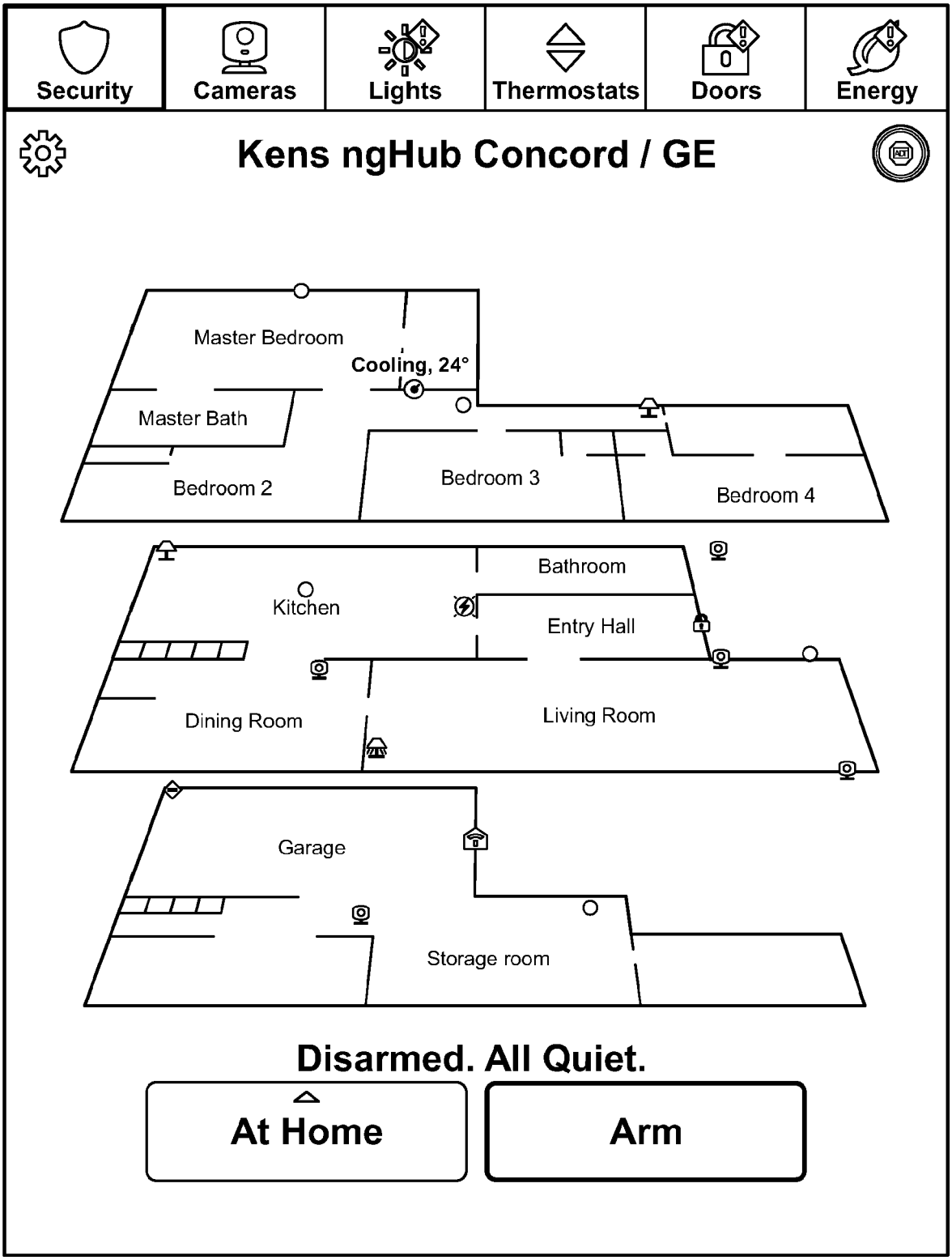

Security
Cameras
Lights
Thermostats
Doors
Energy
Kens ngHub Concord / GE
Master Bedroom
Cooling, 24°
Master Bath
Bedroom 2
Bedroom 3
Bedroom 4
Bathroom
Kitchen
Entry Hall
Dining Room
Living Room
Garage
Storage room
Disarmed. All Quiet.
At Home
Arm

FIG. 83

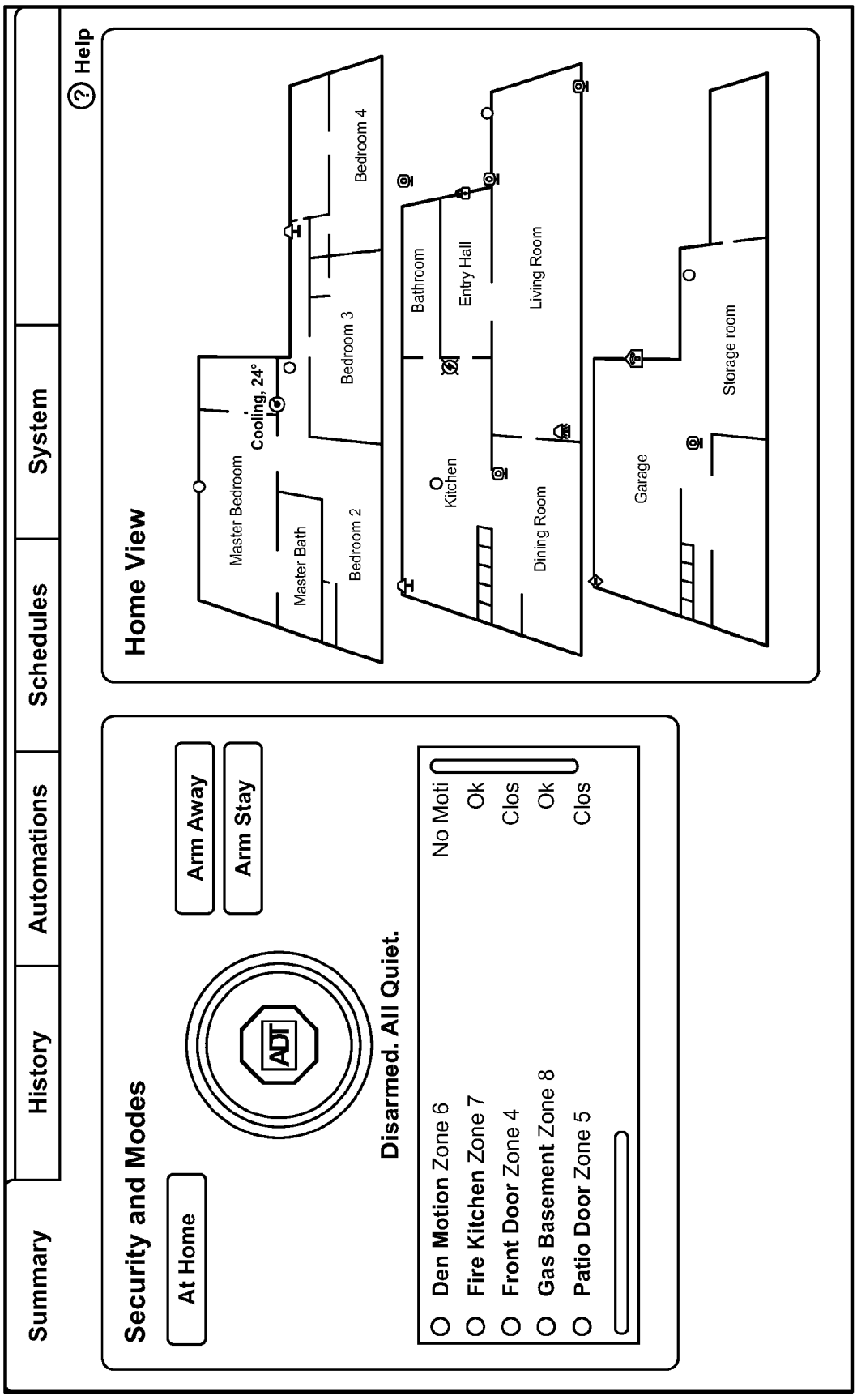

Summary
History
Automations
Schedules
System
Help
Security and Modes
At Home
Arm Away
Arm Stay
Disarmed. All Quiet.
Den Motion Zone 6
Fire Kitchen Zone 7
Front Door Zone 4
Gas Basement Zone 8
Patio Door Zone 5
No Moti
Ok
Clos
Ok
Clos
Home View
Master Bedroom
Cooling, 24°
Master Bath
Bedroom 2
Bedroom 3
Bedroom 4
Bathroom
Entry Hall
Living Room
Kitchen
Dining Room
Garage
Storage room

FIG. 84

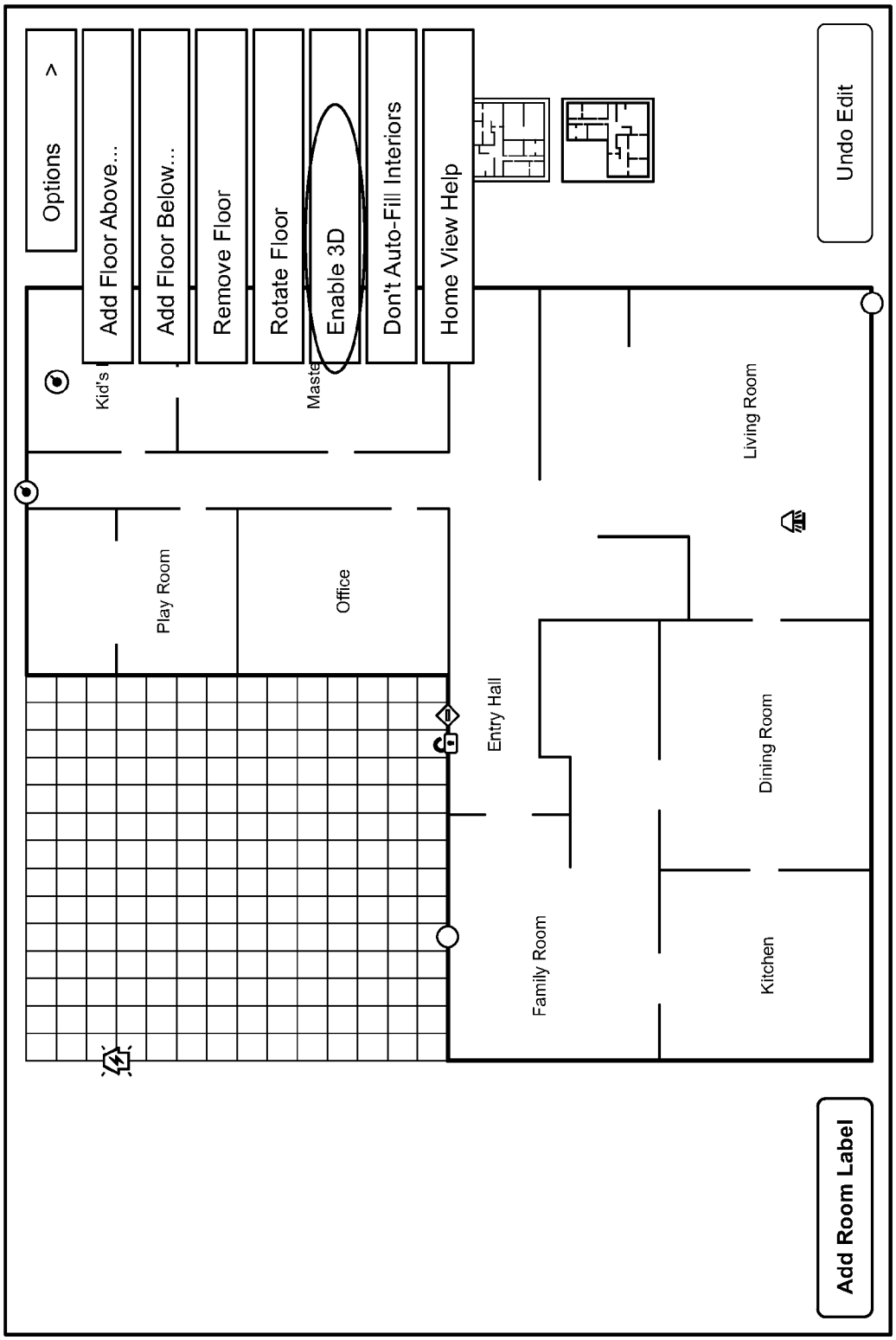

Options >
Add Floor Above...
Add Floor Below...
Remove Floor
Rotate Floor
Enable 3D
Don't Auto-Fill Interiors
Home View Help
Undo Edit
Add Room Label
Kid's
Master
Play Room
Office
Entry Hall
Family Room
Living Room
Dining Room
Kitchen

FIG. 85

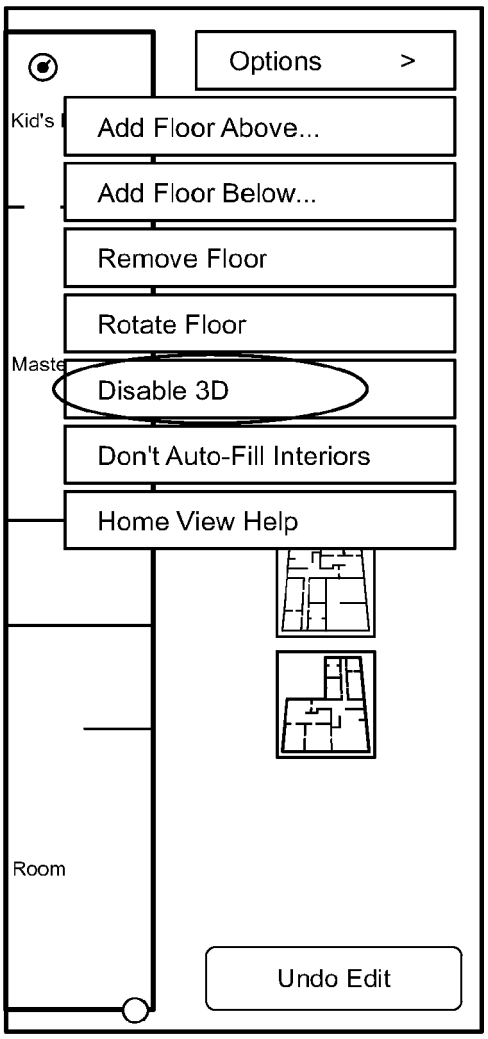

Options >
Add Floor Above...
Add Floor Below...
Remove Floor
Rotate Floor
Disable 3D
Don't Auto-Fill Interiors
Home View Help
Undo Edit
Room

FIG. 86

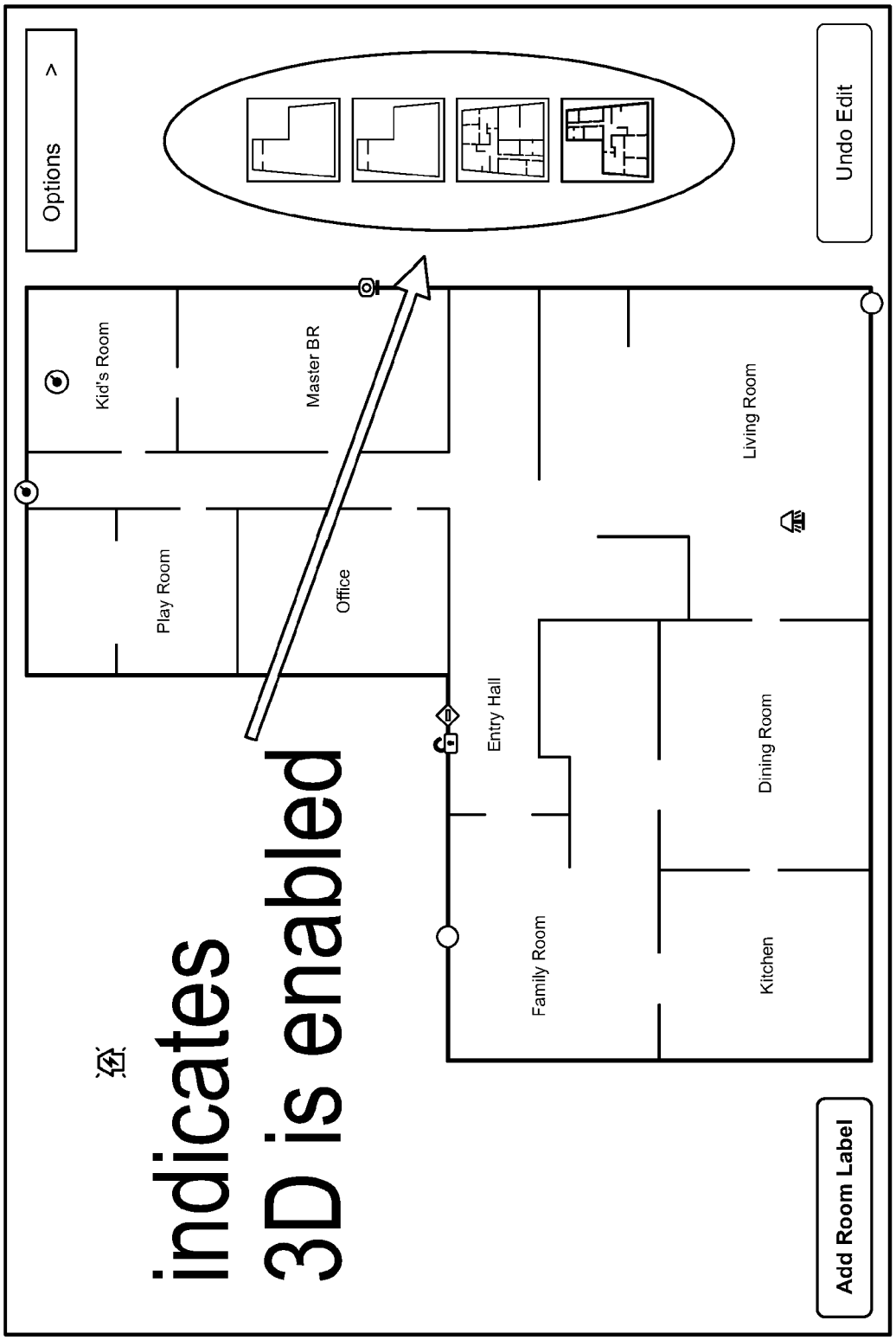

Options >
Undo Edit
Kid's Room
Master BR
Play Room
Office
Entry Hall
Living Room
Dining Room
Family Room
Kitchen
Add Room Label
indicates
3D is enabled

FIG. 87

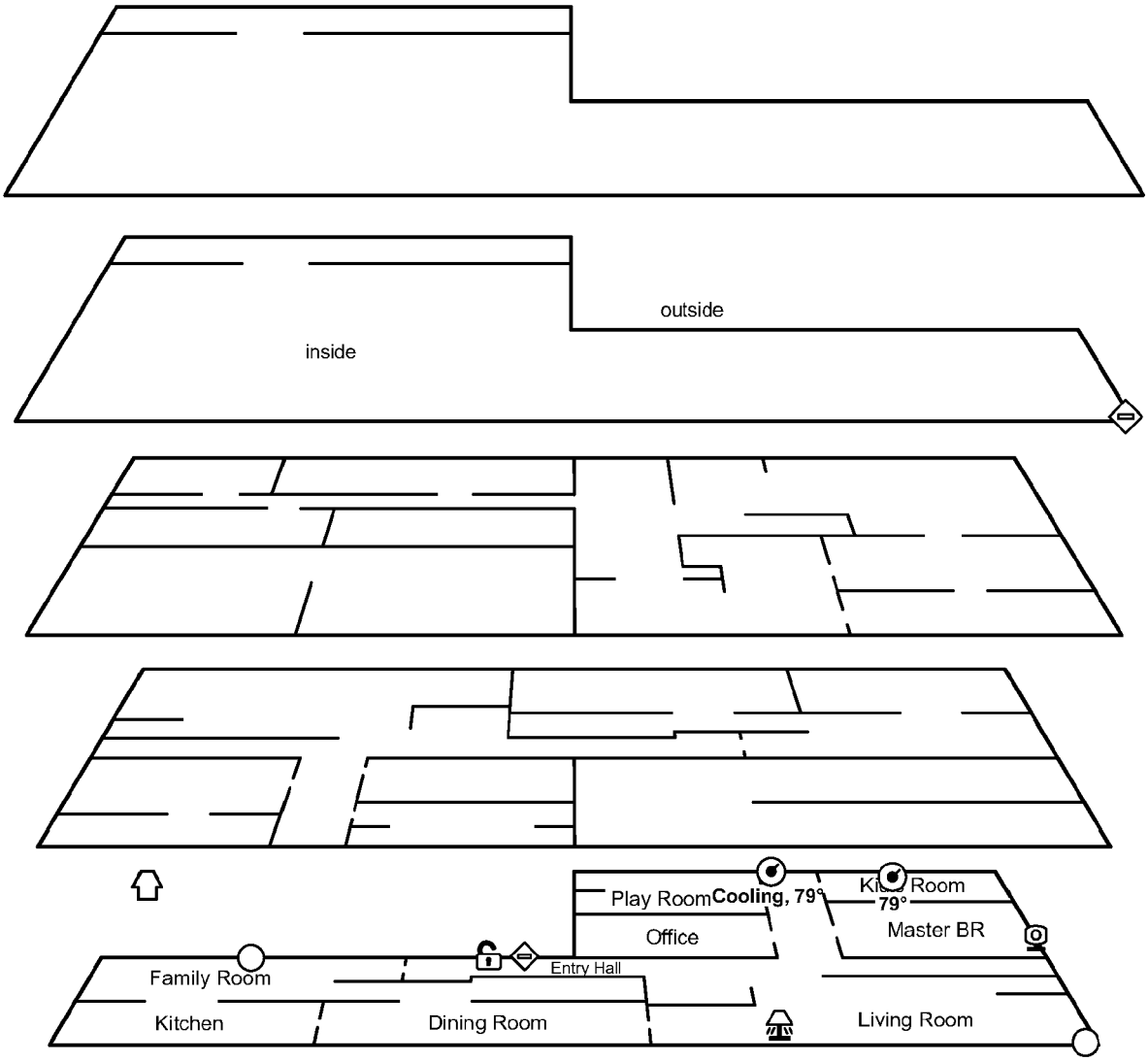

outside
inside
Play Room
Cooling, 79°
79°
Office
Master BR
Entry Hall
Family Room
Kitchen
Dining Room
Living Room

FIG. 88

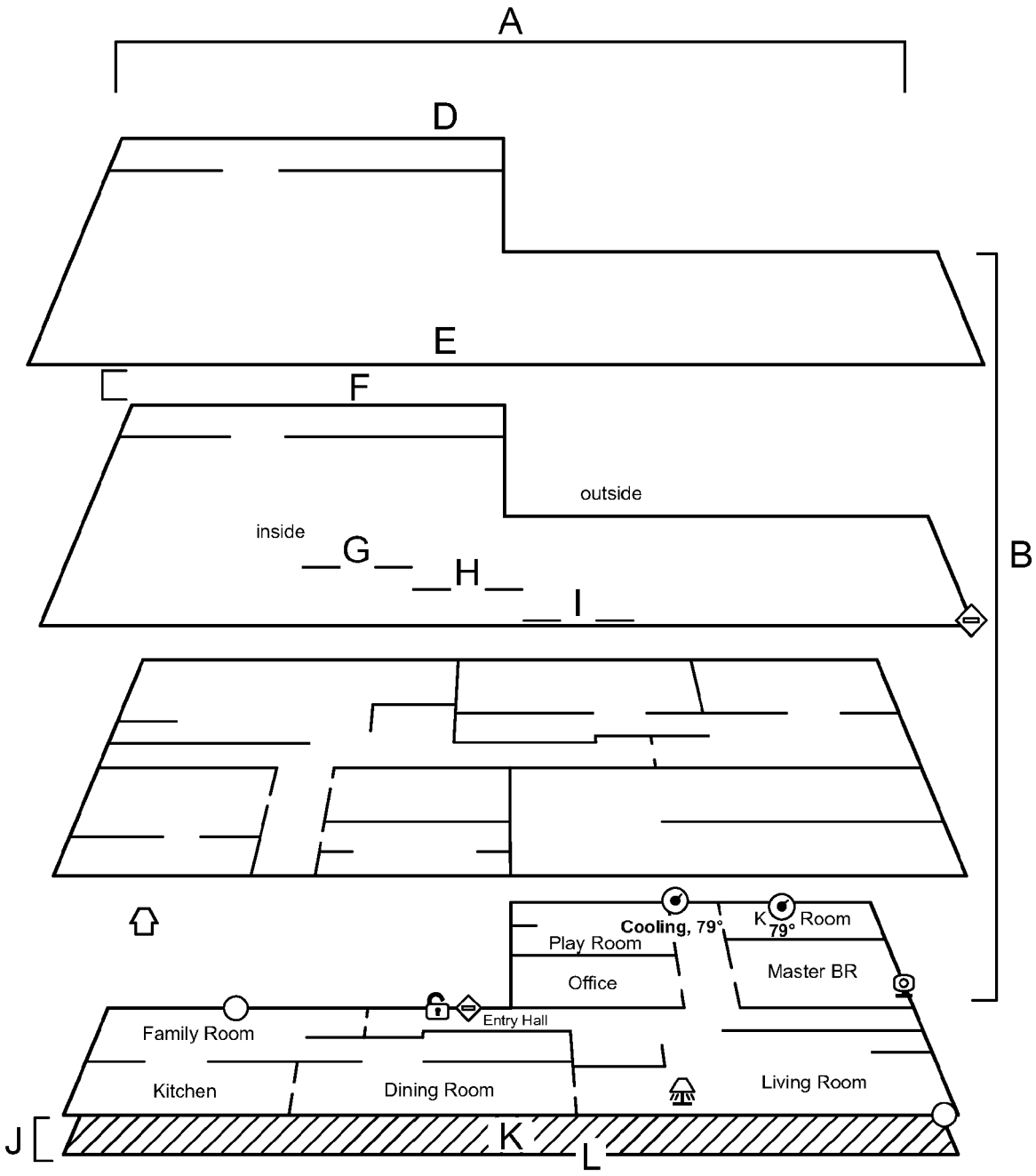
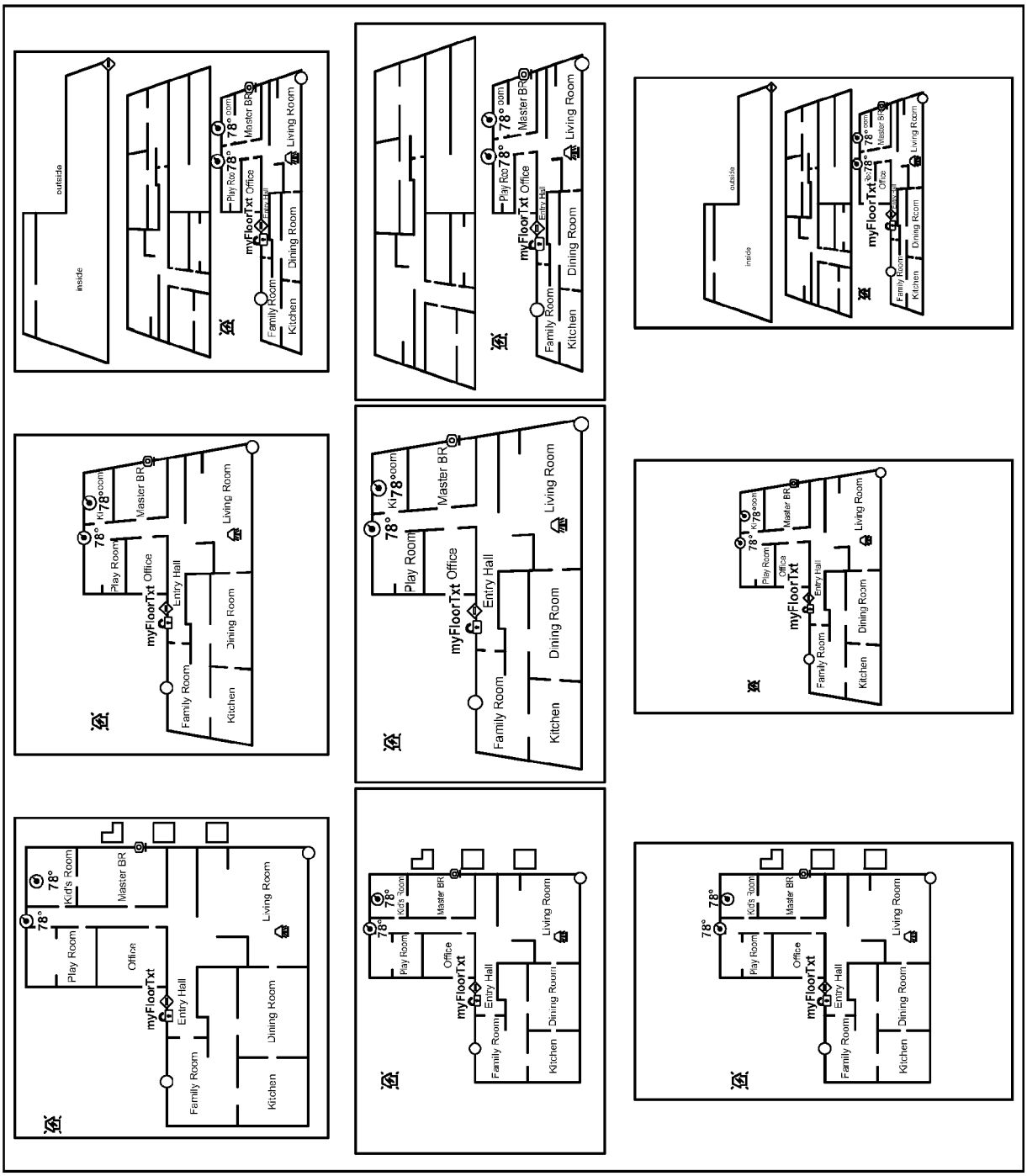

A
D
E
F
outside
inside
G
H
I
B
Cooling, 79°
K
79°
Room
Play Room
Office
Master BR
Entry Hall
Family Room
Kitchen
Dining Room
Living Room
J
K
L

FIG. 89

FIG. 90


outside
inside
myFloorTxt
Office
Entry Hall
Family Room
Dining Room
Kitchen
Living Room
Master BR
Play Room
Kid's Room
78°

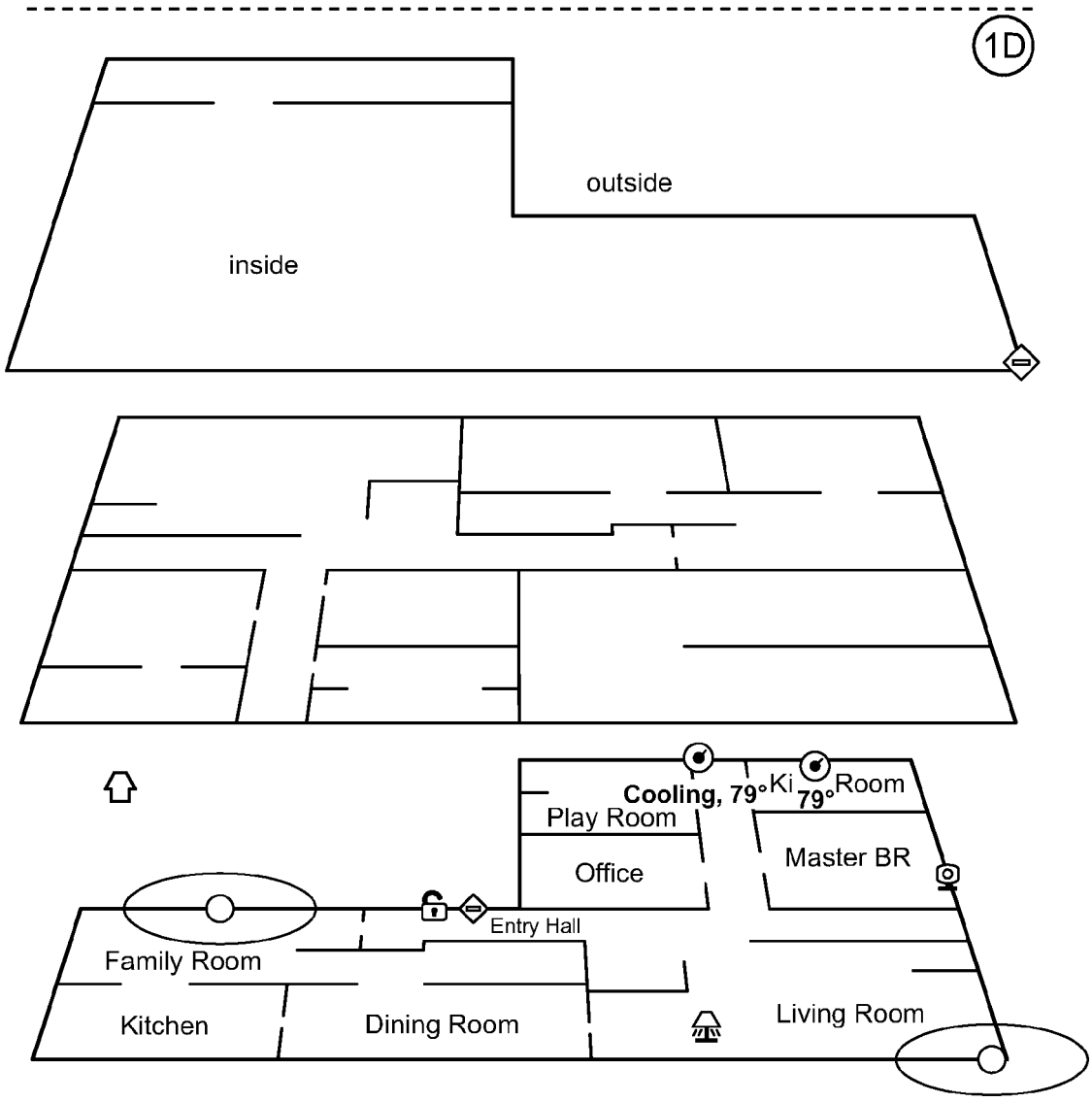

1D
outside
inside
Cooling, 79°
Ki
79°
Room
Play Room
Office
Master BR
Entry Hall
Family Room
Kitchen
Dining Room
Living Room

FIG. 91

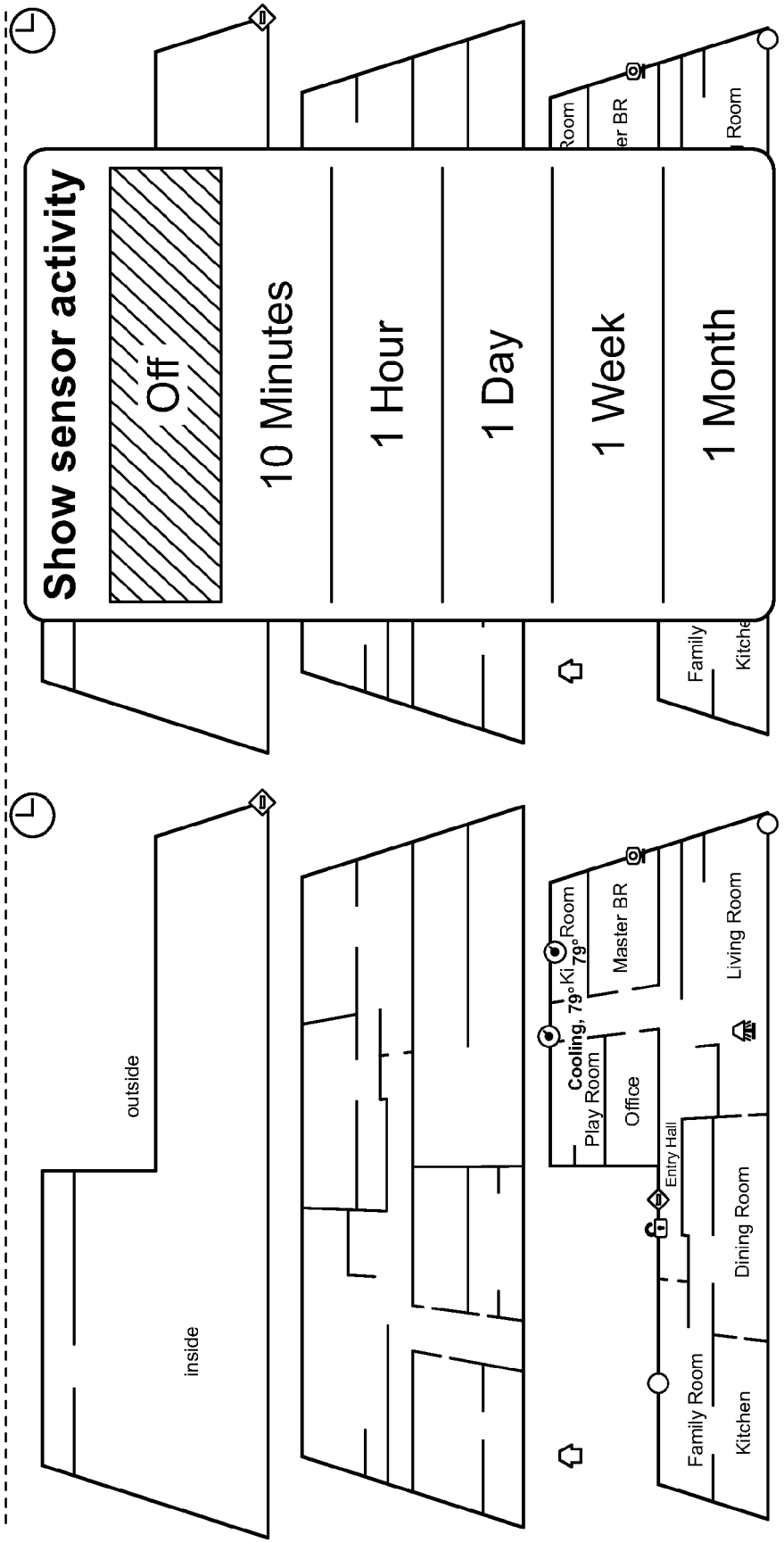

Show sensor activity
Off
10 Minutes
1 Hour
1 Day
1 Week
1 Month
outside
inside
Cooling, 79°
Play Room
Office
Entry Hall
Master BR
Living Room
Dining Room
Family Room
Kitchen

FIG. 92

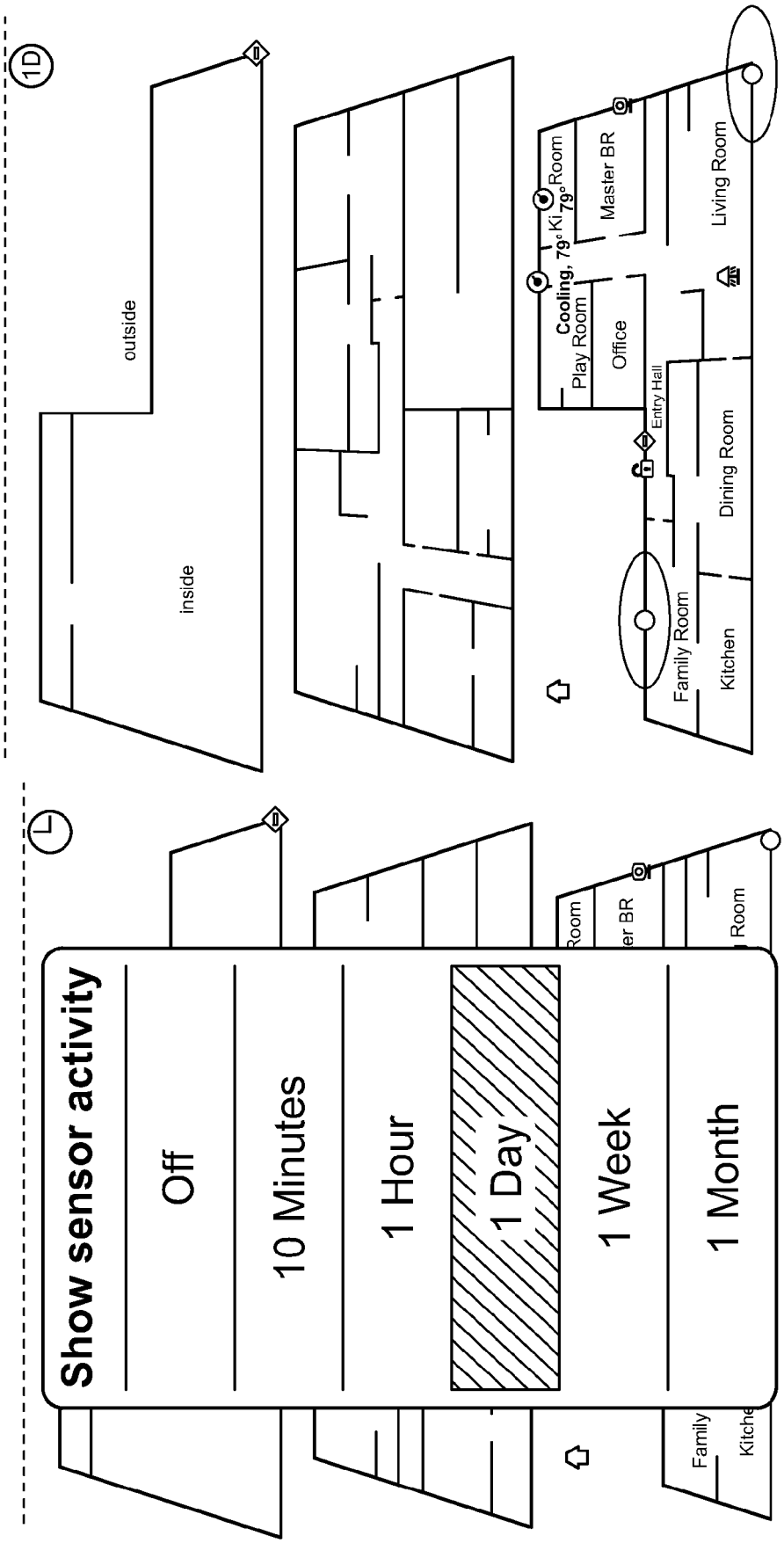

1D
outside
inside
Cooling, 79° Ki
79° Room
Play Room
Office
Master BR
Living Room
Entry Hall
Dining Room
Family Room
Kitchen
1L
Show sensor activity
Off
10 Minutes
1 Hour
1 Day
1 Week
1 Month

FIG. 93

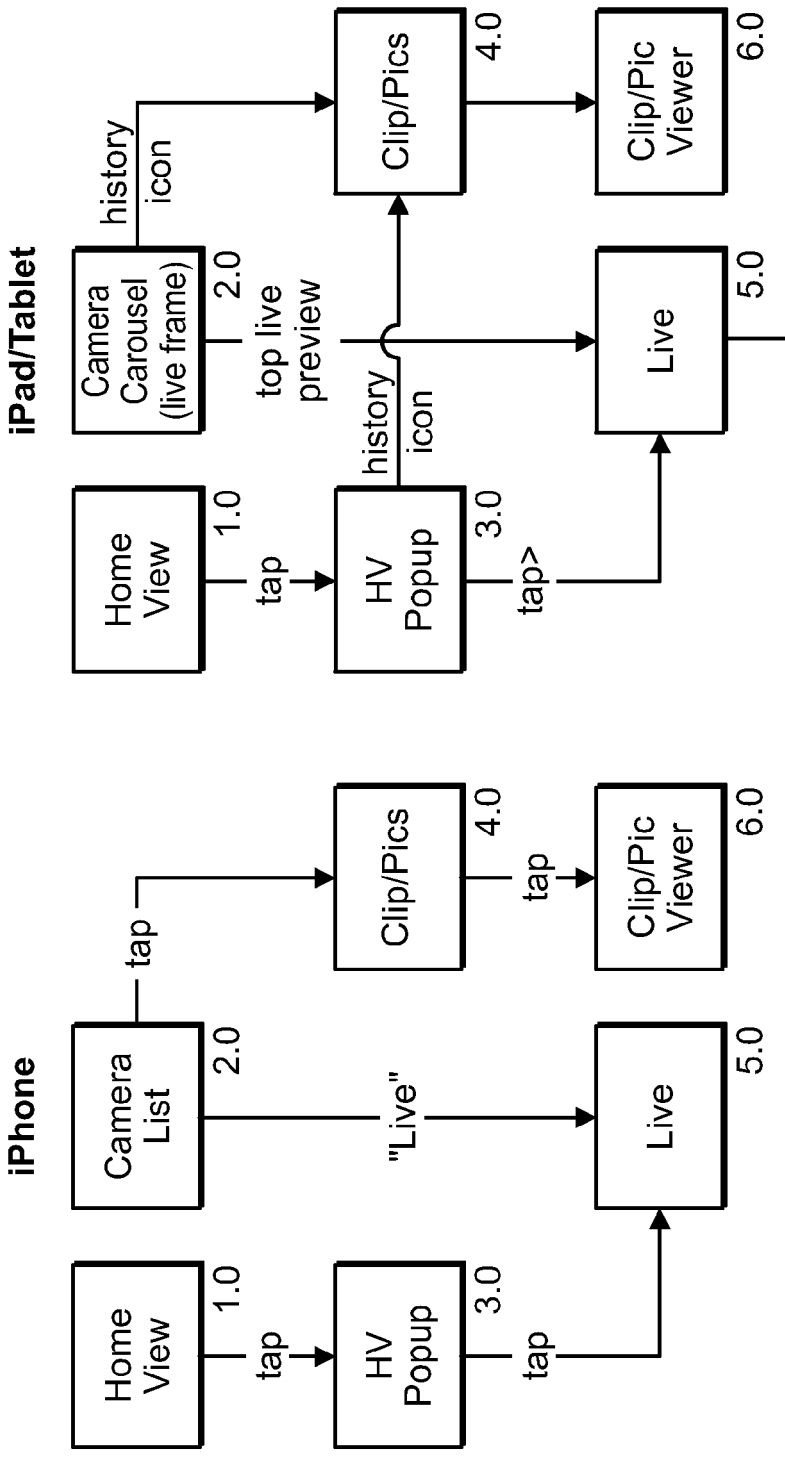


FIG. 94A

FIG. 94B

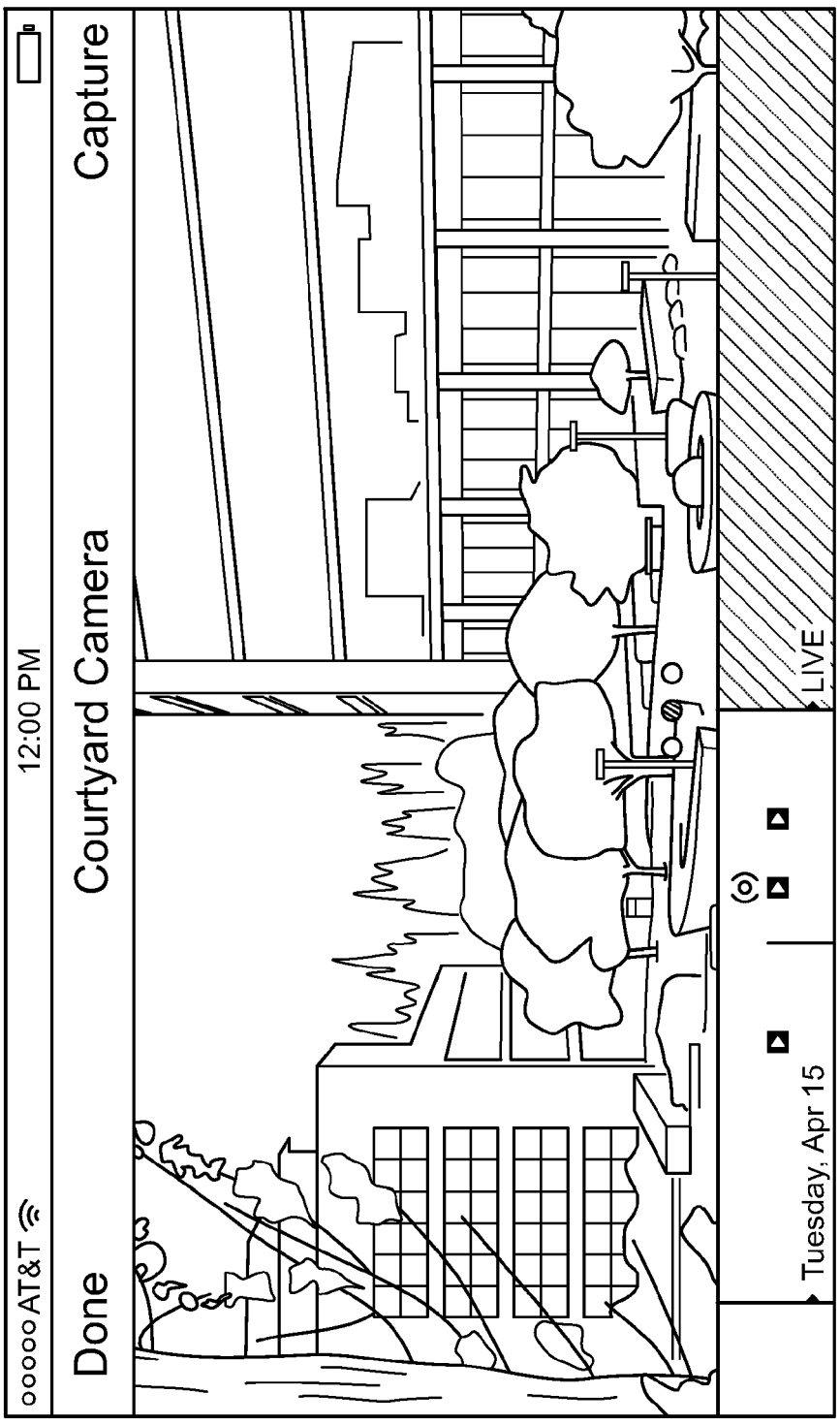

oooo AT&T
12:00 PM
Done
Courtyard Camera
Capture
LIVE
Tuesday, Apr 15

FIG. 95

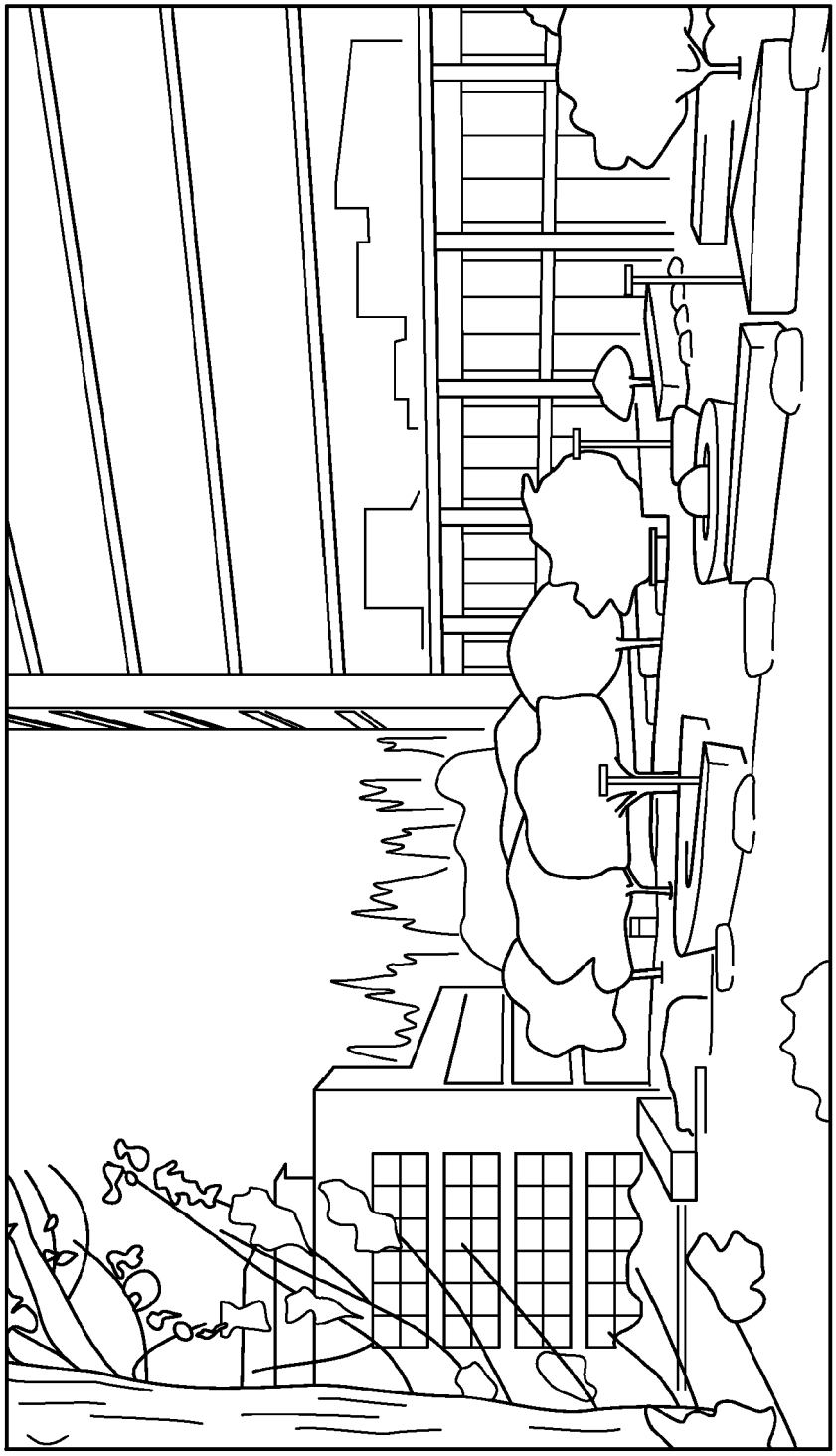


FIG. 96

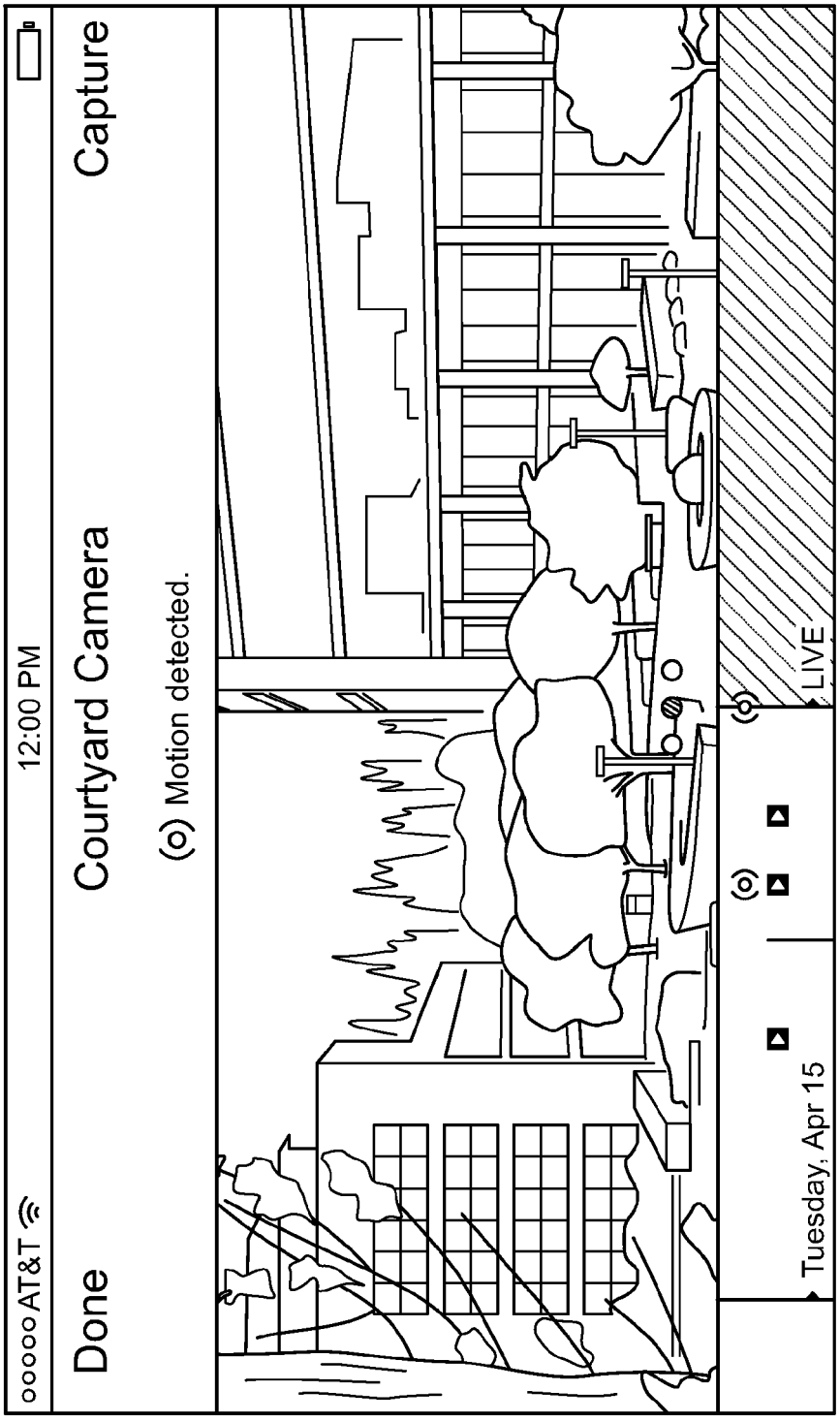

oooooAT&T
12:00 PM
Done
Courtyard Camera
Capture
(o) Motion detected.
LIVE
Tuesday, Apr 15

FIG. 97

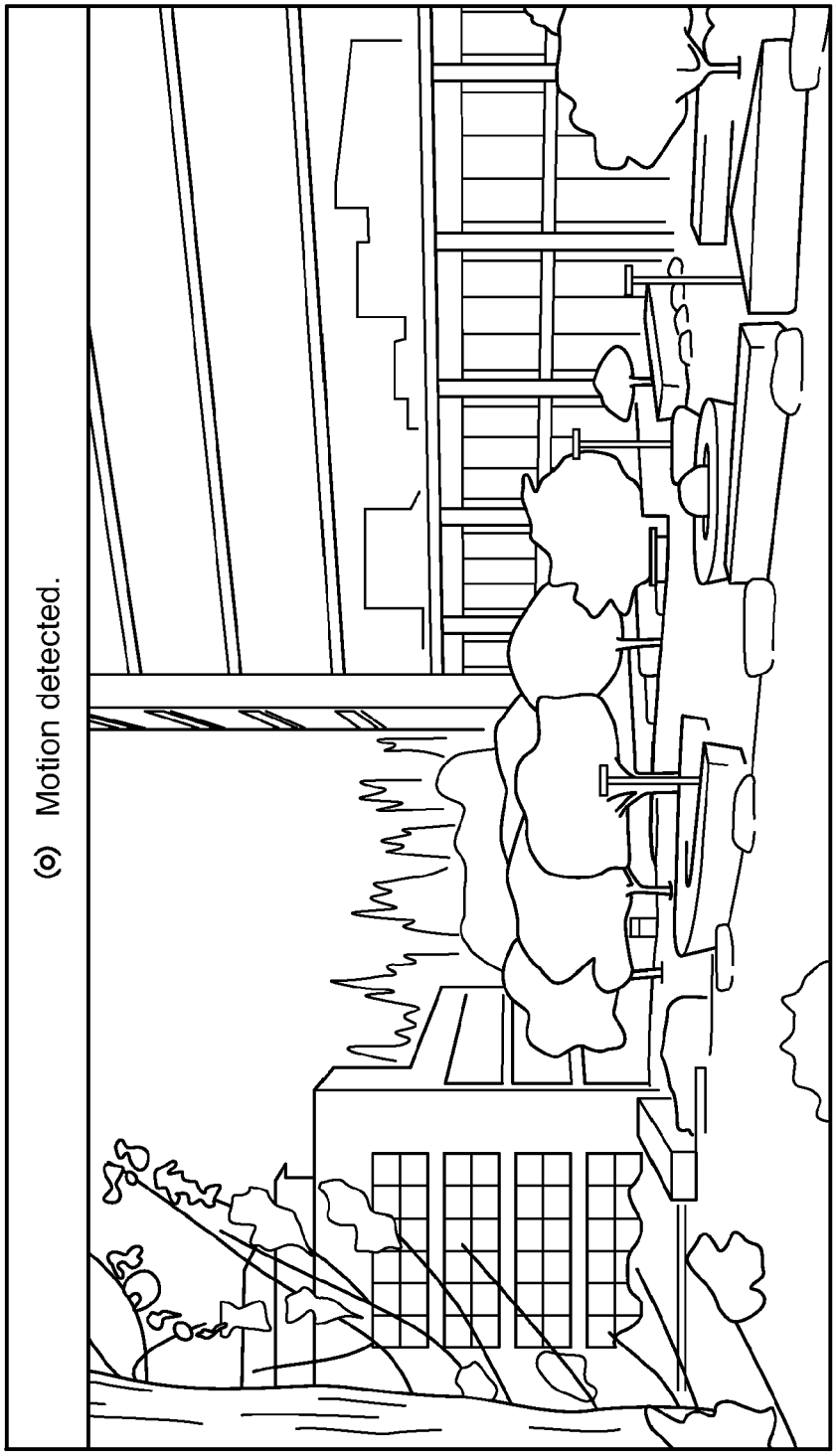


FIG. 98

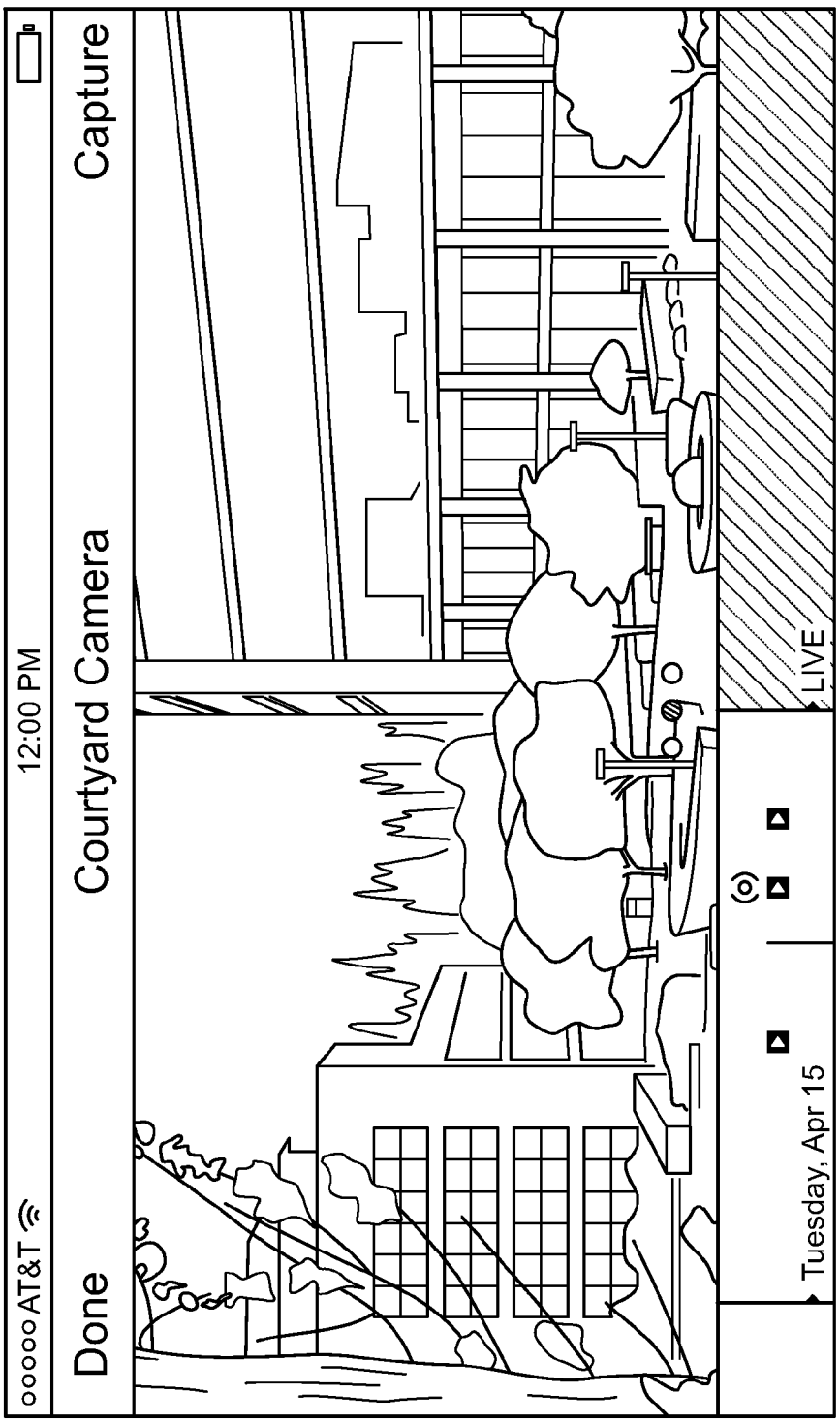

oooo AT&T
12:00 PM
Done
Courtyard Camera
Capture
LIVE
Tuesday, Apr 15

FIG. 99

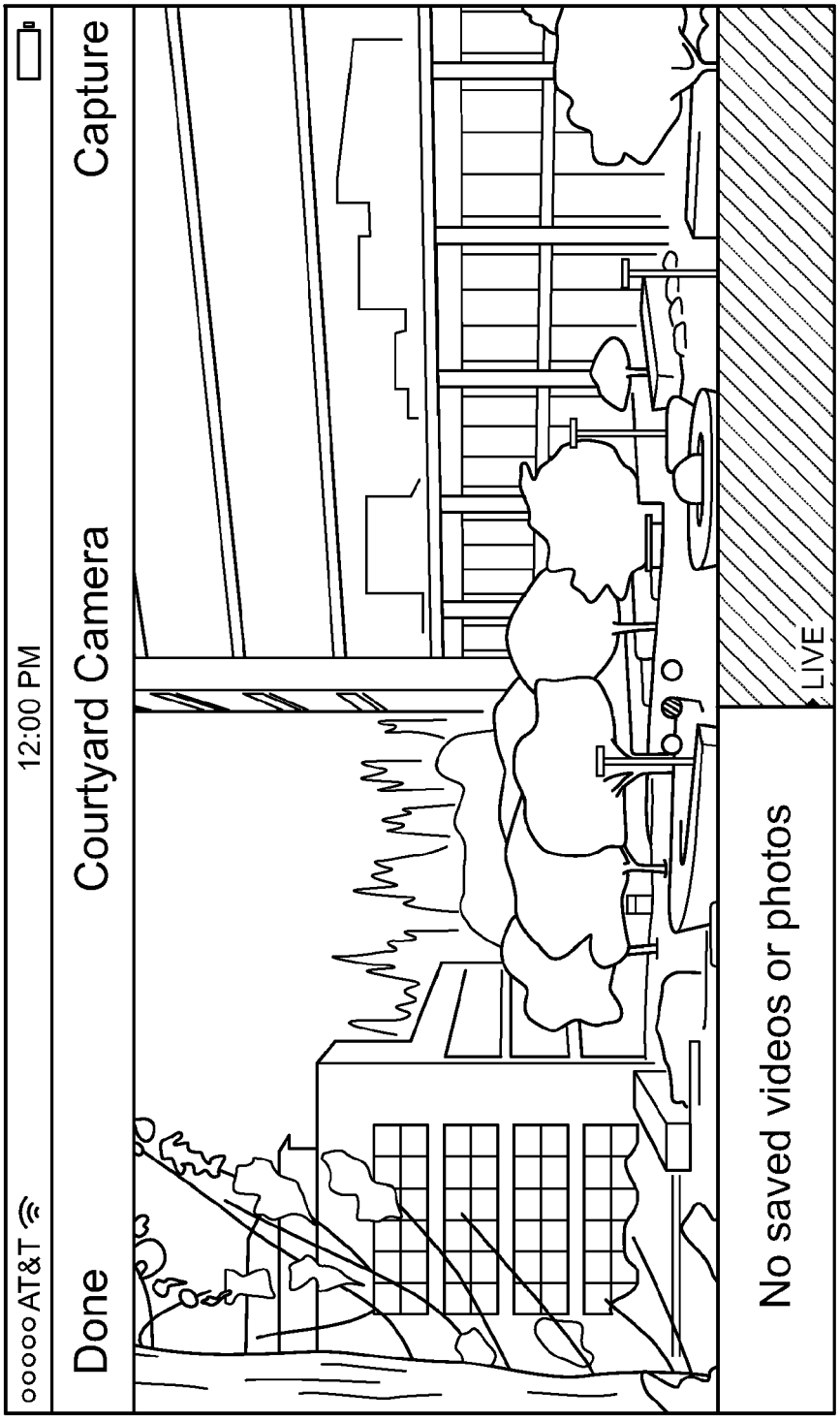

oooo AT&T
12:00 PM
Done
Courtyard Camera
Capture
LIVE
No saved videos or photos

FIG. 100

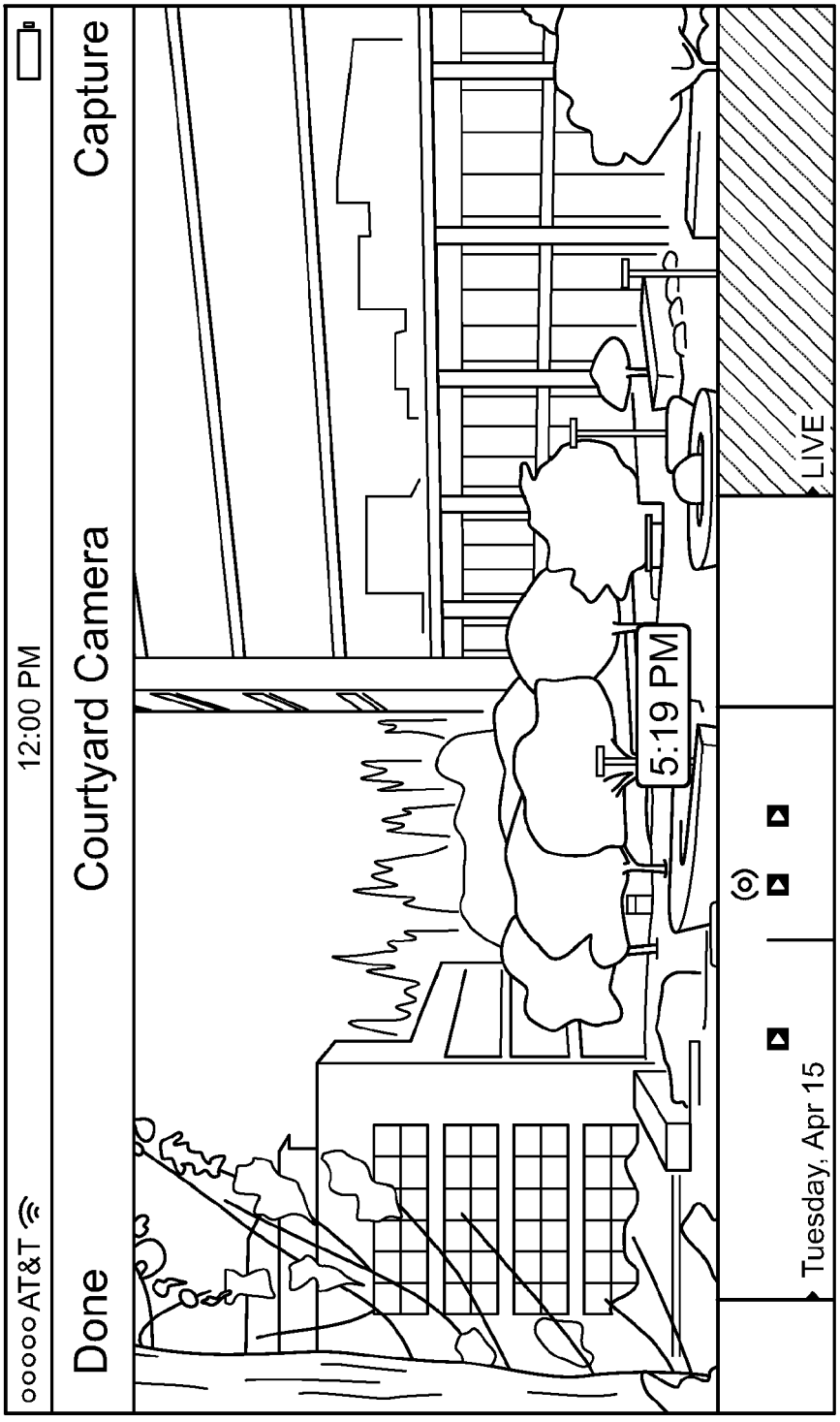

oooooo AT&T
12:00 PM
Done
Courtyard Camera
Capture
5:19 PM
LIVE
Tuesday, Apr 15

FIG. 101

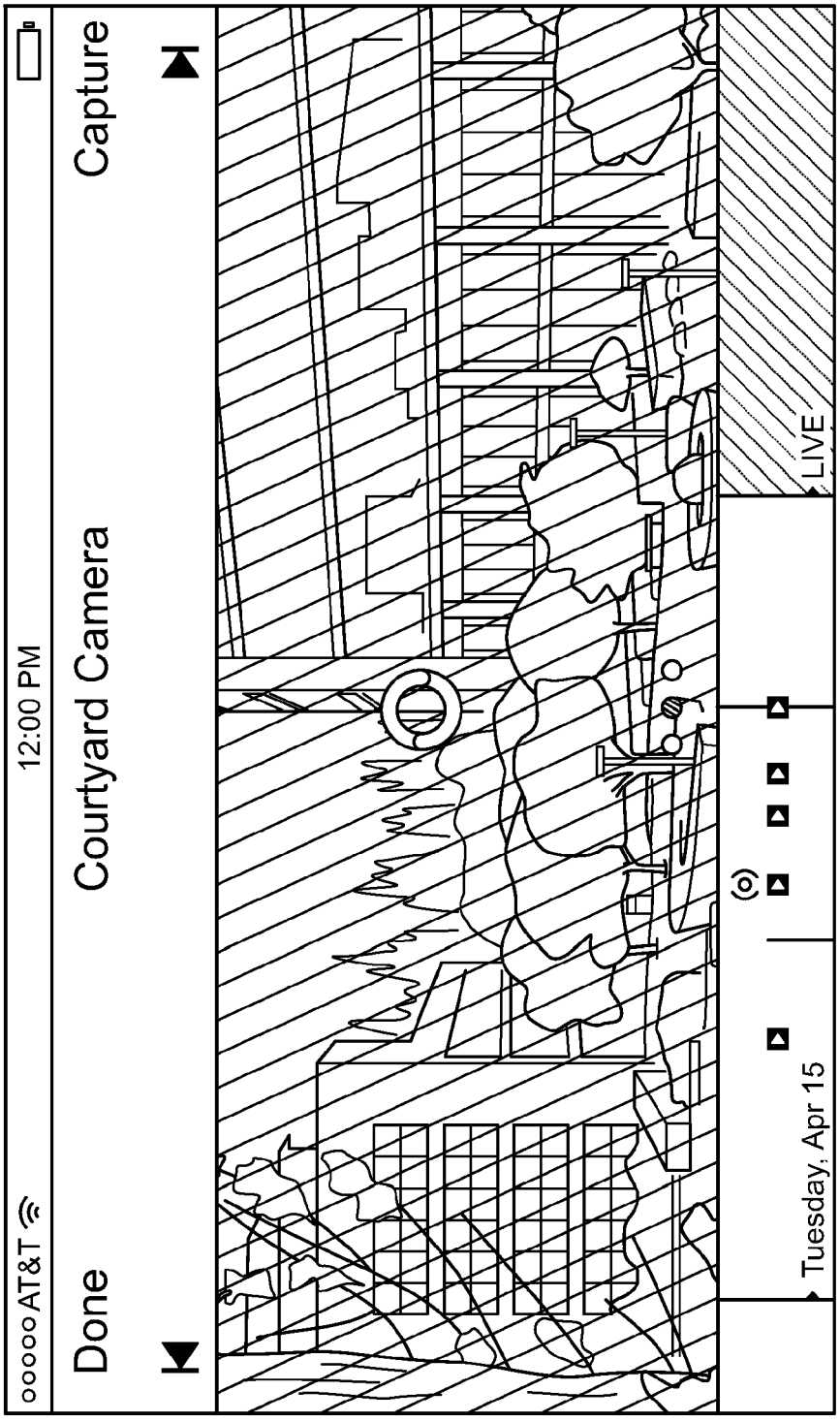

oooooAT&T
12:00 PM
Done
Courtyard Camera
Capture
LIVE
Tuesday, Apr 15

FIG. 102

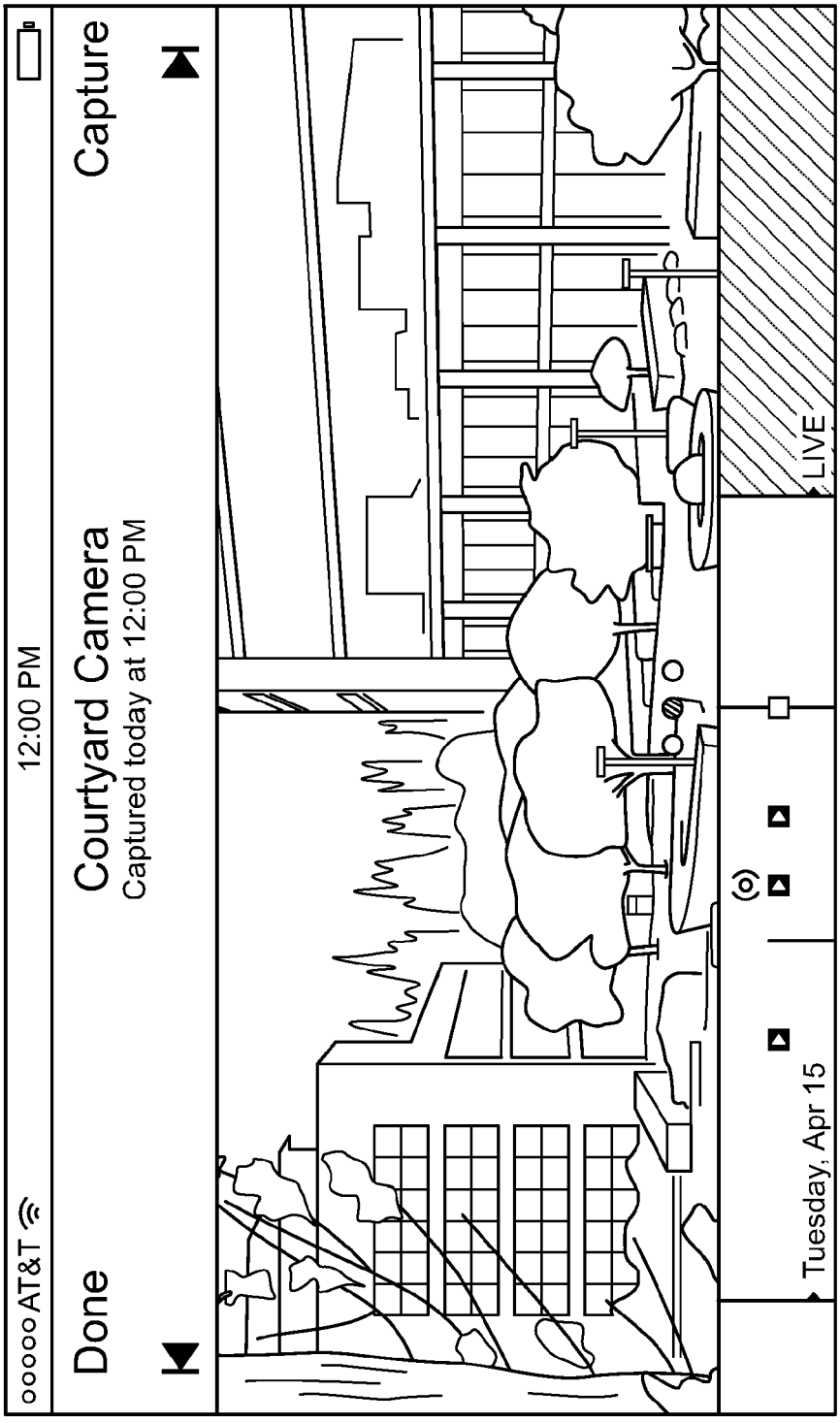

oooooAT&T
12:00 PM
Done
Courtyard Camera
Captured today at 12:00 PM
Capture
LIVE
Tuesday, Apr 15

FIG. 103

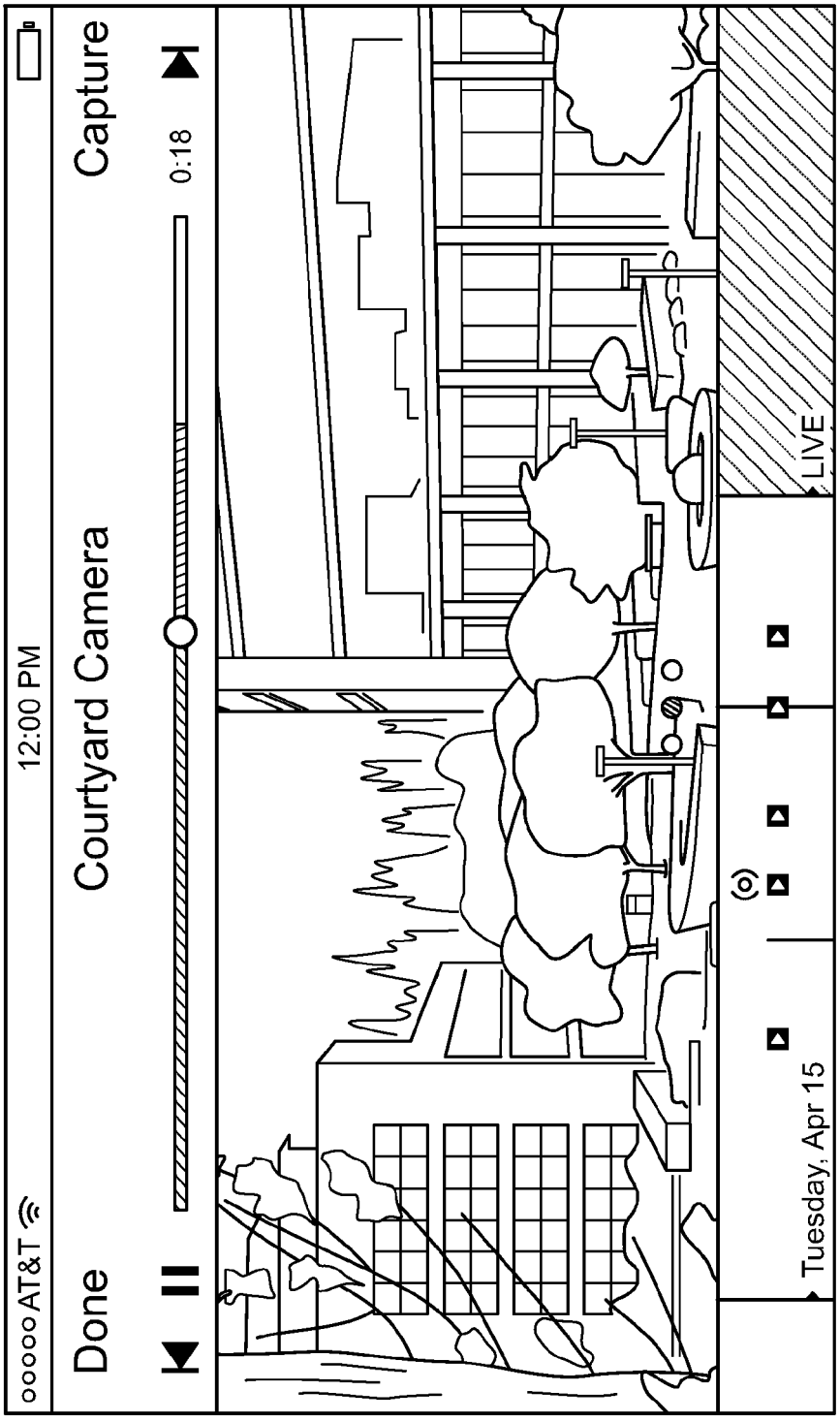

oooooAT&T
12:00 PM
Done
Courtyard Camera
Capture
0:18
LIVE
Tuesday, Apr 15

FIG. 104

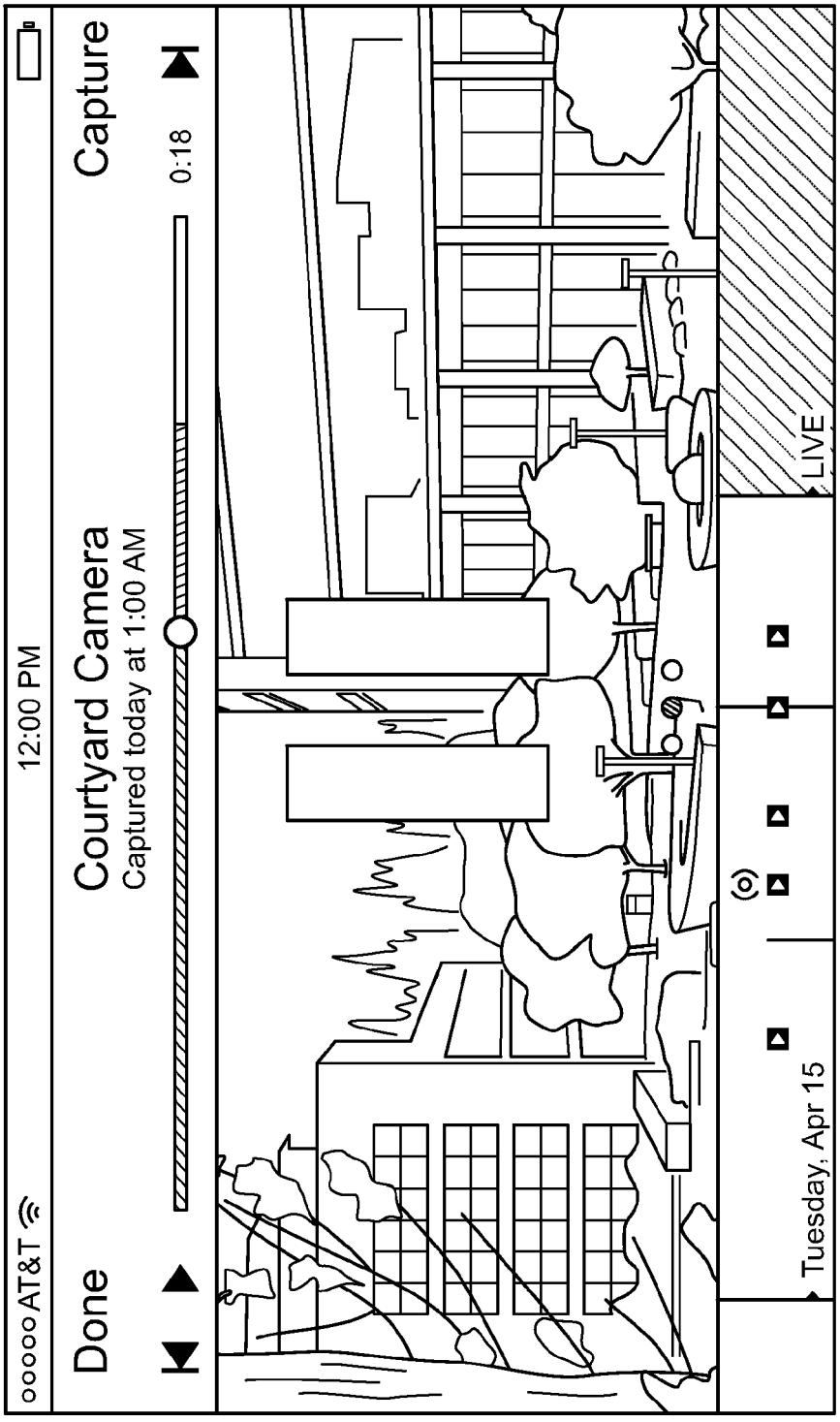

oooooo AT&T
12:00 PM
Done
Courtyard Camera
Captured today at 1:00 AM
Capture
0:18
LIVE
Tuesday, Apr 15

FIG. 105

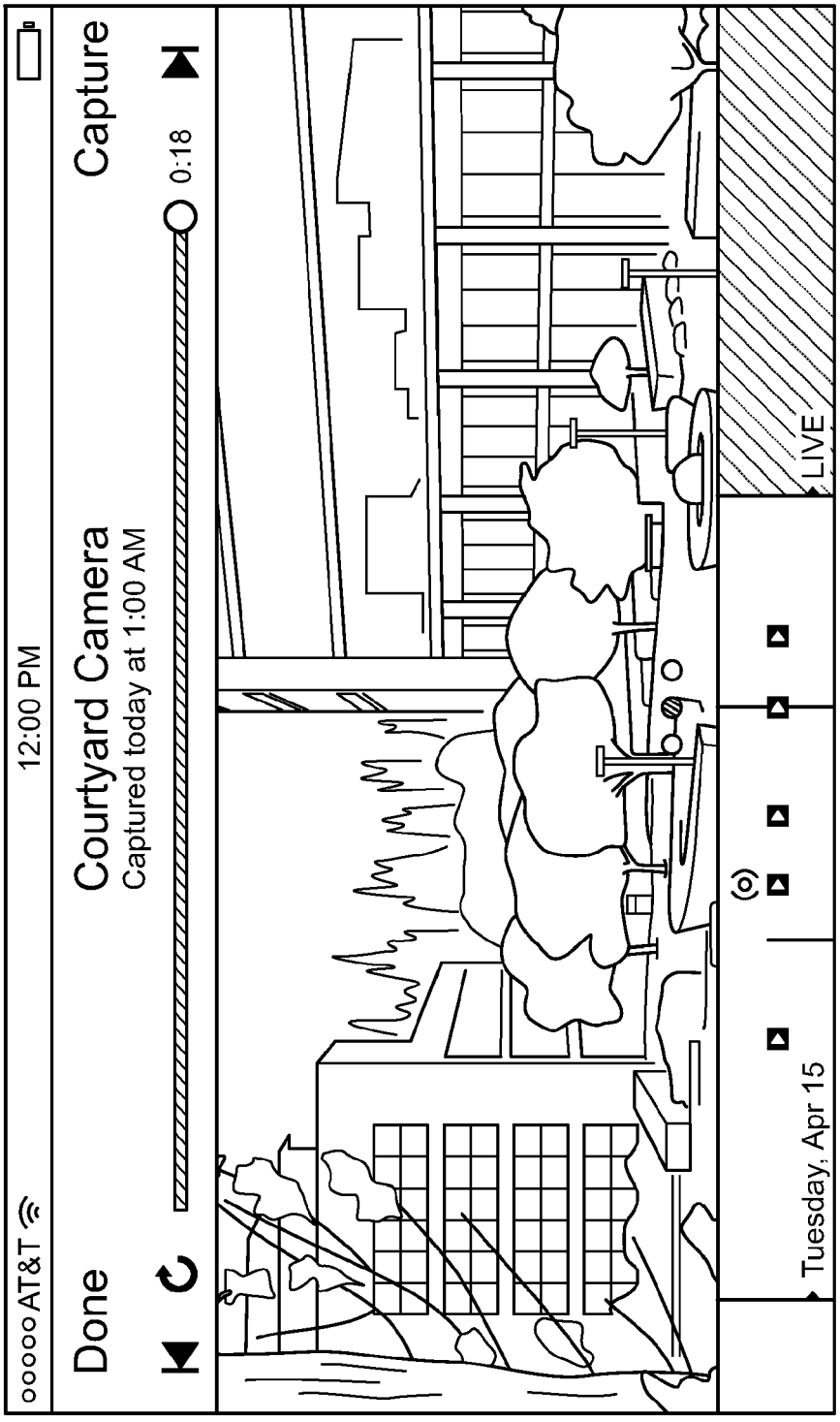

oooooAT&T
12:00 PM
Done
Courtyard Camera
Captured today at 1:00 AM
Capture
0:18
LIVE
Tuesday, Apr 15

FIG. 106

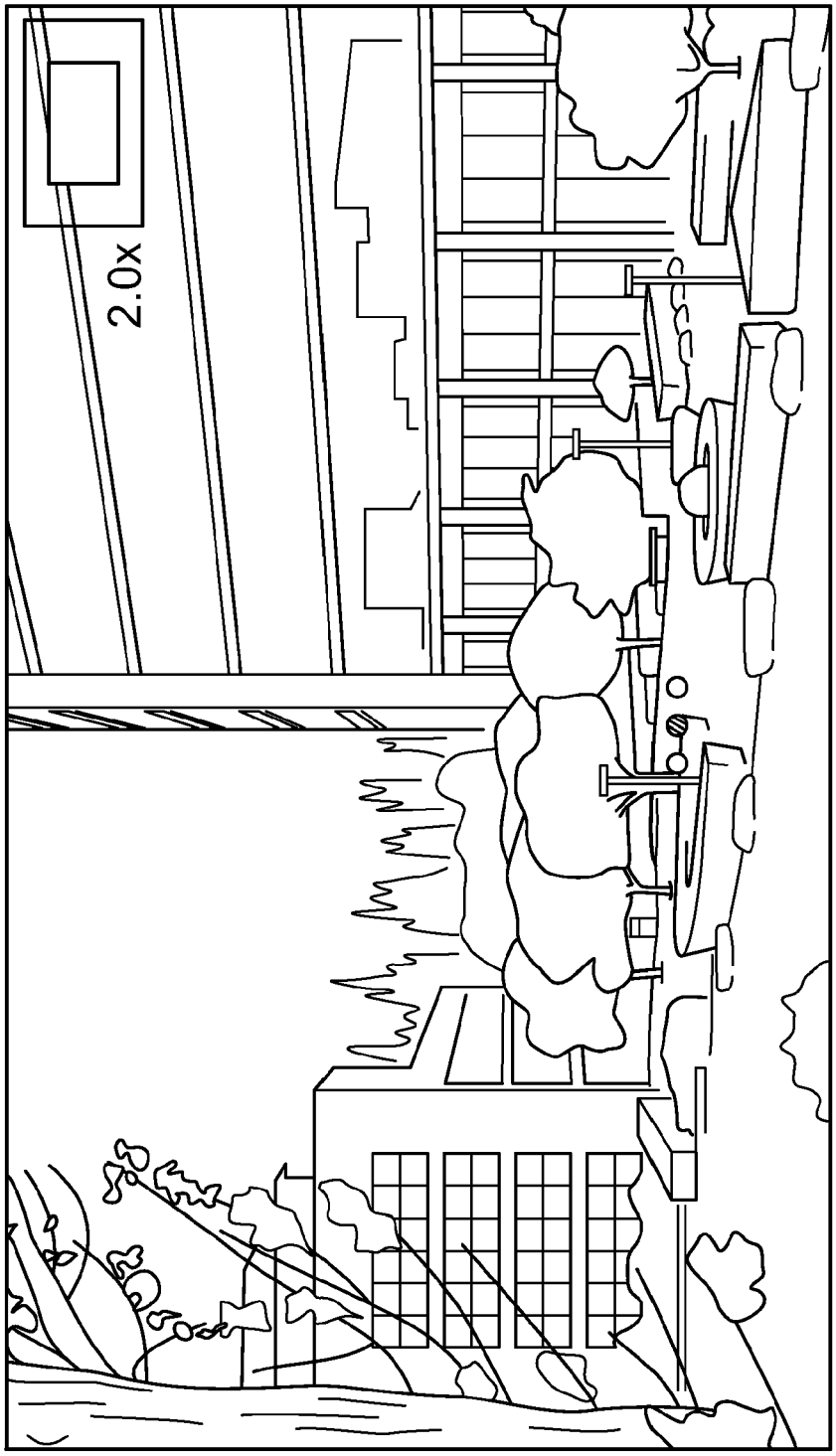


FIG. 107

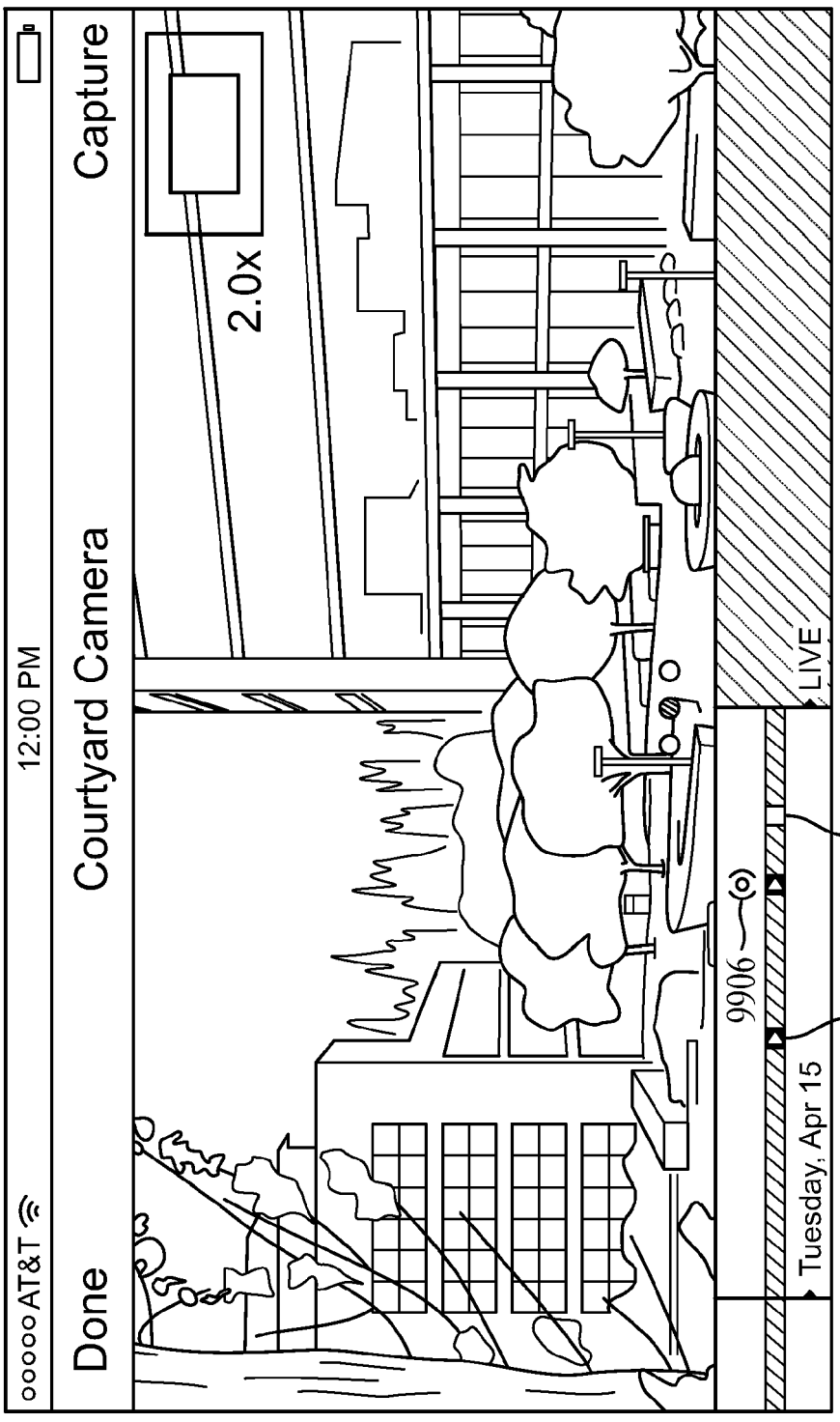

oooo AT&T
12:00 PM
Done
Courtyard Camera
Capture
2.0x
LIVE
Tuesday, Apr 15
9902
9904
9906

FIG. 108

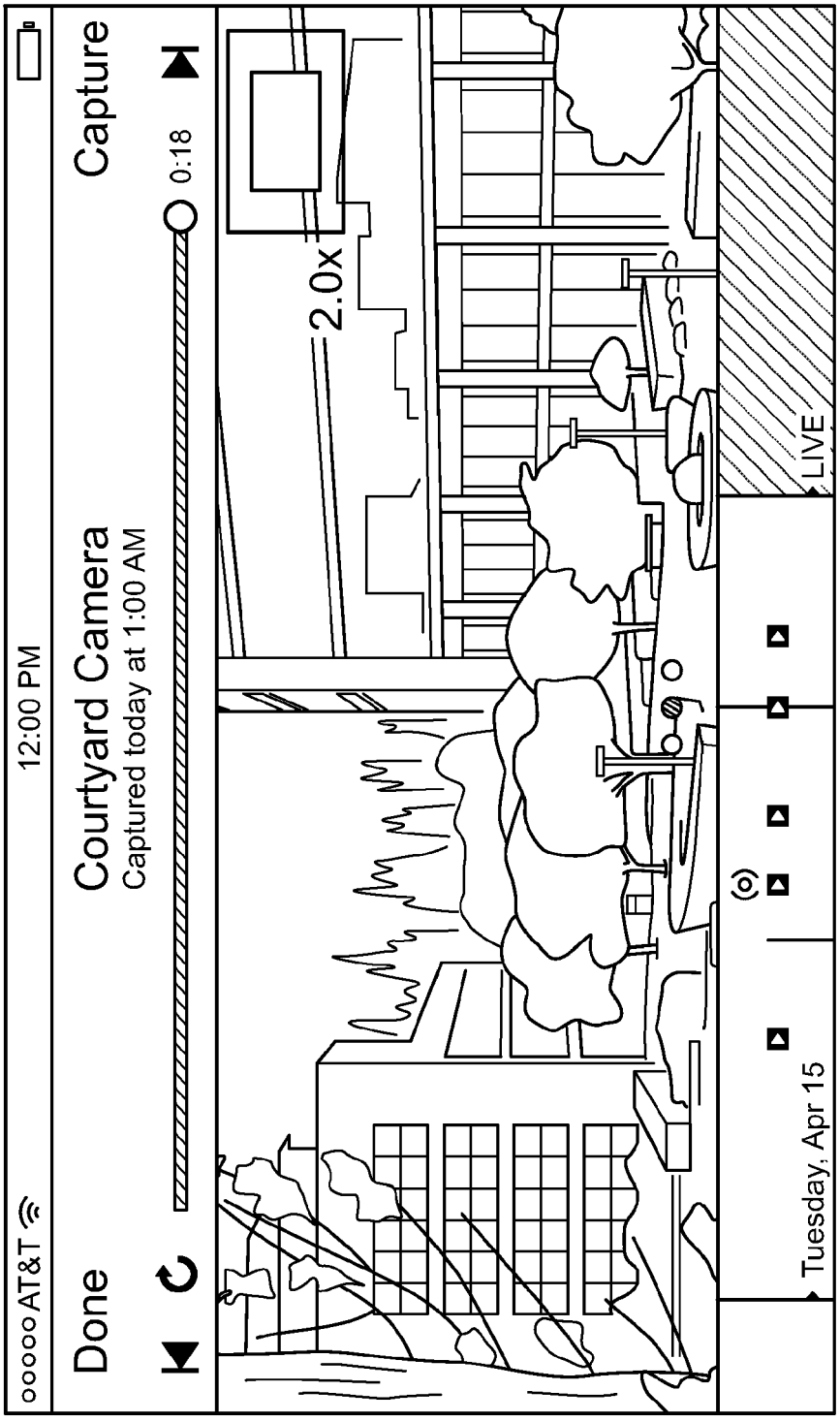

oooooAT&T
12:00 PM
Done
Courtyard Camera
Captured today at 1:00 AM
Capture
0:18
2.0x
LIVE
Tuesday, Apr 15

FIG. 109

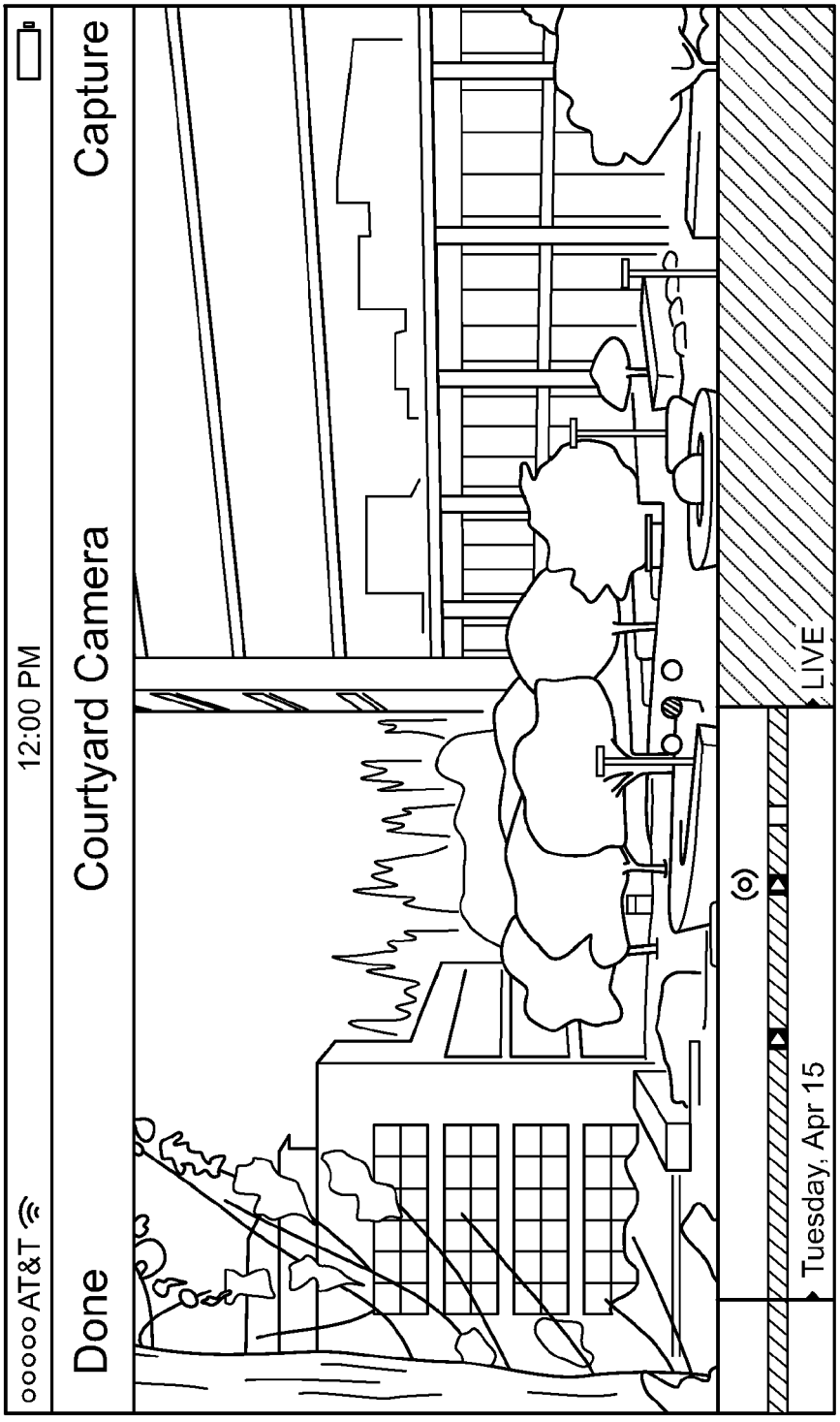

oooooAT&T
12:00 PM
Done
Courtyard Camera
Capture
LIVE
Tuesday, Apr 15

FIG. 110

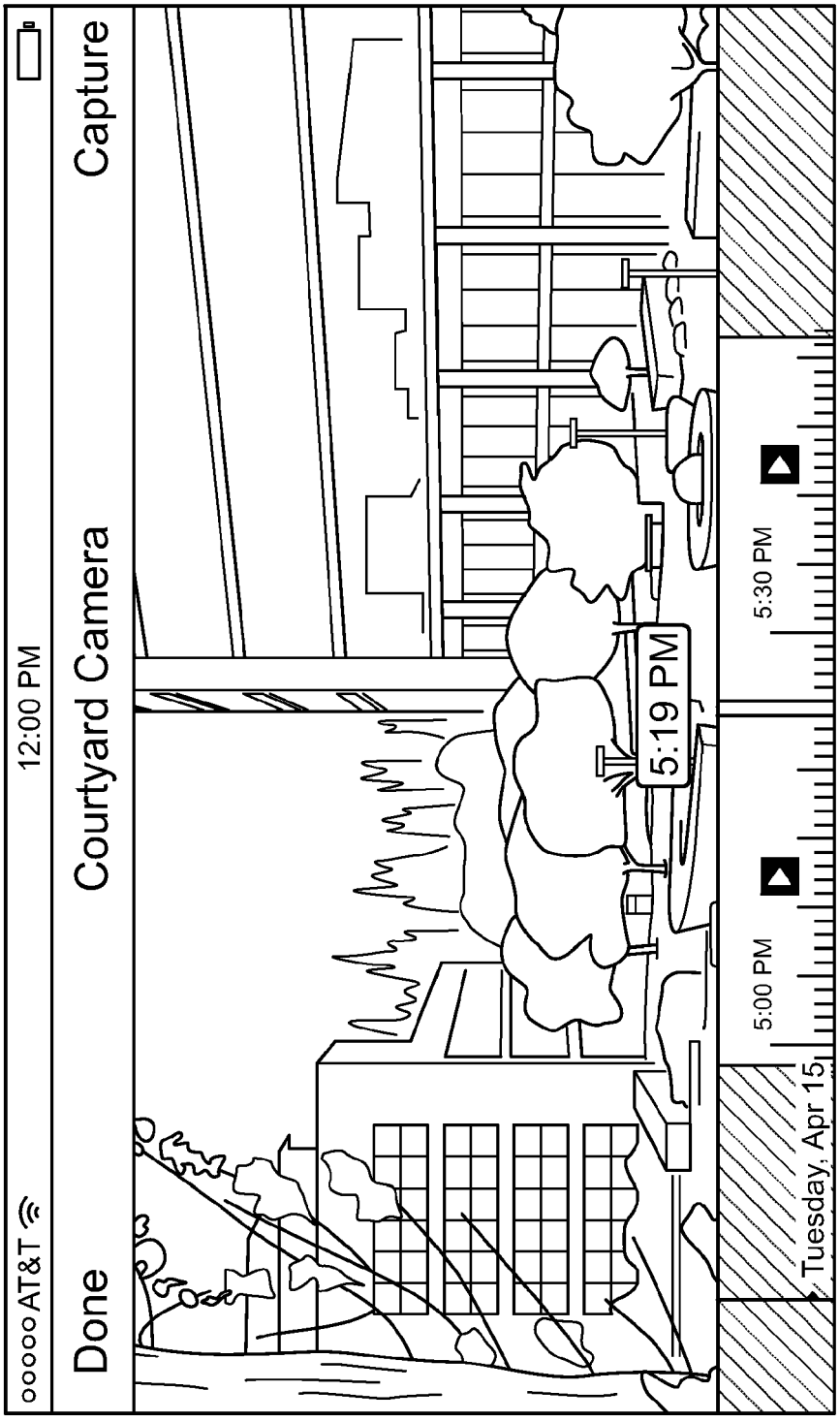

oooooo AT&T
12:00 PM
Done
Courtyard Camera
Capture
5:19 PM
5:30 PM
5:00 PM
Tuesday, Apr 15

FIG. 111

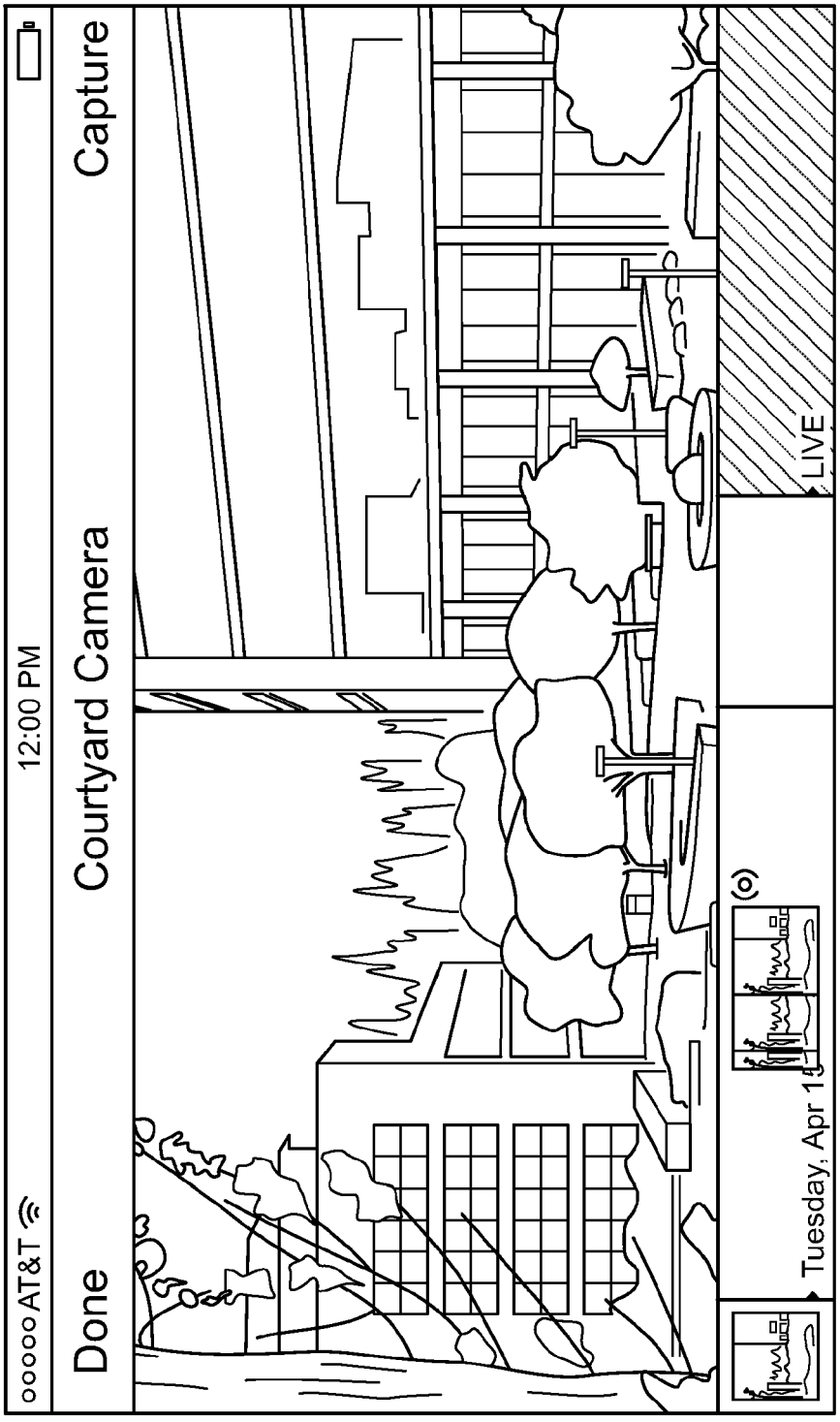

oooooo AT&T
12:00 PM
Done
Courtyard Camera
Capture
LIVE
Tuesday, Apr 1

FIG. 112

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- US 62205872 B **[0001]**
- US 62205922 B **[0002]**
- US 12189780 B **[0003]**
- US 13531757 B **[0004]**
- US 12197958 B **[0005]**
- US 13334998 B **[0006]**
- US 12539537 B **[0007]**
- US 14645808 B **[0008]**
- US 13104932 B **[0009]**
- US 13104936 B **[0010]**
- US 13929568 B **[0011]**
- US 14704045 B **[0012]**
- US 14704098 B **[0013]**
- US 14704127 B **[0014]**
- US 14628651 B **[0015]**
- US 13718851 B **[0016]**
- US 12972740 B **[0017]**
- US 13954553 B **[0018]**
- US 14943162 B **[0019]**
- US 15177915 B **[0020]**
- US 15177448 B **[0021]**
- US 15196281 B **[0022]**
- US 15198531 B **[0023]**
- US 15204662 B **[0024]**