(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 693 573**

(51) Int. CI.:

G08B 25/14 (2006.01)
G08B 25/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.10.2016 E 16192114 (3)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2018 EP 3154040**

(54) Título: **Sistema de control de intrusión inteligente que utiliza dispositivos portátiles y dispositivos BLE**

(30) Prioridad:

06.10.2015 US 201514875854

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.12.2018

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road P.O.Box 377
Morris Plains, NJ 07950, US

(72) Inventor/es:

BABU M, SATHEESH;
VEDIAPPAN, DHARMALINGAM y
KRISHNAN, VISWANATHAN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema de control de intrusión inteligente que utiliza dispositivos portátiles y dispositivos BLE

Campo

La presente solicitud se refiere a sistemas de seguridad y más en concreto a la activación y desactivación de tales sistemas.

Antecedentes

Se sabe que los sistemas protegen a personas y bienes dentro de áreas protegidas. Estos sistemas generalmente se basan en el uso de uno o más sensores que detectan amenazas dentro de las áreas.

Las amenazas a personas y bienes pueden tener cualquier origen. Por ejemplo, un incendio puede matar o herir a ocupantes que han quedado atrapados por un incendio en una casa. Del mismo modo, el monóxido de carbono de un incendio puede matar a las personas mientras duermen.

Alternativamente, un intruso no autorizado, tal como un ladrón, puede representar una amenaza para los bienes dentro del área. También se sabe que los intrusos lesionan o matan a personas que viven dentro del área.

En el caso de intrusos, se pueden colocar sensores en diferentes áreas en función de los usos respectivos de esas áreas. Por ejemplo, si hay personas presentes durante algunas partes de un día normal y no en otras ocasiones, los sensores se pueden colocar a lo largo de la periferia del espacio para brindar protección mientras el espacio esté ocupado, mientras que se pueden colocar sensores adicionales en el interior del espacio y utilizarse cuando el espacio no esté ocupado.

En la mayoría de los casos, los detectores de amenazas están conectados a un panel de control local. En caso de que se detecte una amenaza a través de uno de los sensores, el panel de control puede hacer sonar una alarma sonora local. El panel de control también puede enviar una señal a una estación de control central.

Si bien los sistemas de seguridad convencionales funcionan bien, a veces resulta difícil o incómodo activar y desactivar el sistema durante el desplazamiento a través de áreas con diferentes niveles de seguridad. Por consiguiente, existe la necesidad de mejores métodos y aparatos para activar y/o desactivar tales áreas.

El documento US2012019353(A1) describe sistemas y métodos para activar automáticamente sistemas de control, en los que se puede identificar uno o más parámetros asociados a la activación automática de un sistema de control. El uno o más parámetros pueden ser identificados por un algoritmo de aprendizaje basado en información histórica asociada al sistema de control. Se puede determinar si se han cumplido el uno o más parámetros. Si se determina que se han cumplido el uno o más parámetros, el sistema de control puede ser activado automáticamente. En algunas realizaciones, las operaciones anteriores pueden ser realizadas por un sistema que incluye uno o más ordenadores.

El documento US2014007264(A1) describe un subsistema de reacción a robos siempre disponible que comprende un lector de comunicaciones de campo cercano, una lógica de emparejamiento para identificar un dispositivo NFC como un dispositivo autorizado para activar y desactivar el sistema, una lógica de activación para activar el sistema una vez recibido un comando de activación y una lógica de desactivación para desactivar el sistema una vez recibido un comando de desactivación, en el que el comando de activación y el comando de desactivación pueden utilizar el dispositivo NFC, y en el que el lector NFC es accionado en una pluralidad de estados de accionamiento, permitiendo la activación y la desactivación de la plataforma en la pluralidad de estados de accionamiento.

Sumario de la invención

La presente invención proporciona un aparato como el que se reivindica en los dibujos que se acompañan.

Breve descripción de los dibujos

La figura 1 ilustra un diagrama de bloques de un sistema domótico de acuerdo con la presente invención.

Descripción detallada

Si bien las realizaciones que se describen pueden adoptar muchas formas diferentes, las realizaciones específicas de las mismas se muestran en los dibujos y se describen aquí en detalle en el entendimiento de que la presente descripción debe considerarse como un ejemplo de los principios de esta, así como el mejor modo de poner en práctica la misma, y no pretende limitar la memoria descriptiva o las reivindicaciones a la realización específica ilustrada.

La figura 1 es un diagrama de bloques de un sistema de seguridad 10 mostrado en general de acuerdo con una realización ilustrada. Dentro del sistema se incluye una serie de sensores 12, 14 que detectan amenazas dentro de

un área geográfica protegida 16. El área protegida puede dividirse en varias zonas 18, 20, 22, 24, cada una con un nivel de seguridad diferente.

Los sensores pueden incorporarse en cualquiera de varias formas diferentes. Por ejemplo, al menos algunos de los sensores pueden ser interruptores de seguridad conectados a puertas y/o ventanas proporcionando entrada y salida del área protegida o desplazamiento entre las zonas. Otros de los sensores pueden ser sensores infrarrojos pasivos (PIR) colocados en el interior del área o en cada una de sus zonas para detectar intrusos que hayan podido eludir los sensores ubicados a lo largo de la periferia. Aún otros de los sensores pueden ser cámaras de televisión de circuito cerrado (CCTV) con capacidades de detección de movimiento para detectar intrusos.

Los sensores pueden ser controlados mediante un panel de control ubicado dentro de una de las zonas (como se muestra en la figura 1) o ubicado de forma remota. Tras la activación de uno de los sensores, el panel de control puede enviar un mensaje de alarma a una estación de control central 28. La estación de control central puede responder llamando a la policía.

El sistema de seguridad puede ser controlado mediante una o más interfaces de usuario 30 ubicadas cerca de las entradas al área protegida y/o a cada una de sus zonas. En este sentido, un usuario humano autorizado puede introducir un número de identificación personal (PIN) y activar una tecla de función a través de un teclado 32 para activar o desactivar el sistema de seguridad o una parte del sistema de seguridad dentro de cualquiera de las zonas. La información de estado con respecto a cualquier instrucción introducida se puede mostrar en una pantalla 34.

Por ejemplo, un usuario puede introducir su PIN y una instrucción de desactivación a través de una interfaz de usuario para entrar en el área protegida. Una vez dentro, el usuario puede introducir un comando de permanencia de activación para reactivar los sensores a lo largo del perímetro y para proporcionar detección de intrusión mientras el usuario está dentro del área protegida.

De manera similar, mientras el usuario está dentro del área protegida con los sensores perimetrales activados, puede elegir moverse desde una zona que tenga un nivel de seguridad más bajo a una zona que tenga un nivel de seguridad más alto. En este caso, se le puede solicitar al usuario que vuelva a introducir su PIN y un comando de desactivación para entrar en el área con el nivel de seguridad más alto. Al abandonar el área con el nivel de seguridad más alto y volver a entrar en el área con el nivel de seguridad más bajo, se le puede solicitar al usuario que vuelva a activar la parte del sistema de seguridad en la zona con el nivel de seguridad más alto.

Incluidos dentro del panel de control, los sensores y las interfaces de usuario pueden ser circuitos de control que cumplen la funcionalidad descrita en este documento. Los circuitos de control pueden incluir uno o más aparatos procesadores (procesadores) 36, 38 que funcionan bajo el control de uno o más programas informáticos 40, 42 cargados desde un medio legible por ordenador no transitorio (memoria) 44. Tal como se usa en este documento, la referencia a una etapa realizada por un programa informático también es una referencia al procesador que ejecutó esa etapa.

En la realización ilustrada, el sistema de seguridad (o partes de este) puede desactivarse y/o activarse automáticamente a través de un dispositivo inalámbrico portátil correspondiente 46, 48 llevado por cada uno de una pluralidad de usuarios humanos autorizados. A este respecto, cada uno de los dispositivos portátiles puede incluir un transceptor de radiofrecuencia 50 que transmite una señal de baja potencia (por ejemplo, una señal Bluetooth de baja potencia) que contiene información de identificación. Un receptor o transceptor de radiofrecuencia 52 asociado a cada zona (por ejemplo, ubicado dentro de la interfaz de usuario de la zona) puede detectar al usuario y desactivar automáticamente la zona a medida que el usuario se acerca y volver a activar la parte cuando el usuario abandona el área de la zona.

Los dispositivos portátiles pueden ser cualquier dispositivo (por ejemplo, un teléfono inteligente) con capacidad Bluetooth. Un programa de solicitud de acceso ejecutado en un procesador dentro del dispositivo portátil puede transmitir una solicitud de acceso a la interfaz de usuario cuando el usuario se acerca a una entrada a la zona.

Dentro de la interfaz de usuario, un procesador de acceso correspondiente puede transmitir periódicamente una señalización en favor de los dispositivos portátiles que estén dentro del área. La señalización puede incluir información que identifique la señalización como procedente del sistema de seguridad. El dispositivo portátil puede detectar la señalización, autenticar la fuente de la señalización y, en respuesta, transmitir una solicitud de acceso. La solicitud de acceso puede incluir información de identificación del usuario autorizado.

El procesador de acceso dentro de la interfaz de usuario puede detectar la solicitud de acceso y procesarla en consecuencia. Por ejemplo, el procesador o transceptor puede determinar una distancia que separa la interfaz de usuario y el dispositivo portátil a través de un indicador de intensidad de señal (por ejemplo, indicación de intensidad de señal recibida (RSSI), un índice de error de bits (BER), etc.). El procesador también puede comparar el indicador de intensidad de señal con un valor umbral para detectar que el usuario llega a una distancia predeterminada del borde de la zona.

El procesador de acceso o un procesador asociado dentro del panel de control también puede autenticar la información de identificación del usuario. Al autenticar la solicitud de acceso como procedente de un usuario

autorizado, el procesador de acceso puede desactivar la parte del sistema de seguridad asociada a la interfaz de usuario. El procesador también puede activar una cerradura eléctrica que proporciona acceso físico al usuario a la zona.

Además de la distancia, un procesador de ubicación del panel de control puede determinar una ubicación del dispositivo portátil. Por ejemplo, al transmitirse una solicitud de acceso, 2 o más interfaces de usuario pueden detectar una distancia relativa del dispositivo portátil desde cada interfaz de usuario. Cuando la solicitud es detectada por tres o más interfaces de usuario, se puede determinar la ubicación geográfica del usuario. Cuando la solicitud es detectada por 2 o más interfaces de usuario, entonces se puede determinar la dirección de desplazamiento del usuario. Al usar la ubicación, el procesador de acceso puede volver a activar la parte del sistema de seguridad a medida que el usuario abandona el área de la zona.

Otro procesador dentro del panel de control también puede determinar una velocidad relativa de desplazamiento del usuario. Esto se puede lograr procesando la señal detectada por una sola interfaz de usuario o determinando un cambio en la posición relativa del usuario dentro del área protegida. En este sentido, la velocidad se puede usar para anticipar el tiempo de llegada del usuario a la ubicación de una zona diferente y desactivar o activar la zona a medida que el usuario llega a un borde de la zona. A este respecto, un procesador puede ajustar el umbral de distancia para activar o desactivar el sistema dependiendo de la velocidad del usuario.

El dispositivo portátil también puede incluir uno o más sensores 54 que detecten un parámetro fisiológico del usuario (por ejemplo, frecuencia cardíaca, presión arterial, respiración, etc.). A este respecto, un procesador de salud del dispositivo portátil puede procesar los parámetros fisiológicos del usuario para determinar un estado de salud del usuario.

El estado de salud determinado del usuario puede incluirse dentro de la solicitud de acceso y usarse para activar y desactivar el sistema según sea necesario. Por ejemplo, al detectar una condición de salud que requiera una ambulancia, un procesador puede desactivar una o más zonas o el sistema de seguridad completo.

Al utilizar una o más de la distancia, la ubicación y la salud de los usuarios, un procesador de control de sistema puede generar una lista de zonas para activar y/o desactivar. En este sentido, la zona relativamente más cercana puede ser la primera de la lista para activar o desactivar. Si el usuario se está alejando de la zona más cercana, al llegar a la distancia umbral, la zona se activa. Si el usuario se está moviendo hacia la zona, entonces la zona se desactiva cuando el usuario sobrepase la distancia umbral.

De manera similar, la salud y la velocidad de desplazamiento del usuario pueden usarse para ajustar la lista y los valores umbral asociados a la lista. Si la salud del usuario se ve afectada, la lista puede incluir cada zona que separa al usuario de una entrada utilizada por los paramédicos. En este caso, el umbral se puede establecer para desactivar cada zona a través de la cual se van a desplazar los paramédicos.

De manera similar, si un parámetro de salud medido indicara un problema de salud inminente y el usuario se desplazará en una dirección particular a una velocidad relativamente rápida, entonces la lista se generaría según la velocidad, la dirección de desplazamiento y la gravedad del problema de salud.

En general, el sistema de intrusión actualmente disponible requiere intervención manual para activar/desactivar zonas en una instalación. Incluso aunque un usuario validado esté dentro de una zona, debe desactivar manualmente el sistema. El usuario debe abrir una aplicación en su teléfono inteligente o ir físicamente al teclado del sistema para cambiar el control. No existe un mecanismo inteligente o basado en la ubicación para controlar de forma remota las zonas.

Además, los sensores de todo un edificio se activarán si el sistema se activa y viceversa. El control granular para activar y desactivar las zonas/divisiones no está disponible. Este problema se puede aplicar para la gestión de energía y temperatura también en el edificio.

En la solución que se representa en la figura 1, los dispositivos portátiles basados en BLE/RF de corto alcance se utilizan para identificar la distancia entre el operario y el primer componente/ubicación accesible de sistema de un usuario o un guarda de seguridad de las instalaciones. Cuando el operario/usuario entra en un área particular dentro de los límites de las zonas (más cercanas) en el área, se puede desactivar la misma. Estos límites/factor de distancia permiten al sistema identificar las zonas potenciales que se incluirán en una lista de zonas para activar/desactivar. Estos límites pueden variar dependiendo de la situación.

A un operario (usuario) no se le permite desactivar el sistema si no está en los límites de la zona en particular que está tratando de desactivar. Cuando un operario se desplaza de una zona a otra, las nuevas zonas dentro de los límites del operario se desactivarán automáticamente y la zona de la que vino el operario se activará automáticamente.

Esta solución funciona en 3 etapas. En primer lugar, la ubicación del operario/usuario se identifica dentro de las instalaciones. En segundo lugar, el sistema encuentra las zonas adecuadas en función de la ubicación identificada. En tercer lugar, el sistema envía el comando activar/desactivar a las zonas según la ubicación del operario.

Cuando un usuario entra en las instalaciones, los usuarios de los dispositivos portátiles comienzan a comunicarse con el sistema de intrusión utilizando transpondedores BLE/RF. En función de la intensidad de señal, se calcula una distancia precisa entre la Etiqueta que lleva el usuario y el transpondedor del sistema de seguridad. Esta distancia ayuda al controlador maestro a decidir si debe activarse o desactivarse una sola zona o varias zonas. La información procedente de BLE/Portátil también se utilizará para autenticar al usuario a fin de garantizar que sea realmente un usuario válido que tenga el privilegio y la autoridad para activar/desactivar el sistema.

El sistema identifica las zonas adecuadas en función de la ubicación del usuario. Esta etapa de funcionamiento genera una lista de zonas para ser activadas/desactivadas durante el movimiento del usuario. Los criterios para generar la lista pueden basarse en uno o más criterios y pueden combinarse para su efectividad. La lista de zonas seleccionadas clasifica el estado actual del sistema. Por ejemplo, en una situación de emergencia, la lista de zonas incluirá todas las zonas para acelerar el movimiento de emergencia de los ocupantes. Otros casos basados en la velocidad del movimiento de personas combinado con factores de salud del usuario permiten que el sistema forme la lista de zonas de manera que las zonas en las rutas se desactiven para operaciones más rápidas.

La preparación de la lista de zonas puede ocurrir durante cualquiera de los eventos que se describen a continuación. Por ejemplo, un aparato (dispositivo portátil) puede comunicar datos de uno o más monitores de salud en forma de alerta/notificación. En caso de que el aparato comunique cualquier señal de salud alta o baja, el sistema activará el sistema de intrusión para generar la lista de zonas desactivadas de forma que el usuario pueda moverse fácilmente hacia una salida.

El sistema permite un movimiento más rápido del Usuario entre zonas. Dentro de las instalaciones, si el usuario se mueve relativamente más rápido que una velocidad de movimiento normal, entonces el sistema generará la lista de zonas activadas/desactivadas de mayor radio para adaptarse a la velocidad del usuario.

El sistema puede adaptarse al número de personas en una sola zona. Dentro de las instalaciones, si un gran número de usuarios se reúne en una sola zona, el sistema utilizará sus alertas/notificaciones de monitores de salud como fuentes de información para evaluar la situación, si existe alguna anomalía, se determinará un mayor número de zonas dentro de un radio mayor de la ubicación actual.

El sistema también puede adaptarse a situaciones de activación/desactivación basadas en el comportamiento/amenaza de usuario. En este caso, el sistema añade las alertas/notificaciones de monitor de salud de todos los usuarios en las instalaciones para predecir el estado/amenaza actual en las instalaciones y generar una lista de zonas para desactivar/activar a fin de permitir una evacuación más rápida.

El sistema también puede detectar intrusos que hacen mal uso de los procedimientos de entrada establecidos. Por ejemplo, si un intruso sigue de cerca a cualquier usuario legítimo para entrar con el mismo, entonces el intruso no puede permanecer oculto en las instalaciones porque solo las zonas asociadas al usuario legítimo se desactivarán con el movimiento del usuario legítimo.

El sistema de la figura 1 tiene una serie de características novedosas. Con respecto a factores humanos, el sistema enriquece la experiencia del usuario ya que la activación/desactivación ocurre sin una clave manual en proceso. Además, todas las zonas se mantienen siempre en estado activado, excepto las zonas en las que permanecen los usuarios. El sistema proporciona una forma inteligente para activar/desactivar el sistema de intrusión de manera selectiva que mejora la seguridad de las instalaciones. Esto se puede usar como un activador para el sistema de iluminación del edificio para encender/apagar de manera selectiva las luces solo cuando pase un usuario. Esto se puede integrar en el sistema HVAC del edificio para mantener la temperatura ambiente solo para los sitios que estén ocupados y así obtener una eficiencia energética. Esta solución también detecta el seguimiento de cerca de intrusos a usuarios legítimos.

En general, el sistema incluye un sistema de automatización de edificios que protege un área geográfica protegida, una pluralidad de zonas geográficas no superpuestas dentro del área protegida, al menos un dispositivo Bluetooth portátil llevado por un usuario humano autorizado dentro del área protegida, un receptor Bluetooth asociado a cada una de la pluralidad de zonas que detecta el dispositivo portátil cerca de la zona y un controlador de seguridad que activa y desactiva al menos una de la pluralidad de zonas en función de la detección del dispositivo portátil cerca de la al menos una zona.

Alternativamente, el sistema puede incluir un sistema de automatización de edificios que protege un área geográfica protegida, una pluralidad de zonas geográficas no superpuestas dentro del área protegida, al menos un dispositivo inalámbrico de baja potencia llevado por un usuario humano autorizado dentro del área protegida, al menos un receptor inalámbrico de baja potencia asociado a cada una de la pluralidad de zonas que determina una distancia del dispositivo portátil desde la zona y un controlador de seguridad que activa y desactiva cada una de la pluralidad de zonas en función de la distancia del dispositivo portátil desde la zona.

Alternativamente, el sistema puede incluir un sistema de seguridad que protege un área geográfica protegida, una pluralidad de zonas geográficas no superpuestas dentro del área protegida, una pluralidad de dispositivos Bluetooth portátiles, llevado cada uno por un usuario humano autorizado respectivo dentro del área protegida, un receptor Bluetooth asociado a cada una de la pluralidad de zonas que determina una distancia de cada uno de la pluralidad

de dispositivos portátiles desde la zona, un procesador que determina una ubicación de cada uno de la pluralidad de dispositivos portátiles dentro del área protegida en función de la distancia del dispositivo portátil desde cada una de las zonas y un controlador de seguridad que activa y desactiva cada una de la pluralidad de zonas en función de las ubicaciones respectivas de cada uno de la pluralidad de dispositivos portátiles.

De lo anterior, se observará que numerosas variaciones y modificaciones pueden efectuarse sin apartarse del ámbito de aplicación de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Aparato que comprende:

un sistema de automatización de edificios (10) que protege un área geográfica protegida;

una pluralidad de zonas geográficas no superpuestas (18, 20, 22, 24) dentro del área geográfica protegida;

al menos un dispositivo inalámbrico de baja potencia (46, 48) dentro del área geográfica protegida;

una pluralidad de receptores inalámbricos de baja potencia (52) asociados a la pluralidad de zonas geográficas no superpuestas, en el que un receptor respectivo de la pluralidad de receptores inalámbricos de baja potencia detecta el al menos un dispositivo inalámbrico de baja potencia próximo a una zona geográfica de la pluralidad de zonas geográficas no superpuestas, y en el que el receptor respectivo de la pluralidad de receptores inalámbricos de baja potencia determina una distancia del al menos un dispositivo inalámbrico de baja potencia desde la zona geográfica de la pluralidad de zonas geográficas no superpuestas;

un controlador de seguridad (26, 30) que activa y desactiva la pluralidad de zonas geográficas no superpuestas en función de la distancia determinada del al menos un dispositivo inalámbrico de baja potencia desde la una zona geográfica de la pluralidad de zonas geográficas no superpuestas; y

un procesador (36, 38) que determina una ubicación geográfica del al menos un dispositivo inalámbrico de baja potencia en función de una señal recibida por el receptor respectivo de la pluralidad receptores inalámbricos de baja potencia,

en el que el procesador (36, 38) crea una lista de la pluralidad de zonas geográficas no superpuestas para ser desactivadas en función de la ubicación geográfica del al menos un dispositivo inalámbrico de baja potencia.

2. Aparato según la reivindicación 1, en el que el procesador (36, 38) mide un indicador de intensidad de señal de la señal.

3. Aparato según la reivindicación 2, en el que el indicador de la intensidad de señal incluye uno de un valor de indicador de intensidad de señal recibida y un valor de índice de error de bits.

4. Aparato según la reivindicación 2, en el que el procesador (36, 38) compara el indicador de la intensidad de señal con un valor umbral.

5. Aparato según la reivindicación 1, que comprende además un sensor (12, 14) que mide un parámetro de salud de un usuario autorizado.

6. Aparato según la reivindicación 5, en el que el procesador (36, 38) compara el parámetro de salud con un valor umbral, detecta que el parámetro de salud supera el valor umbral y, en respuesta, desactiva la zona geográfica de la pluralidad de zonas geográficas no superpuestas (18, 20, 22, 24).

7. Aparato según la reivindicación 1, en el que el sistema de automatización de edificios (10) comprende un sistema de seguridad.

8. Aparato según la reivindicación 1, en el que el procesador determina una velocidad de desplazamiento del al menos un dispositivo inalámbrico de baja potencia (46, 48) en función de cambios en la ubicación geográfica del al menos un dispositivo inalámbrico de baja potencia.

9. Aparato según la reivindicación 8, en el que el procesador (36, 38) compara la velocidad de desplazamiento con al menos un valor umbral y ajusta la distancia para activar y desactivar la pluralidad de zonas geográficas no superpuestas (18, 20, 22, 24) en función de la velocidad de desplazamiento.

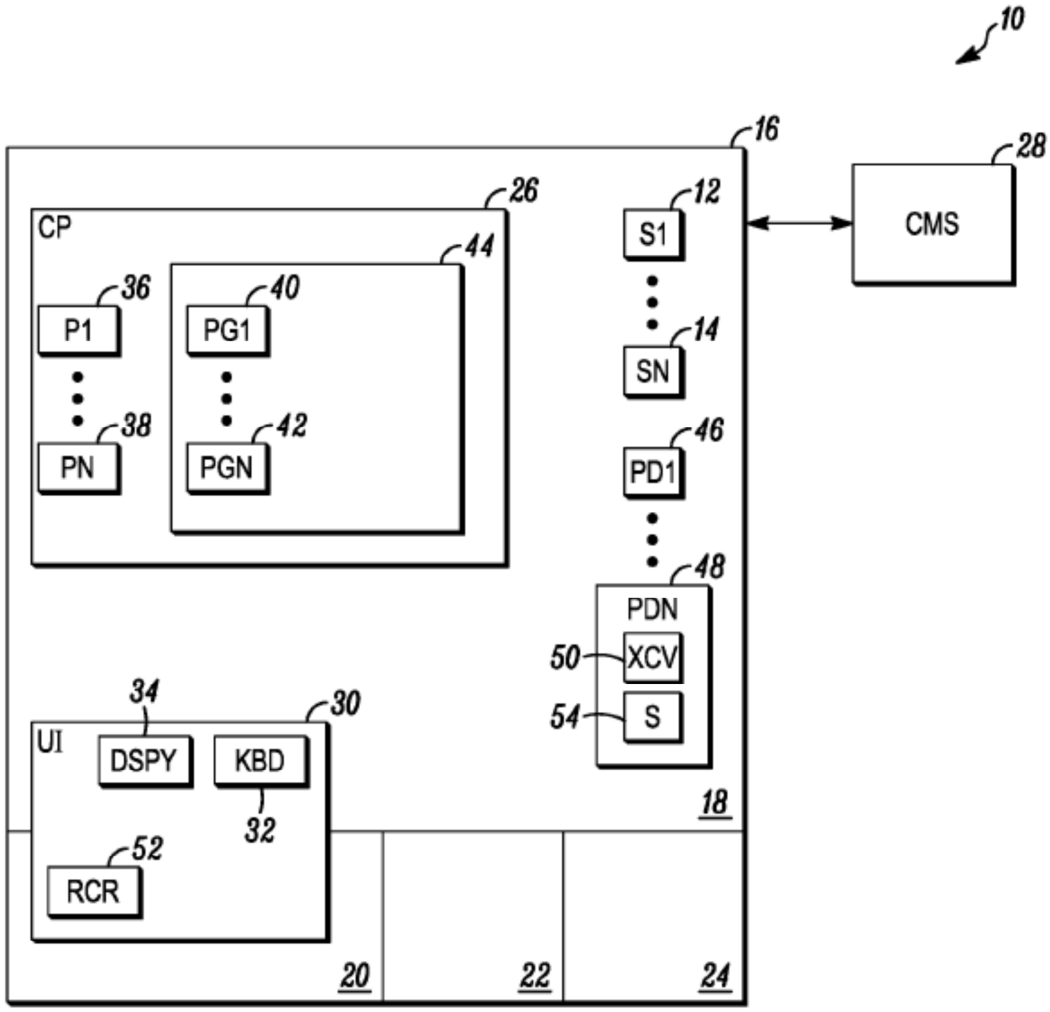
10
16
28
CMS
26
CP
44
36
P1
40
PG1
38
PN
42
PGN
12
S1
14
SN
46
PD1
48
PDN
50
XCV
54
S
34
30
UI
DSPY
KBD
32
52
RCR
18
20
22
24

FIG. 1