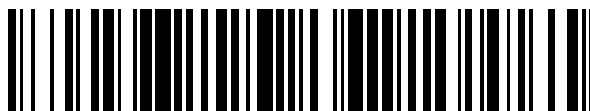


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 791 728**

51 Int. Cl.:

H04N 7/18 (2006.01)

G08B 13/196 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **26.03.2015** E 15161214 (0)

97 Fecha y número de publicación de la concesión europea: **18.03.2020** EP 2934004

54 Título: **Sistema y procedimiento de actualizaciones de parámetros de cámara basados en zonas virtuales en sistemas de vídeo vigilancia**

30 Prioridad:

14.04.2014 US 201414251887

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

05.11.2020

73 Titular/es:

**HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road
Morris Plains, NJ 07950, US**

72 Inventor/es:

**MEGANATHAN, DEEPAK SUNDAR y
GOPINATH, VIVEK**

74 Agente/Representante:

ELZABURU, S.L.P

Observaciones:

Véase nota informativa (Remarks, Remarques o Bemerkungen) en el folleto original publicado por la Oficina Europea de Patentes

ES 2 791 728 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

Sistema y procedimiento de actualizaciones de parámetros de cámara basados en zonas virtuales en sistemas de vídeo vigilancia

Campo

- 5 El campo está dirigido a sistemas de seguridad y más particularmente a sistemas de video vigilancia.

Antecedentes

Se conocen sistemas para proporcionar seguridad en una o más áreas aseguradas predefinidas. Seguridad en este caso significa la detección de amenazas a la seguridad de los ocupantes humanos y/o activos dentro del área asegurada.

- 10 Las amenazas pueden presentarse por cualquiera de una serie de eventos diferentes, tales como incendios, gas natural, intrusos, etc. Para mitigar el daño potencial causado por tales amenazas, es importante detectar las amenazas lo antes posible.

- 15 Las amenazas pueden detectarse utilizando cualquiera de una serie de tecnologías diferentes. Por ejemplo, algunos sistemas pueden basarse por completo en el uso de sensores en puertas y ventanas que conducen al área asegurada y/o el uso de una serie de detectores de incendios y/o gases distribuidos por toda el área.

- 20 Si bien el aparato de detección es efectivo en algunos casos, dicho aparato no se puede usar en todas las aplicaciones, particularmente cuando hay un gran número de personas presentes tal como un aeropuerto o en aplicaciones industriales donde las amenazas de bajo nivel tales como las llamas o la presencia de gases son parte de un proceso de fabricación. En tales casos, la seguridad puede complementarse o reemplazarse sustancialmente con una o más cámaras de vigilancia.

En muchos casos, la una o más cámaras de seguridad pueden estar acopladas a un conjunto correspondiente de monitores de seguridad (pantallas) en una estación de guardia. En este caso, un guardia humano puede monitorear constantemente las pantallas para indicación de amenazas. El video de cada cámara también se puede grabar a través de un sistema de grabación de video en red.

- 25 Si bien tales sistemas funcionan bien, un guardia puede no siempre notar una amenaza que se muestra en un monitor. Incluso cuando un guardia advierte una amenaza, es posible que el guardia no siempre tenga tiempo o una comprensión cognitiva suficiente de la situación para optimizar de manera efectiva las cámaras para mostrar o grabar la amenaza. En consecuencia, existe la necesidad de mejores métodos para mostrar y registrar tales amenazas.

- 30 La solicitud de Patente del Reino Unido GB2408880A, de 08 de junio de 2005 describe un sistema para monitorear imágenes generadas por una pluralidad de cámaras, analizar imágenes para actividades, seleccionar y mejorar imágenes de interés y grabar incidentes que se consideran de interés para el operador.

- 35 La solicitud de Patente de los Estados Unidos US 2012/0194336 A1, de 2 de agosto de 2012, describe un sistema de seguridad configurado para mostrar una representación de un área en una pantalla, con iconos para representar una pluralidad de sensores, tales como video, radar, sensores perimetrales, donde el usuario puede seleccionar sensores para su visualización o configuración.

Compendio de la invención

La presente invención proporciona un método como se define en la reivindicación 1. El método puede incluir las características de una cualquiera o más de las reivindicaciones dependientes 2 a 11.

- 40 La presente invención también proporciona un sistema como se define en la reivindicación 12. El sistema puede incluir las características de una cualquiera o más de las reivindicaciones dependientes 13 a 15.

Breve descripción de los dibujos

La Figura 1 ilustra un diagrama de bloques de un sistema de seguridad de acuerdo con el presente documento;

La Figura 2 es una pantalla de ventanas de video que se puede mostrar por el sistema de la Figura 1;

- 45 La Figura 3 es un mapa de un área asegurada protegida por el sistema de seguridad de la Figura 1;

La Figura 4 representa el mapa de la Figura 3 con una porción identificada para un mayor nivel de vigilancia;

La Figura 5 representa un mapa tridimensional y una porción seleccionada del área asegurada protegida por el sistema de seguridad de la Figura 1; y

La Figura 6 representa un mapa a nivel de calle y una porción seleccionada del área asegurada protegida por el sistema de seguridad de la Figura 1.

Descripción detallada

5 Si bien las realizaciones descritas pueden tomar muchas formas diferentes, las realizaciones específicas de las mismas se muestran en los dibujos y se describirán en la presente memoria en detalle con el entendimiento de que la presente descripción debe considerarse como un ejemplo de los principios de la misma, así como el mejor modo de practicar la misma, y no está destinado a limitar la solicitud o las reivindicaciones a la realización específica ilustrada.

10 La Figura 1 es un diagrama de bloques de un sistema de seguridad 10 mostrado generalmente de acuerdo con una realización ilustrada. Incluido dentro del sistema puede haber una serie de sensores 12, 14 utilizados para detectar amenazas dentro de un área asegurada 16.

15 Los sensores pueden basarse en cualquiera de una serie de tecnologías diferentes. Por ejemplo, al menos algunos de los sensores pueden ser interruptores de límite que funcionan como sensores de intrusión colocados en puertas y/o ventanas que permiten el acceso y la salida desde el área asegurada. Alternativamente, los sensores pueden ser sensores de infrarrojos pasivos (PIR) que detectan intrusos que han podido superar cualquier barrera física (por ejemplo, puertas, paredes, etc.) que rodea el área asegurada.

Los sensores también pueden incluir uno o más sensores ambientales tales como detectores de llama y/o gas. Los sensores ambientales pueden distribuirse por toda el área asegurada.

20 El área asegurada también puede incluir una serie de cámaras de video 18, 20. Las cámaras pueden ubicarse por toda el área asegurada o en un área específica donde se sabe que ocurren amenazas con frecuencia.

Los sensores y las cámaras pueden ser monitoreados por un panel de control 22 ubicado dentro del área asegurada o en una ubicación remota. Al detectar una amenaza a través de uno de los sensores o cámaras, el panel de control puede componer y enviar un mensaje de alarma a una estación central de monitoreo 24.

25 Incluida dentro del panel de control una circuitería de control que proporciona la funcionalidad del sistema de seguridad. La circuitería de control puede incluir uno o más aparatos procesadores (procesadores) 26, 28, cada uno de los cuales funciona bajo el control de uno o más programas informáticos 30, 32 cargados desde un medio legible por ordenador (memoria) no transitorio 34. Como se usa en la presente memoria, la referencia a un paso de un programa de ordenador también hace referencia al procesador que ejecutó ese paso.

30 Incluido dentro de la memoria del sistema de seguridad puede haber un archivo 50 de modelo de información de construcción (BIM). El archivo BIM puede incluir un mapa que incluye información tridimensional (es decir, coordenadas geográficas) de elementos estructurales del área asegurada. El modelo BIM también puede incluir las coordenadas geográficas de cada una de las cámaras dentro del área asegurada.

35 El sistema de seguridad también puede incluir un grabador de video en red (NVR) 36. El NVR graba video de cada una de las cámaras en un archivo respectivo dentro de la memoria. El archivo incluye un identificador de la cámara respectiva que proporciona cada uno de los cuadros de video y un tiempo de grabación de cada cuadro. El archivo también puede incluir un identificador del área geográfica capturada en las imágenes.

40 Se proporciona una interfaz de usuario (UI) 38 para el control del sistema de seguridad y sus cámaras. A este respecto, el video de las cámaras puede presentarse en una pantalla 40. La selección de las cámaras para mostrar en la pantalla del visualizador puede realizarse a través de una pantalla táctil del visualizador y una interfaz gráfica de usuario (GUI) o mediante un teclado separado 42.

45 Por ejemplo, un procesador de interfaz puede presentar un conjunto de iconos (teclas de control de software) 44, 46 a lo largo de un lado de la pantalla. Al menos algunas de las teclas de control pueden estar asociadas con cada una de las cámaras. Para mostrar el video de una cámara en la pantalla, el operador puede usar un ratón para colocar un cursor 48 sobre el ícono de la cámara y activar un interruptor en un ratón asociado con el cursor. El procesador de interfaz puede monitorear la posición del cursor y al detectar el cursor sobre el ícono de una cámara y activar el interruptor, el procesador de interfaz puede activar un procesador de pantalla asociado con la cámara. El procesador de pantalla puede abrir una ventana en la pantalla que muestra imágenes en tiempo real de la cámara dentro de la ventana.

50 Además de mostrar imágenes de cámaras individuales, al menos algunas de las teclas de control pueden usarse para mostrar agrupaciones de cámaras (salvas de cámaras) dentro de la misma ventana o ventanas diferentes. De manera similar, se pueden usar otras teclas de control para activar cámaras en porciones seleccionadas del área asegurada.

En general, los operadores de circuito cerrado de televisión (CCTV) encuentran que las aplicaciones de sistemas de seguridad convencionales no son muy amigables para el operador en términos de monitoreo en directo y

configuración. Sería deseable si los operadores de CCTV pudieran concentrarse más en las actividades que ocurren en las cámaras y áreas monitoreadas en lugar de los requisitos de acceso y control.

5 Por ejemplo, en un escenario, un operador de CCTV puede notar actividad sospechosa que involucra a una persona u objeto en el campo de visión de una cámara en particular. En este caso, el operador está más interesado en obtener la mayor cantidad de detalles posible de las cámaras y sensores del área monitoreada, ya que una vez grabado, el video no puede mejorarse de manera real.

10 En la mayoría de los casos, es difícil explotar la capacidad de imagen más alta posible de todas las cámaras en un sistema debido al diseño del sistema y los costos operativos. Por ejemplo (debido a las limitaciones de ancho de banda), un NVR usado en conjunto con 32 cámaras puede no tener la capacidad de grabar video con máxima resolución y cuadros por segundo.

15 En general, un sistema debe construirse con la capacidad de aumentar la calidad de grabación en ciertas situaciones. Por ejemplo, en el caso de un evento de seguridad, la configuración de los parámetros de calidad de video podría aumentarse a un nivel máximo. Sin embargo, esto debería preconfigurarse y, a menudo, es difícil juzgar cuándo implementar este tipo de configuración, ya que se puede observar actividad sospechosa en cualquier cámara por todas las instalaciones.

20 En una realización ilustrada, el ajuste de la configuración se puede lograr mediante un conjunto de pasos muy simples realizados por un operador o usuario humano. Por ejemplo, el sistema de seguridad puede detectar un evento y el usuario puede definir un área de alto riesgo alrededor del evento. En otra realización, el usuario puede percibir actividad sospechosa en video en directo, identificar una cámara que proporciona una vista del evento en un mapa y definir el área de alto riesgo alrededor de la cámara.

Se puede identificar más de un área de alto riesgo en cualquier instante en el tiempo. En cada caso, el operador define un área alrededor del evento.

25 Al detectar un evento o actividad sospechosa, los parámetros de calidad de video de esa cámara se pueden aumentar (o disminuir) en función del riesgo percibido. Si bien ciertos parámetros se discutirán a continuación, cualquier parámetro de calidad se puede ajustar para mejorar la calidad de la imagen.

Al identificar un área de alto riesgo, puede aumentarse la calidad de video de al menos algunas cámaras en esa área. En otras áreas no designadas (áreas de bajo riesgo), los parámetros de calidad de video pueden reducirse para preservar el ancho de banda del sistema. En otras áreas más (por ejemplo, Sala de servidores, centro de datos, etc.), la calidad puede considerarse como de misión crítica y nunca puede disminuirse.

30 En otras realizaciones, algunas cámaras dentro de un sistema pueden designarse solo para monitoreo en directo y no para grabación. Si una de estas cámaras se encuentra dentro de una zona de alto riesgo, entonces el sistema automáticamente comienza a grabar estas cámaras mientras el área permanezca bajo la designación de alto riesgo.

35 En general, la Figura 2 muestra una pantalla 100 que puede mostrarse en el visualizador de la interfaz de usuario. Mientras que ve la pantalla, el operador puede notar una actividad sospechosa (paso 1) de una persona u objeto en una de las vistas de la cámara.

En respuesta, el operador puede usar el cursor para seleccionar la ventana 102 que muestra la actividad sospechosa. El procesador de interfaz puede detectar la selección de la ventana y mostrar un menú de teclas de control que pueden seleccionarse individualmente para observar y registrar mejor la actividad sospechosa.

40 Por ejemplo, el operador puede seleccionar (paso 2 de la Figura 2) la tecla de control etiquetada "Mostrar vista de mapa" o el operador puede seleccionar un icono BIM en la pantalla. En respuesta, el procesador de interfaz puede detectar la selección de la tecla de control Mostrar vista de mapa o BIM y transferir un identificador de la cámara desde la ventana seleccionada a un procesador de mapas. El procesador de mapas, a su vez, recupera el mapa del área asegurada del archivo BIM y representa el mapa en la interfaz de usuario como se muestra en la Figura 3. La cámara que proporciona la vista seleccionada se puede mostrar superpuesta sobre el mapa y se puede representar como una imagen resaltada (o intermitente) de una cámara. El procesador también puede representar un círculo, cualquier forma geométrica o un dibujo a mano alrededor de la cámara, como se muestra en la Figura 3.

45 A continuación, el operador puede seleccionar (paso 1 en la Figura 4) una porción del área asegurada para mejorar la visualización de la actividad sospechosa. El operador puede identificar la porción seleccionada al rodear la porción seleccionada con una línea dibujada sobre el mapa del área asegurada que se muestra en la pantalla. Para hacer esto, el operador puede colocar el cursor sobre la porción seleccionada y activar un interruptor en el ratón seguido de mover el cursor a lo largo de la línea alrededor de la porción seleccionada del área asegurada. Al terminar el círculo u otra forma, el usuario suelta el interruptor del ratón para completar la identificación de la porción. Al soltar el interruptor, el procesador de interfaz también puede mostrar un menú de riesgo asociado con la porción seleccionada.

Alternativamente, el usuario puede usar su dedo para trazar el contorno de la porción seleccionada. En este caso, el procesador de interfaz detecta el contacto inicial del dedo del usuario y la interrupción del contacto.

5 El procesador de interfaz detecta la activación inicial del interruptor (o el contacto con el dedo del usuario) y la ubicación geográfica relativa del cursor en la ubicación. El procesador de interfaz luego rastrea el cursor como una sucesión o lugar de ubicaciones geográficas a medida que el usuario traza el círculo u otra forma que encierra la porción seleccionada.

10 El procesador de interfaz puede transferir entonces el lugar geométrico de los puntos a un procesador de identificación que identifica cualquier cámara adicional dentro de la porción seleccionada. El procesador de identificación puede hacer esto comparando las coordenadas geográficas de cada cámara dentro del área asegurada con las coordenadas geográficas del área rodeada por la línea. El procesador de identificación (o el procesador de interfaz) puede superponer cualquier cámara identificada sobre la porción seleccionada como se muestra en la Figura 4 junto con un identificador de la cámara.

15 A continuación, el usuario puede seleccionar (paso 2 en la Figura 4) el nivel de riesgo dentro de la porción seleccionada. En este sentido, el nivel de riesgo seleccionado define el nivel de calidad de imagen proporcionado por cada una de las cámaras dentro de la porción seleccionada.

20 El nivel de calidad de imagen puede ser cambiado o mejorado de otro modo por un procesador de calidad de imagen que detecte la selección de la porción del área asegurada y el nivel de riesgo. En respuesta, el procesador puede ajustar uno o más parámetros de la cámara (por ejemplo, la resolución de cada cuadro (generalmente aumentada para obtener una imagen más detallada), la cantidad de cuadros por segundo (FPS) (aumentada para obtener más detalles de la imagen), el tamaño de un grupo de imágenes (GOP) (generalmente disminuido para obtener una mejor calidad de imagen), la relación de compresión (generalmente disminuida para obtener una mejor calidad de imagen), la velocidad de bits (generalmente aumentada para obtener más datos), etc.). Cualquier parámetro de cámara que aumente o disminuya la calidad del video puede considerarse y no limitarse a los discutidos en la presente memoria. En este sentido, cada uno de los niveles de riesgo puede tener un conjunto

25 diferente de parámetros de cámara asociados con cada nivel de riesgo.

Además, cada cámara identificada puede tener su propio conjunto de parámetros asociados con cada nivel de amenaza. Esto puede ser necesario debido a la ubicación de ciertas cámaras. Por ejemplo, una cámara cerca de una entrada o cerca de un activo de alto valor en una casa o fábrica puede requerir una calidad de imagen muy mejorada al detectar actividad sospechosa.

30 El procesador de calidad de imagen también puede ajustar automáticamente el nivel de calidad de imagen de otras cámaras ubicadas fuera de la porción seleccionada (por ejemplo, a resolución CIF, 1 FPS, etc.). En este caso, el procesador de calidad de imagen puede reducir el nivel de calidad de imagen de las cámaras fuera de la porción seleccionada para conservar el ancho de banda. Por ejemplo, el NVR puede tener una capacidad limitada y la reducción del ancho de banda de las otras cámaras puede ser necesaria para no exceder la capacidad de procesamiento del NVR.

35

De manera similar, el operador de CCTV puede rodear manualmente un área particular y seleccionar la designación de bajo riesgo que se muestra en el paso 2 de la Figura 4. De esta manera, un operador puede configurar por separado áreas de bajo riesgo.

40 Como ejemplo más específico, un NVR puede tener una limitación de velocidad de cuadro de 480 FPS y solo podría manejar 16 cámaras que proporcionan video a 30 FPS. Según la realización ilustrada (y donde hay más de 16 cámaras), las cámaras de alto riesgo se establecen en 30 FPS y las de no riesgo se establecen en menos de 30 FPS.

45 Según la realización ilustrada, la identificación de una porción del área asegurada junto con la selección de un alto nivel de amenaza para esa porción hace que el sistema de seguridad mejore la calidad de las imágenes entregadas desde cada una de las cámaras identificadas a los monitores de la estación de guardia. El nivel mejorado de calidad de imagen puede mantenerse durante un tiempo predeterminado (por ejemplo, 5 minutos, 10 minutos, etc.) después de la detección inicial de actividad sospechosa. Alternativamente, el usuario puede activar una tecla de control para cancelar la calidad de imagen mejorada en cualquier momento.

50 El nivel mejorado de calidad de imagen permite al usuario humano del sistema de seguridad observar mejor la naturaleza de la actividad sospechosa. El nivel mejorado de actividad también es una característica del video grabado por el NVR. En este caso, el nivel mejorado de calidad de imagen permite un mejor análisis forense de la actividad sospechosa en un momento posterior si la actividad sospechosa fuera parte de un acto criminal.

55 La Figura 5 representa otro ejemplo del uso del sistema. En el ejemplo de la Figura 5, el usuario ha seleccionado un modelo o mapa tridimensional (3-D) de despiece de un edificio a partir del archivo BIM. En este ejemplo, el usuario puede usar un procesador modelo para navegar hacia arriba y hacia abajo a través del modelo 3-D del edificio. Las representaciones gráficas del área asegurada se pueden presentar como mapas de piso 2-D, mapas de sitio o dibujos CAD y donde los mapas o dibujos pueden estar en formatos JPEG o BMP.

5 Como también se muestra (paso 1 en la Figura 5), el usuario ha seleccionado un piso particular del edificio y ha dibujado una línea alrededor de una porción del piso. En este ejemplo, el procesador de identificación ha identificado y mostrado una serie de cámaras dentro y fuera de la porción seleccionada del piso. En un segundo paso (paso 2 en la Figura 5), el usuario ha seleccionado un nivel de alto riesgo para controlar la calidad de la imagen dentro de la porción seleccionada del piso del edificio.

La ventaja del ejemplo de la Figura 5 es que el usuario puede observar otras cámaras en el área de la actividad sospechosa. Esto permite al usuario cancelar la selección de la porción y volver a ingresar una porción más grande o más pequeña del área asegurada con el fin de cambiar la calidad de imagen de un número mayor o menor de cámaras.

10 La Figura 6 representa otro ejemplo más. En este caso, el usuario (paso 1 de la Figura 6) ha seleccionado un mapa de toda la ciudad del archivo BIM con el fin de dibujar una línea alrededor de un conjunto de calles y áreas asociadas. En el segundo paso (paso 2 de la Figura 6), el usuario selecciona el nivel de riesgo que define la calidad de imagen de cada cámara dentro de la porción seleccionada.

15 En general, el sistema puede ejecutar los pasos que incluyen un procesador de un sistema de vigilancia que detecta la identificación de una porción de un área asegurada a través de un dibujo realizado por un operador en un diagrama del área asegurada, el procesador que identifica al menos una cámara dentro de la porción identificada del área asegurada, el procesador que aumenta un nivel relativo de calidad de imagen para cada una de la al menos una cámara y el procesador que graba video con el mayor nivel de calidad de imagen de cada una de la al menos una cámara identificada durante un período de tiempo predeterminado donde la calidad de la imagen aumenta al realizar una o más de aumento de resolución de imagen, aumento de cuadros por segundo, disminución del valor de un grupo de imágenes (GOP), disminución de la relación de compresión y aumento de la velocidad de bits.

20 Alternativamente, el sistema incluye un procesador de un sistema de vigilancia que detecta la identificación de una porción de un área asegurada a través de un dibujo realizado por un operador en un diagrama del área asegurada, un procesador del sistema de vigilancia que identifica al menos una cámara dentro de la porción identificada del área asegurada, un procesador del sistema de vigilancia que aumenta un nivel relativo de calidad de imagen para cada una de la al menos una cámara y un grabador que graba video con el mayor nivel de calidad de imagen de cada una de la al menos una cámara identificada durante un período de tiempo predeterminado donde la calidad de la imagen aumenta al realizar uno o más de aumento de resolución de imagen, aumento de los cuadros por segundo, disminución del valor de un grupo de imágenes (GOP), disminución de la relación de compresión y aumento de la velocidad de bits.

25 De lo anterior, se observará que se pueden efectuar numerosas variaciones y modificaciones sin apartarse del alcance de la presente. Debe entenderse que no se pretende ni debe inferirse ninguna limitación con respecto al aparato específico ilustrado en la presente memoria. Por supuesto, se pretende cubrir mediante las reivindicaciones adjuntas todas de tales modificaciones que entren dentro del alcance de las reivindicaciones. Además, los flujos lógicos representados en las figuras no requieren el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. Se pueden proporcionar otros pasos, o se pueden eliminar pasos, de los flujos descritos, y se pueden agregar o eliminar otros componentes de las realizaciones descritas.

30
35

REIVINDICACIONES

1. Un método que comprende:

5 un procesador (26, 28) de un sistema de vigilancia (10) que detecta la selección de al menos una porción de un área asegurada a través de un dibujo alrededor de la al menos una porción hecha por un operador en un diagrama del área asegurada, en donde el procesador también detecta la porción restante del área asegurada como una zona no seleccionada;

el procesador (26, 28) que identifica al menos una cámara (18, 20) dentro de la al menos una porción seleccionada del área asegurada;

10 el procesador (26, 28) que ajusta un nivel relativo de calidad de imagen para cada una de la al menos una cámara (18, 20); y

15 el procesador (26, 28) que graba video con el nivel ajustado de calidad de imagen de cada una de la al menos una cámara identificada durante un período de tiempo predeterminado donde la calidad de imagen se ajusta cambiando cualquier parámetro de cámara que aumente o disminuya la calidad de video o realizando uno o más de aumentar o disminuir la resolución de la imagen, aumentar o disminuir los cuadros por segundo, disminuir o aumentar el valor de un grupo de imágenes (GOP), disminuir o aumentar la relación de compresión y aumentar o disminuir la velocidad de bits.

2. El método según la reivindicación 1, en donde el dibujo hecho por el operador se define por el dedo del operador que traza un contorno sobre la porción.

20 3. El método según la reivindicación 1, que comprende además que el operador observe actividad sospechosa a través de una visualización de una imagen de una cámara (18, 20) y que el operador haga clic en un icono de modelo de información de construcción (BIM).

4. El método según la reivindicación 3, que comprende además un procesador del sistema de vigilancia que destaca la cámara en el modelo BIM del área asegurada.

25 5. El método según la reivindicación 1, que comprende además que el operador seleccione un nivel de criticidad de la grabación del video.

6. El método según la reivindicación 5, que comprende además un procesador (26, 28) que selecciona un nivel relativamente alto de resolución para una cámara seleccionada en base al nivel de criticidad seleccionado.

30 7. El método según la reivindicación 1, que comprende además un procesador (26, 28) que determina un ancho de banda de la grabación de video de la cámara identificada y que reduce una resolución de al menos otra cámara (18, 20) ubicada en una porción de bajo o sin riesgo dentro del área asegurada.

8. El método según la reivindicación 1, en donde el dibujo comprende además un círculo, cualquier forma geométrica o dibujo a mano que define un límite que abarca la porción.

9. El método según la reivindicación 1, en donde la porción comprende además un edificio dentro del área asegurada.

35 10. El método según la reivindicación 9, en donde la porción comprende además un piso del edificio.

11. El método según la reivindicación 1, en donde la porción comprende además una calle que pasa a través del área asegurada.

12. Un sistema que comprende:

40 un procesador (26, 28) de un sistema de vigilancia (10) que detecta la identificación de una porción de un área asegurada a través de un dibujo hecho por un operador en un diagrama alrededor de la porción del área asegurada;

un procesador (26, 28) del sistema de vigilancia que identifica al menos una cámara (18, 20) dentro de la porción identificada del área asegurada;

un procesador (26, 28) del sistema de vigilancia que aumenta un nivel relativo de calidad de imagen para cada una de la al menos una cámara (18, 20); y

45 un grabador que graba video con el mayor nivel de calidad de imagen de cada una de la al menos una cámara (18, 20) identificada durante un período de tiempo predeterminado donde la calidad de la imagen aumenta al realizar uno o más de aumento de resolución de imagen, aumento de los cuadros por segundo, disminución del valor de un grupo de imágenes (GOP), disminución de la relación de compresión y disminución de la velocidad de bits.

13. El sistema según la reivindicación 12, que comprende además una pantalla táctil en donde el dibujo hecho por el operador está definido por el dedo del operador que traza un contorno sobre la porción en la pantalla táctil.
14. El sistema según la reivindicación 12 que comprende además una interfaz de usuario (38) en donde el operador observa actividad sospechosa a través de una visualización de una imagen de una cámara y el operador hace clic en un icono de modelo de información de construcción (BIM) a través de la interfaz de usuario (38).
15. El sistema según la reivindicación 14, que comprende además un procesador del sistema de vigilancia que destaca la cámara en el diagrama del área asegurada.

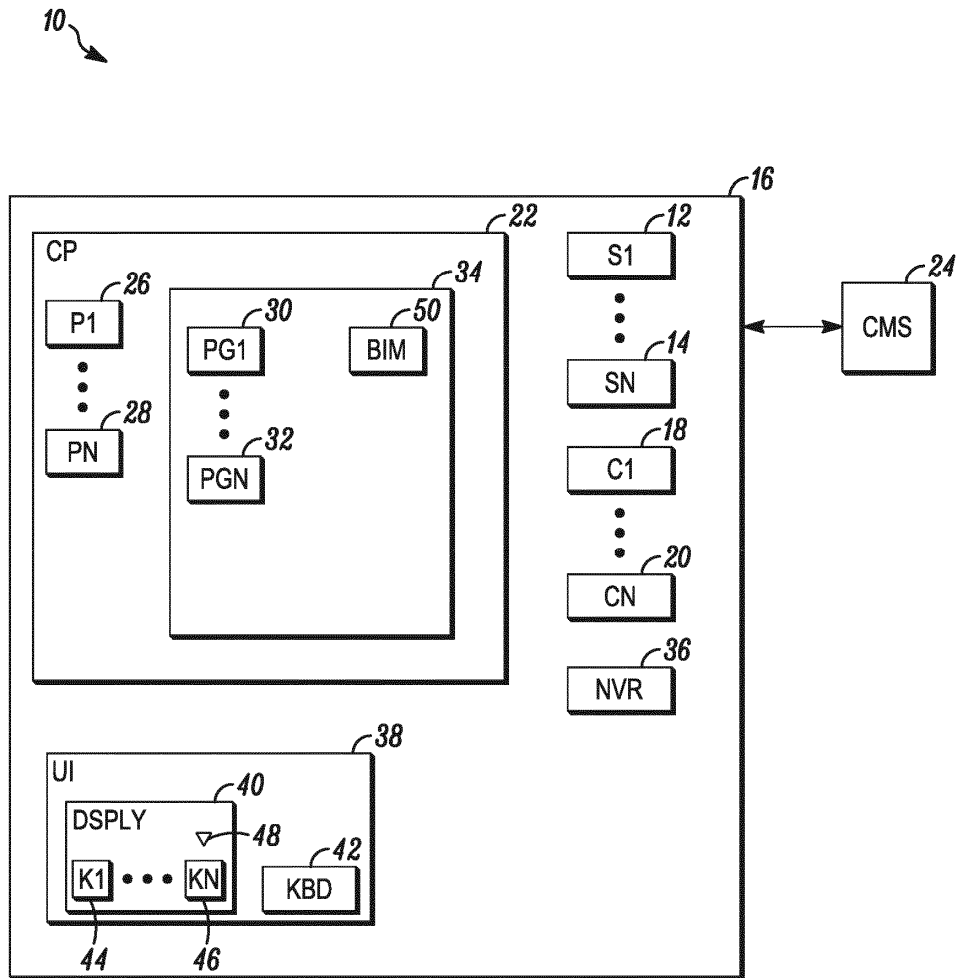


FIG. 1

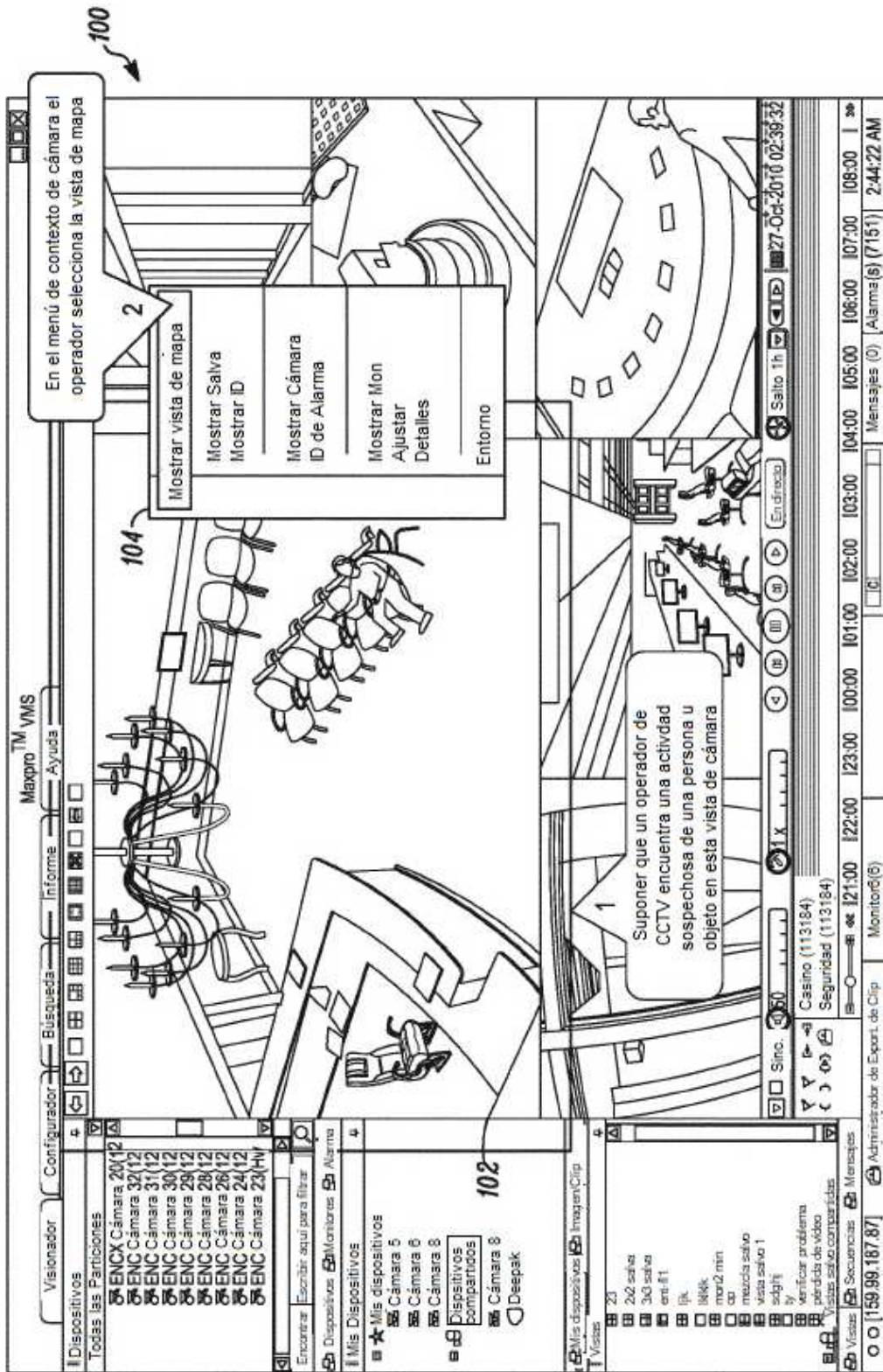


FIG. 2

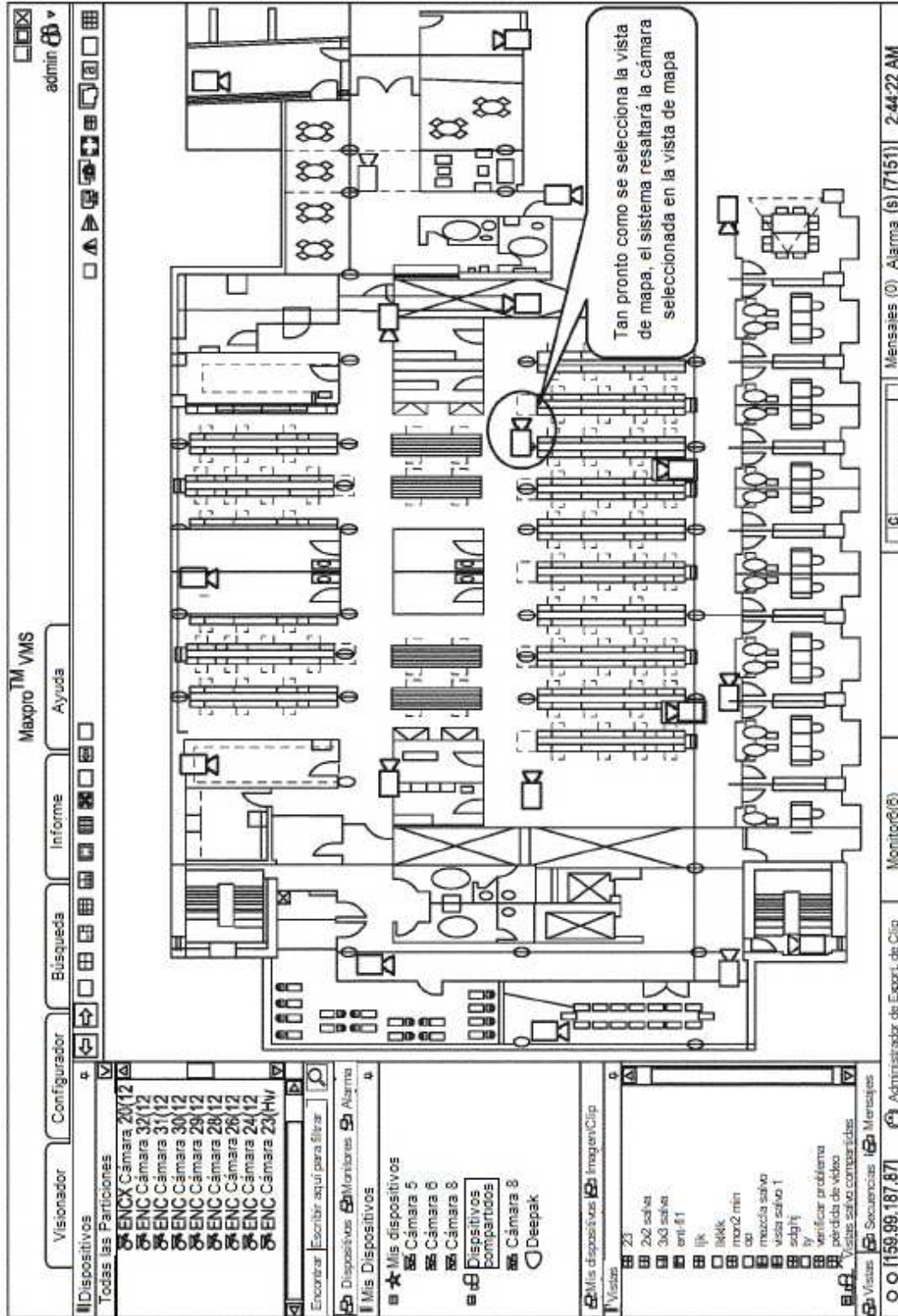


FIG. 3

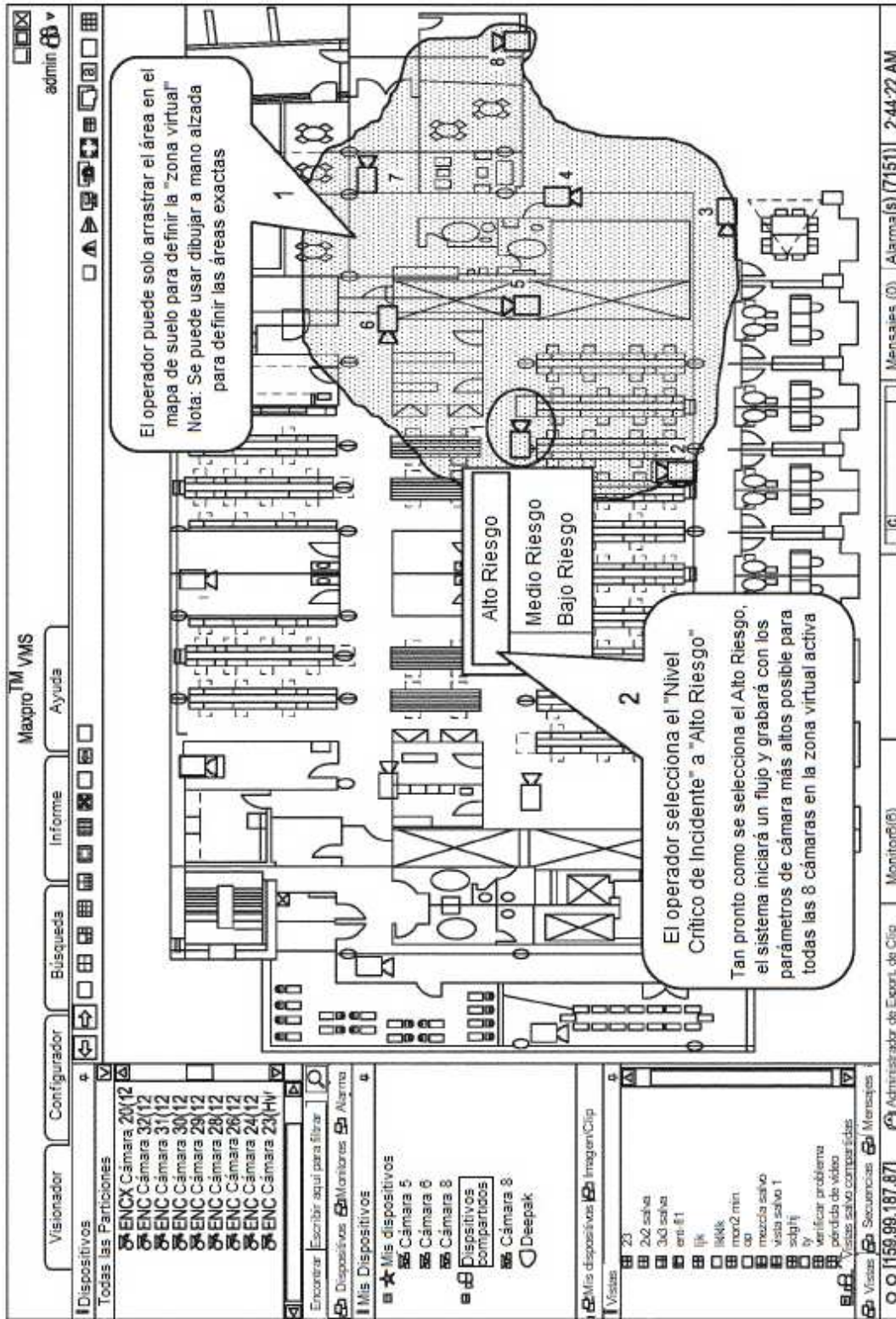


FIG. 4

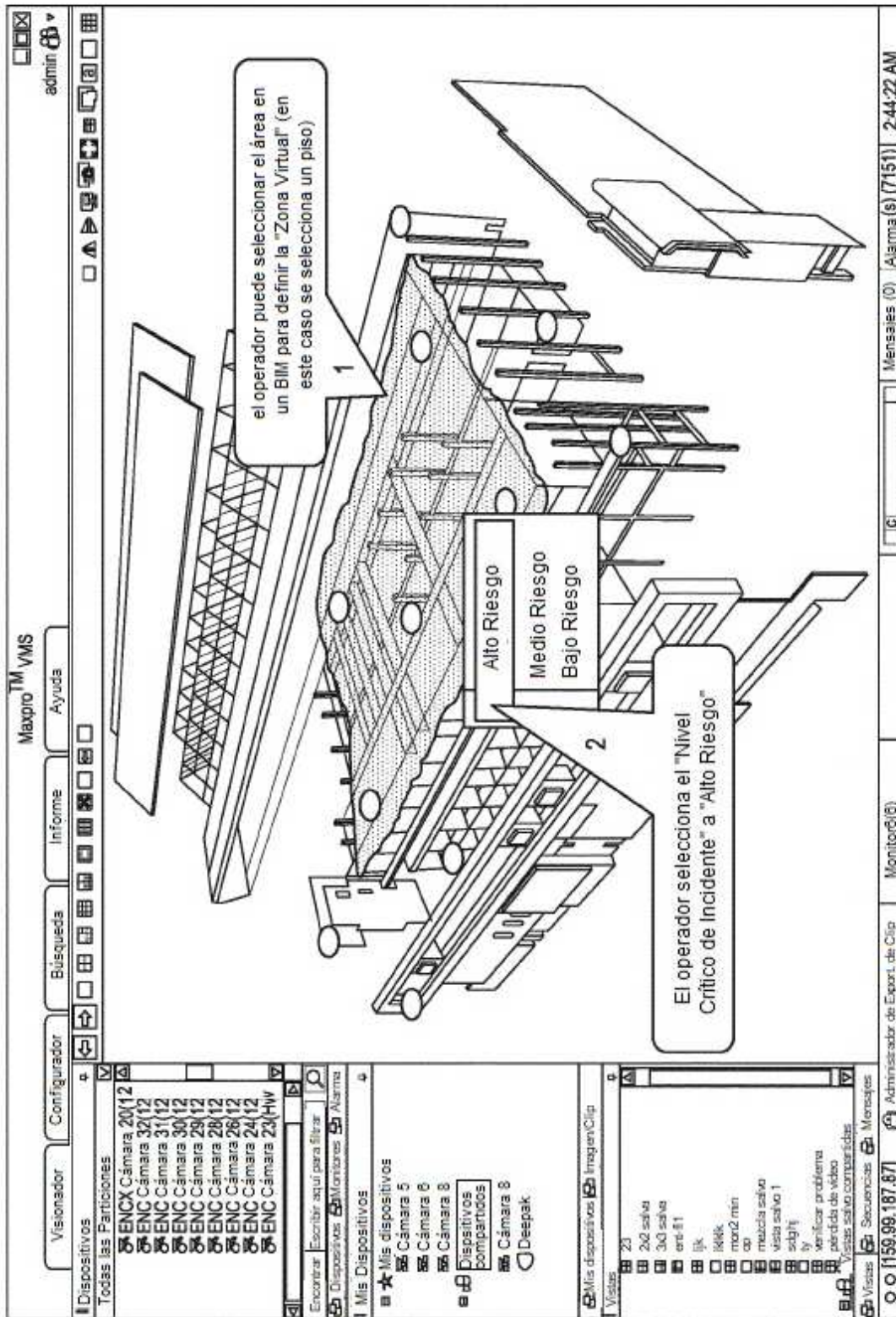


FIG. 5

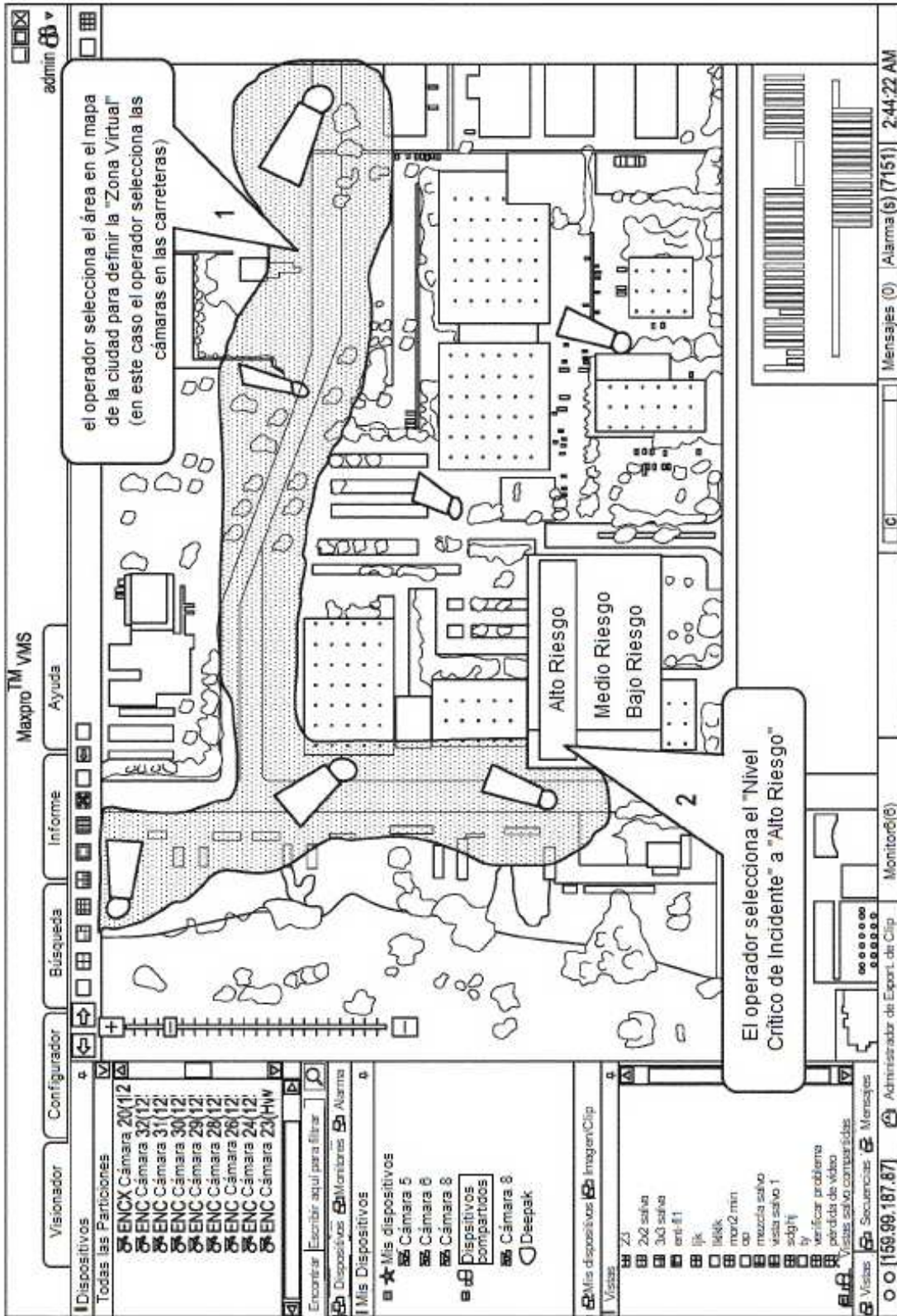


FIG. 6