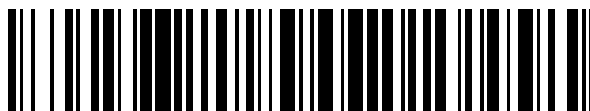


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 682 819**

51 Int. Cl.:

G08B 25/14 (2006.01)

G08B 29/04 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **22.04.2016** E 16166748 (0)

97 Fecha y número de publicación de la concesión europea: **20.06.2018** EP 3093827

54 Título: **Sistemas de generación automática de informes de datos de pronóstico procedentes de sensores inalámbricos conectados en malla en una nube informática**

30 Prioridad:

12.05.2015 US 201514709552

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

21.09.2018

73 Titular/es:

**HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road, M/S 4D3, P.O. Box 377
Morris Plains, NJ 07950, US**

72 Inventor/es:

**KRISHNAMURTHY, DIVYASHREE;
SAMAGA, ASHA;
THAWALE, VIDHYA;
RAJKUMAR, MALATHY;
DIVAKARA, MANJUNATHA y
SHARMA, SUSHIL**

74 Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 682 819 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistemas de generación automática de informes de datos de pronóstico procedentes de sensores inalámbricos conectados en malla en una nube informática

5

CAMPO TÉCNICO

Esta solicitud de patente se refiere a sistemas de seguridad y, más en particular, a sensores inalámbricos utilizados dentro de dichos sistemas.

10

ANTECEDENTES DE LA INVENCION

Se conocen sistemas para proteger a personas y bienes dentro de zonas protegidas. Dichos sistemas se suelen basar en el uso de uno o más sensores inalámbricos que detectan amenazas a los bienes dentro de la zona protegida.

15

Las amenazas a personas y los bienes se pueden originar a partir de cualquier cantidad de fuentes diferentes. A modo de ejemplo, un incendio puede matar o lesionar a los ocupantes que quedaron atrapados por un incendio en una vivienda. Del mismo modo, el monóxido de carbono de un incendio puede matar a las personas mientras duermen.

20

De forma alternativa, un intruso no autorizado, tal como un ladrón, puede representar una amenaza para los bienes dentro de la zona. Es conocido, además, que intrusos hieren o matan a personas que viven en la zona.

25

En el caso de intrusos, se pueden colocar sensores en diferentes zonas sobre la base de los usos respectivos de esas zonas. A modo de ejemplo, si las personas están 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 proporcionar protección cuando el espacio está ocupado, mientras que sensores adicionales se pueden colocar en el interior del espacio y se utilizan cuando el espacio no está ocupado.

30

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

35

Aunque los sistemas de seguridad convencionales, que utilizan sensores inalámbricos, funcionan bien, a veces están sujetos a fallos no previstos. En consecuencia, existe la necesidad de mejores métodos y aparatos para diagnosticar dichos sistemas.

40

La Publicación de Patente Europea nº EP2637147 A1 describe un método para probar un sistema de alarma, que incluye la desconexión automática del enlace del sistema de alarma a su centro de control a distancia.

SUMARIO DE LA INVENCION

La presente invención se define por las reivindicaciones adjuntas.

45

BREVE DESCRIPCION DE LOS DIBUJOS

La Figura 1 ilustra un diagrama de bloques de un sistema de seguridad de conformidad con el mismo.

50

DESCRIPCION DETALLADA

Aunque las formas de realización dadas a conocer pueden tomar numerosas formas diferentes, las formas de realización específicas de las mismas se muestran en los dibujos y se describirán aquí, en detalle, con el entendimiento de que la presente idea inventiva se debe considerar como una ejemplificación de los principios de la misma, así como su mejor forma de puesta en práctica, y no pretende limitar la solicitud, o las reivindicaciones, a la forma de realización específica ilustrada.

55

La Figura 1 ilustra un sistema de seguridad 10 que se muestra, en general, de conformidad con una forma de realización ilustrada. Dentro del sistema de seguridad se puede incluir una cantidad de sensores 12, 14 utilizados para detectar amenazas dentro de una zona geográfica protegida 16. Las amenazas se pueden originar a partir de cualquiera de varias fuentes distintas. A modo de ejemplo, un intruso puede representar una amenaza para personas y/o bienes dentro de una vivienda o negocio. De modo similar, una fuga de fuego o de gas puede amenazar la seguridad de esas mismas personas y/o bienes.

60

En consecuencia, los sensores pueden ponerse en práctica en cualquiera de una serie de formas diferentes. A modo de ejemplo, al menos algunos de los sensores pueden ser interruptores colocados en las puertas y ventanas que

65

proporcionan entrada y salida de la zona protegida. Otros sensores pueden ser sensores infrarrojos pasivos (PIR), situados dentro de la zona protegida con el fin de detectar intrusos que han podido eludir los sensores a lo largo de la periferia de la zona protegida. Otros sensores pueden ser, además, detectores de humo y/o fuego.

5 Dentro de la zona protegida se incluye, además, un panel de control o controlador 18. El panel de control puede estar situado dentro de la zona protegida, tal como se ilustra en la Figura 1, o situado de forma distante.

10 El panel de control puede controlar la activación de los sensores. A la activación de uno de los sensores, el panel de control puede generar un mensaje de alarma y enviarlo a una estación de supervisión central 20. La estación de supervisión central puede responder mediante la convocatoria de la ayuda adecuada (a modo de ejemplo, policía, departamento de bomberos, etc.).

15 El sistema de seguridad puede ser controlado por un usuario humano a través de una interfaz de usuario 22. En la interfaz de usuario puede estar incluida una pantalla de visualización 24 y un teclado 26.

20 Situada dentro del panel de control, la interfaz de usuario, y cada uno de los sensores, puede ser uno o más aparatos procesadores (procesadores) 30, 32, cada uno funcionando bajo el control de uno o más programas informáticos 34, 36 cargados a partir de un soporte legible por ordenador no transitorio (memoria) 38. Tal como aquí se utiliza, la referencia a una etapa puesta en práctica por un programa informático se refiere, además, al procesador que ejecutó dicha etapa.

25 El sistema de seguridad puede activarse y desactivarse a través de la interfaz de usuario. A este respecto, un usuario autorizado puede introducir un número de identificación personal (PIN) y una instrucción a través del teclado. La instrucción puede ser una instrucción de activación, de una activación a distancia y/o una orden de desactivación.

30 Un procesador de estado puede supervisar la interfaz de usuario para la entrada procedente del usuario humano. A la detección un PIN, el procesador de estado puede comparar el PIN introducido con los PINs de usuarios autorizados. Si el PIN introducido coincide con el PIN de un usuario autorizado, entonces el procesador de estado ejecuta la instrucción. En caso contrario, la entrada se puede ignorar, o se genera un mensaje de error.

35 En el estado de activación, un procesador de alarma supervisa cada uno de los sensores para activación. Al detectar la activación de uno de los sensores, el procesador de alarma compone y envía un mensaje de alarma a la estación de supervisión central. El mensaje de alarma puede incluir un identificador del sistema (p.ej., número de cuenta, dirección postal, etc.), un identificador del sensor y el momento de activación.

40 En general, los sensores de la Figura 1 son dispositivos inalámbricos que se comunican con el panel de control en uno o más canales de radiofrecuencia. Por consiguiente, un transceptor de radiofrecuencia respectivo 40, situado dentro del panel de control y cada uno de los sensores, se proporciona en soporte de dicha comunicación inalámbrica.

45 A modo de ejemplo, el panel de control puede incluir uno o más procesadores de comunicación que definen una súper-trama para la comunicación entre el panel de control y los sensores. La súper-trama se puede definir, a su vez, por un número de ranuras temporales de acceso múltiple por división de tiempo (TDMA) que vuelven a producirse durante un período de tiempo predeterminado. Algunas de las ranuras se pueden reservar para ser utilizadas por los sensores bajo un protocolo 6LowPan/IPv6/IoT.

50 La súper-trama puede incluir una ranura reservada para una baliza, y ranuras reservadas para el intercambio de mensajes entre los sensores y el panel de control bajo la norma IEEE 802.15.4 y/o el protocolo 6LowPAN. La baliza puede identificar un punto de inicio de la súper-trama e incorpora una cantidad de campos de datos que definen, cada uno, aspectos respectivos de la súper-trama.

55 Cada sensor del sistema de la Figura 1 puede tener una dirección corta y una dirección IPv6 (6LowPan) y un identificador MAC (MAC ID). El sistema de direccionamiento facilita el acceso de los sensores por cualquier otro dispositivo compatible con IPv6, tal como se describe en varias publicaciones de Internet of Things (IoT). Lo que antecede permite que los sensores se organicen por respectivos procesadores en redes de estrella o árbol.

60 El estado operativo del panel de control (p.ej., activado, desactivado, con anomalía operativa, etc.) se puede transmitir como parte de la carga útil de la baliza. Si es necesario, se puede transmitir, además, un indicador detallado del estado del panel dentro de las respectivas ranuras bajo los protocolos 6LowPAN/802.15.4. Las ranuras de control de la baliza se pueden utilizar, además, para enviar mensajes de demanda a partir del panel de control a dispositivos finales (p.ej., sensores, etc.) sobre la base de las direcciones IEEE802.15.4 de los dispositivos finales.

65 En una forma de realización ilustrada, un procesador de supervisión del panel de control supervisa una serie de aspectos operativos y ambientales internos de cada sensor para indicaciones de posibles fallos. Esto se puede conseguir mediante un sistema de informes dentro de cada uno de los sensores que recopila e informa, periódicamente, sobre una serie de indicadores de fiabilidad del sensor. Lo anterior se puede lograr a través de un

procesador de informes dentro del sensor que recopila de forma automática y envía periódicamente los indicadores al panel de control o el procesador de supervisión del panel de control puede sondear, de forma periódica, a cada uno de los sensores para conocer los indicadores de confiabilidad.

5 Los indicadores de fiabilidad se pueden proporcionar a partir de cualquiera de varias fuentes diferentes dentro de cada sensor. A modo de ejemplo, una fuente puede ser un procesador de supervisión de tensión que vigila la tensión de la batería del sensor. Otra fuente puede ser un procesador de intensidad de señal, que supervisa un nivel de energía de paquetes transmitidos por el sensor al panel, ya sea directamente o a través de otro de los sensores. Otra fuente puede ser, además, uno o más procesadores de contador que cuentan la cantidad de paquetes que se transmiten y reciben por período de tiempo (p.ej., por hora, por día, etc.). En este sentido, un procesador de contador puede contabilizar la cantidad de paquetes que se originan dentro del sensor y que se intercambian con el panel de control. Otro procesador de contador puede contar la cantidad de paquetes que se intercambian con el panel de control en representación de un sensor secundario de la red de malla.

15 Otra fuente puede ser un procesador de calidad de enlace que supervisa una calidad de enlace del canal de comunicación entre el sensor y el panel. El procesador de calidad de enlace puede controlar el número de errores durante un período de tiempo, como una medida de la calidad del enlace de comunicación entre el sensor y el panel.

20 Otra fuente de información de fiabilidad se puede proporcionar, además, por un procesador de detección de temperatura dentro del sensor. En este caso, el procesador de detección de temperatura puede estar acoplado a un elemento de detección que detecta y mide una temperatura de los procesadores del sensor.

25 En la forma de realización ilustrada, el procesador de generación de informes de cada sensor puede recoger dichos indicadores de fiabilidad (p.ej., temperatura, calidad de enlace, potencia de transmisión, número de paquetes transmitidos por período de tiempo, etc.) y transmitir estos valores al procesador de supervisión del panel de control. Los indicadores informados de cada sensor se pueden guardar en un archivo respectivo 50, 52. El procesador de supervisión, u otro procesador relacionado, puede comparar los indicadores de fiabilidad con una cantidad de criterios 54, 56, con el fin de identificar uno o más modos de fallo potenciales para el informe del sensor a los indicadores.

30 Cuando se detecta un modo de fallo potencial, el procesador de supervisión puede enviar una notificación correspondiente 58, 60 asociada con los criterios a una aplicación en la nube informática 44, a través de Internet 42. La aplicación en la nube informática, a su vez, puede informar del posible fallo a un dispositivo portátil 48 de una persona responsable del sensor.

35 A este respecto, la aplicación en la nube informática puede incluir uno o más programas informáticos que se ejecutan en un aparato procesador (procesador) 46. De modo similar, el dispositivo portátil de la persona responsable puede ser un teléfono inteligente.

40 La notificación enviada a la persona responsable se puede determinar por el tipo de modo de fallo implicado. Se incluye con la notificación un identificador del sensor por localización y tiempo. La identificación del sensor puede basarse en una ubicación geográfica del sensor y/o sistema de seguridad (p.ej., una dirección del sistema de seguridad, localización de GPS, etc.). Como alternativa, o de forma adicional, a notificación puede incluir un identificador separado y/o una localización de GPS del sensor dentro de la zona protegida.

45 Las notificaciones y los criterios están formateados para el posible fallo implicado. A modo de ejemplo, una notificación de un posible fallo puede ser una predicción de fallo de la batería, o un nivel bajo de la batería en función de la cantidad de paquetes transmitidos y recibidos por el sensor. En este caso, los criterios pueden estar basados en un nivel umbral de paquetes que pueden transmitirse y recibirse por período de tiempo.

50 La situación en la que un sensor transmite y recibe demasiados paquetes durante un período de tiempo puede ser causada por cualquiera de una serie de factores diferentes. A modo de ejemplo, un sensor en una red de malla puede estar situado en una localización central en donde varios sensores secundarios deben confiar en el sensor situado en el centro para comunicarse con el panel de control. Sin embargo, lo anterior puede dar lugar a un fallo prematuro de batería del sensor situado en una posición central que está desproporcionado con los sensores circundantes.

55 Para abordar este modo de fallo potencial particular, uno de los criterios puede comparar el número de paquetes intercambiados en nombre de un nodo secundario con un valor umbral de nodo secundario. Si un sensor supera el valor umbral, en este caso se puede enviar una notificación adecuada a la persona responsable. La notificación puede incluir un aviso de que el sensor está en peligro de fallo de la batería debido a la excesiva actividad del paquete de nodo secundario y la sugerencia de que los sensores en la zona deben re-situarse de modo que se reduzca la actividad del nodo secundario por intermedio del sensor.

65 Otro criterio puede estar basado en el nivel de potencia de la señal transmitida de cada sensor. A modo de ejemplo, el panel puede detectar una disminución pronunciada y constante en la intensidad de la señal y etiquetarse para una

notificación de baja intensidad de señal. En este caso, una indicación de baja intensidad de señal es de mayor valor que un bajo nivel de tensión de la batería puesto que es una indicación mucho más prematura del fallo inminente de la batería.

5 Otros criterios pueden estar basados en una temperatura del sensor medida o detectada. En este caso, un aumento pronunciado y continuo de la temperatura puede ser un indicador de que el sensor está demasiado cerca de una fuente de calor externa, o de que el procesador sensor no funciona bien debido a un fallo del software o al fallo del hardware. La alta temperatura es una indicación probable de un fallo inminente del sensor. En este caso, la notificación enviada puede ser una advertencia de alta temperatura para el sensor.

10 Otro criterio puede basarse en el nivel de calidad del enlace de radiofrecuencia entre el sensor y el panel de control. En este caso, los criterios pueden ser simplemente un valor umbral de calidad de enlace. En este caso, la baja calidad del enlace puede deberse a una localización deficiente del sensor y a una incompatibilidad del sensor con su ubicación. A modo de ejemplo, el sensor puede estar situado detrás de un poste de metal u otra estructura conductora. La notificación, en este caso, puede incluir la sugerencia de que el sensor debe moverse a una posición mejor.

15 Cada una de las condiciones de fallo potencial se puede comunicar por el panel a la nube informática. La nube informática recibe una notificación del posible fallo junto con la ubicación GPS del panel y puede notificarlo a los instaladores que pueden estar trabajando cerca de las instalaciones del panel para su atención inmediata. La aplicación en la nube informática puede enviar notificaciones a un usuario autorizado, distribuidor del sensor u otra persona responsable, incluyendo una indicación del motivo del fallo del sensor, o posible fallo o condición de drenaje de la batería, o problemas ambientales, o mal funcionamiento, junto con la gravedad de la situación. Si la persona responsable es un distribuidor, el distribuidor puede llamar a los usuarios finales y advertir al usuario final de la actividad de mantenimiento necesaria para evitar penalizaciones por falsas alarmas que, de otro modo, se producirían debido a un sensor defectuoso.

20 A partir de lo que antecede, ha de observarse que se pueden realizar numerosas variaciones y modificaciones sin desviarse del alcance de la misma. Debe entenderse que no se pretende o debe inferirse ninguna limitación con respecto al aparato específico ilustrado en este documento. Por supuesto, las reivindicaciones adjuntas están previstas para cubrir todas las modificaciones que caigan dentro del alcance de las reivindicaciones. Además, los flujos lógicos ilustrados en las figuras no requieren el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. Se pueden proporcionar otras etapas, o se pueden eliminar etapas, a partir de los flujos descritos, y se pueden añadir otros componentes, o eliminarlos de las formas de realización descritas.

35

REIVINDICACIONES

1. Un aparato que comprende:
 - 5 un primer sensor inalámbrico (12, 14), en donde el primer sensor inalámbrico (12, 14) detecta amenazas dentro de una zona geográfica protegida (16);
 - un segundo sensor inalámbrico, en donde el segundo sensor inalámbrico (12, 14) detecta las amenazas dentro de la zona geográfica protegida (16);
 - 10 un procesador (30, 32) de cada uno de los primero y segundo sensores inalámbricos (12, 14) que detecta las condiciones operativas internas del sensor (12, 14) e informa sobre las condiciones operativas internas;
 - un procesador de panel de control (30, 32) que recibe y correlaciona las condiciones operativas internas de un sensor entre el primer sensor inalámbrico y el segundo sensor inalámbrico (12, 14) con un modo de fallo potencial, e informa del modo de fallo potencial a una aplicación en la nube informática (44); y
 - 15 un procesador en la nube informática (46) de la aplicación en la nube informática (44) que determina una localización del sensor (12, 14) e informa del modo de fallo potencial y la localización a una persona responsable del sensor (12, 14),
 - 20 en donde el primer sensor inalámbrico (12, 14) y el segundo sensor inalámbrico (12, 14) están dispuestos en una red de malla.
- 25 2. El aparato según la reivindicación 1, en donde el procesador del panel de control (30, 32) es parte de un panel de control (18) que supervisa una pluralidad de sensores (12, 14), que incluye el primer sensor inalámbrico (12, 14) y el segundo sensor inalámbrico (12, 14).
- 30 3. El aparato según la reivindicación 2, en donde el procesador del panel de control (30, 32) sondea a cada uno de la pluralidad de sensores (12, 14) para obtener datos.
4. El aparato según la reivindicación 2, en donde la pluralidad de sensores (12, 14) comprende uno o más detectores de humo, detectores de monóxido de carbono y detectores de intrusión.
- 35 5. El aparato según la reivindicación 1 que comprende, además, un contador dentro de al menos el primer sensor inalámbrico (12, 14), que determina la cantidad de veces en que el primer sensor inalámbrico (12, 14) ha transmitido datos.
- 40 6. El aparato según la reivindicación 2 que comprende, además, un contador dentro de al menos el primer sensor inalámbrico (12, 14) que determina una cantidad de veces en que el primer sensor inalámbrico (12, 14) ha retransmitido datos a partir de otros de entre la pluralidad de sensores (12, 14).
- 45 7. El aparato según la reivindicación 1, en donde el procesador (30, 32) de al menos el primer sensor inalámbrico (12, 14) determina e informa de una temperatura del primer sensor inalámbrico (12, 14).
8. El aparato según la reivindicación 1, en donde el procesador (30, 32) de al menos el primer sensor inalámbrico (12, 14) determina e informa de una potencia de transmisión del primer sensor inalámbrico (12, 14).
- 50 9. El aparato según la reivindicación 2, en donde el procesador (30, 32) de cada uno de entre el primero y segundo sensores inalámbricos (12, 14) comunica las condiciones operativas internas al panel de control (18).
10. El aparato según la reivindicación 9, en donde las condiciones operativas internas comunicadas al panel de control (18) comprenden, además, una o más de una cantidad de veces que el sensor (12, 14) ha transmitido datos al panel de control (18), una cantidad de veces que el sensor (12, 14) ha retransmitido los datos a partir de otros de entre la pluralidad de sensores (12, 14) al panel de control (18), una tensión de la batería, una temperatura del sensor (12, 14), y una potencia de transmisión.
- 55 11. El aparato según la reivindicación 10, en donde el procesador del panel de control (30, 32) correlaciona la temperatura del sensor (12, 14) con el modo de fallo potencial.
- 60 12. El aparato según la reivindicación 11, en donde el procesador del panel de control (30, 32) correlaciona una tasa de elevación de la temperatura del sensor (12, 14) con el modo de fallo potencial.
- 65 13. El aparato según la reivindicación 10, en donde el procesador del panel de control (30, 32) correlaciona el número de veces que el sensor (12, 14) ha transmitido los datos al panel de control (18) con el modo de fallo potencial.

14. El aparato según la reivindicación 10, en donde el procesador del panel de control (30, 32) correlaciona la potencia de transmisión con el modo de fallo potencial.

5 15. El aparato según la reivindicación 14, en donde el procesador del panel de control (30, 32) correlaciona una tasa de disminución en la potencia de transmisión con el modo de fallo potencial.

10

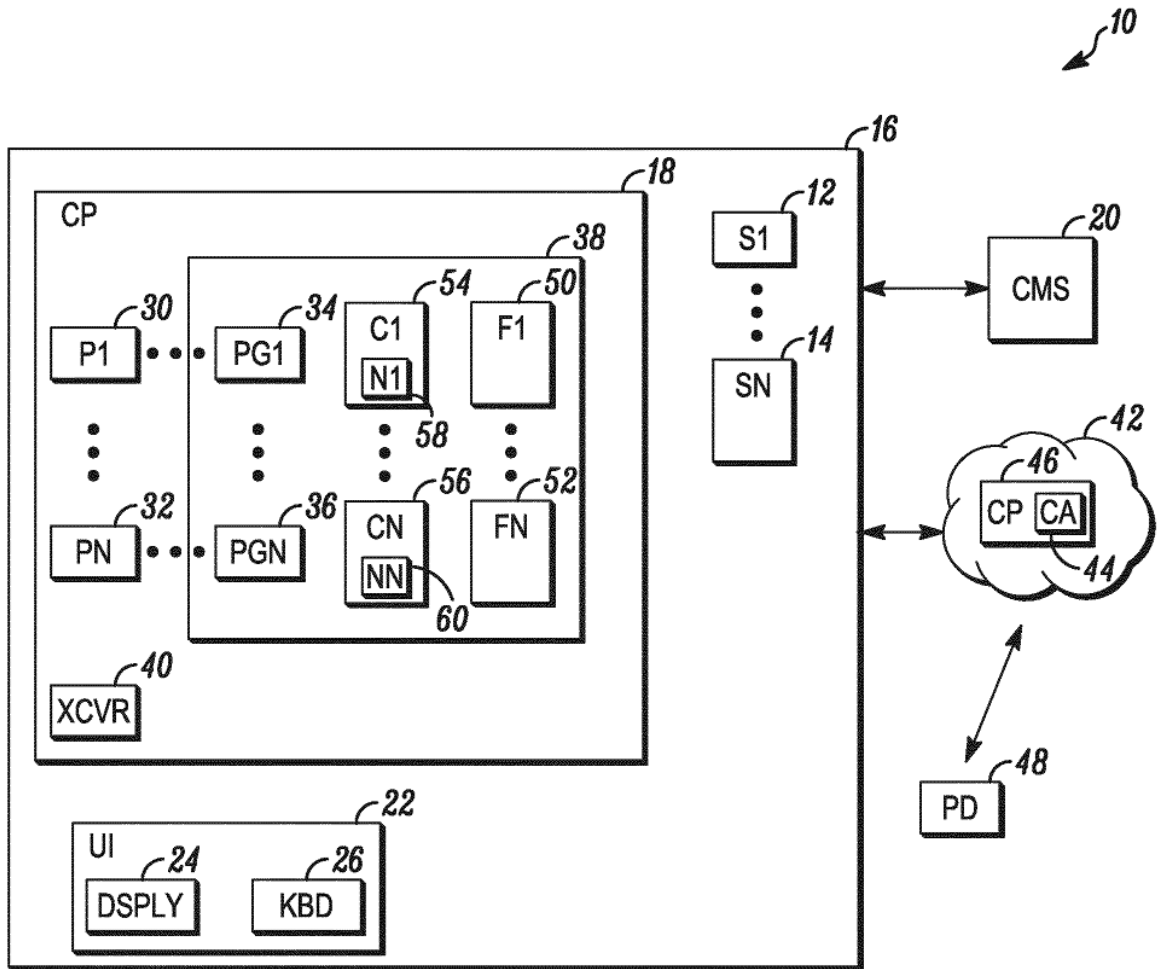


FIG. 1