(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 373 801**

(51) Int. CI.:
G08B 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08161440 .6**
(96) Fecha de presentación: **30.07.2008**
(97) Número de publicación de la solicitud: **2081163**
(97) Fecha de publicación de la solicitud: **22.07.2009**

(54) Título: **SISTEMA DE SEGURIDAD Y MULTI-AMENAZA Y PROCEDIMIENTO DE ESPECIFICACIÓN DEL MISMO.**

(30) Prioridad:
21.01.2008 NL 1034935

(45) Fecha de publicación de la mención BOPI:
08.02.2012

(45) Fecha de la publicación del folleto de la patente:
08.02.2012

(73) Titular/es:
THALES NEDERLAND B.V.
ZUIDELIJKE HAVENWEG 40 P.O. BOX 42
7550 GD HENGELO, NL

(72) Inventor/es:
Hiemstra, Johannes;
Guillot, Antoine;
Koelman, Ger y
Garnier, Bernard

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Sistema de seguridad y protección multi-amenaza y procedimiento de especificación del mismo

La presente revelación pertenece al dominio de los sistemas de seguridad y protección. Más específicamente, cuando el propósito del sistema es asegurar la seguridad y protección de una gran área, el diseño y conceptos operativos así como los equipos y el procesamiento de la información serán de una clase similar a los usados en los sistemas de Comandos, Control, Comunicaciones, Ordenadores, Inteligencia y Vigilancia y Reconocimiento militares (C4ISR). A diferencia de esta última categoría de sistemas, los sistemas de seguridad y protección del tipo de esta invención no tienen el propósito de gestión de operaciones militares. Estos tienen el objetivo de tratar con violaciones de leyes y regulaciones específicas y con cierto tipo de amenazas como el terrorismo, contrabando de drogas, falsificación y daños ambientales. En la mayor parte de países, el trato de estas amenazas es responsabilidad de una o más agencias administrativas o departamentos ministeriales, a veces coordinados por un departamento de seguridad interior. El sistema está basado en una diversidad de sensores de diferentes tecnologías (electromagnéticos, electro ópticos, electro acústicos) tales como los radares, sonar, sistemas de imagen por láser y equipos de comunicaciones tales como la transmisión de VHF. Estos dispositivos están permanentemente posicionados en localizaciones adecuadas o a bordo de un portador. El portador puede ser un vehículo terrestre, por encima o por debajo del agua o una aeronave, todos ellos tripulados o no tripulados, una baliza o un satélite. También es posible que uno o más sub-sistemas específicos también reporten datos de inteligencia recogidos de fuentes tales como la monitorización de las comunicaciones, observación humana sobre el terreno, supervisión del tráfico de Internet o medios similares.

Un dominio privilegiado para el uso de tales sistemas es el de la seguridad y protección ya que todos los riesgos mencionados anteriormente están posiblemente presentes y puede estar involucrado un número significativo de agencias. Pero los sistemas de la técnica anterior tienen limitaciones significativas.

Una primera limitación de los sistemas de la técnica anterior que tienen el propósito de dirigir múltiples amenazas es que los sistemas de monitorización de sensores generalmente procesan pistas instantáneas. Los datos procedentes de múltiples sensores pueden fusionarse y pueden obtenerse los datos de identificación a partir de los Sistemas de Identificación Automática (AIS) que se han hecho obligatorios por la Organización Marítima Internacional (IMO) a bordo de embarcaciones comerciales por encima de un cierto tamaño. Pero luego los operadores y los centros de operación se quedan sin más asistencia para ayudarles a correlacionar los datos de seguimientos instantáneos y de seguimientos no instantáneos, por ejemplo los datos procedentes de diferentes sensores y de fuentes de inteligencia o efectuar comprobaciones de consistencia, analizar las desviaciones de los patrones esperados para detectar anomalías con un suficiente nivel de confianza. La falta de integración de los flujos de datos procedentes de diferentes orígenes tiene la consecuencia de interfaces complejas hombre máquina y de una baja eficacia de los operadores que tienen que tomar decisiones.

Una segunda limitación de los sistemas de la técnica anterior se hace evidente en el instante de diseño de un sistema de esta clase. Estos sistemas son del tipo "un hombre en el bucle" (MITL) en el sentido de que requieren la intervención humana antes de tomar una acción. Como consecuencia, la Interfaz Humano Ordenador (HCI) es incluso más crítica que para otros sistemas para la eficacia del funcionamiento del sistema y sus requisitos de dotación. El procedimiento de especificación normalizado es dirigir los elementos de especificación técnica independientemente de los requisitos operacionales. La falta de integración de las dos categorías de objetivos, entradas y restricciones dará como resultado un rediseño significativo de las diversas etapas para el proyecto y a un sistema sub-optimo al final, en términos de fiabilidad de las alertas y el coste operativo global.

Por ejemplo, el documento WO 2005/124714 desvela un sistema para la detección y presentación de indicaciones de amenazas, incluyendo dicho sistema detectores. Pero este documento de la técnica anterior no desvela el procesamiento de datos de las diferentes clases tales como los seguimientos de radar y las fuentes de inteligencia y el modo en el que debería diseñarse tal sistema, siendo ambas características necesarias para mejorar la eficacia de los operadores.

Por lo tanto, es un propósito de la presente invención superar ambas limitaciones. La invención proporciona un sistema de seguridad y protección que es capaz de integrar datos de seguimientos instantáneos con datos de seguimientos no instantáneos para aumentar la eficacia de los operadores en la asignación de niveles de amenaza a los seguimientos. La adecuación del diseño del sistema a los requisitos operativos de los usuarios se mejora mediante la integración de objetivos organizativos y técnicos y las restricciones en una misma especificación y procedimiento de diseño.

Para estos efectos, las invenciones proporcionan un sistema de seguridad y protección para un área definida que comprende sensores adecuados para capturar un primer conjunto de datos de seguimientos instantáneos sobre un primer conjunto de objetos localizados en dicha área o en la proximidad de la misma, comprendiendo dicho primer conjunto de datos de seguimientos instantáneos al menos un vector de posición en tiempo real y datos de la velocidad desde al menos un sensor sobre al menos uno de los objetos de dicho primer conjunto de objetos, fuentes de información adecuadas para capturar un segundo conjunto de datos de seguimientos no instantáneos sobre un segundo conjunto de objetos caracterizado porque comprende además un conjunto de procedimientos de ordenador

adaptados para correlacionar elementos del primer conjunto de objetos con elementos del segundo conjunto de objetos, comprendiendo dicho segundo conjunto de datos de seguimientos no instantáneos al menos un elemento de información sobre uno de identificación, historia de posición/comportamiento de al menos uno de los objetos de dicho segundo conjunto de objetos, que están en dicho sistema y para calcular niveles de amenaza de los elementos del primer conjunto de objetos de dichos primero y segundo conjuntos de datos asignados a dichos elementos.

También proporciona un procedimiento para el diseño de la especificación de un sistema de seguridad y protección para un área que comprende las etapas de definir a través de al menos una interacción con algunos de los usuarios del sistema las misiones a realizar por el sistema y los recursos adaptados para cumplir dichas misiones caracterizados porque dichos recursos son de un tipo seleccionado a partir de un grupo que comprende al menos sensores, adaptados para adquirir en tiempo real el vector de posición y los datos de velocidad de objetos, fuentes de información adaptadas para adquirir al menos un elemento de información sobre uno de: identificación, historia de posición/comportamiento de al menos un objeto, centros de operación, adaptados para realizar procedimientos de ordenador para correlacionar elementos de un primer conjunto de objetos con elementos de un segundo conjunto de objetos y para calcular los niveles de amenaza de los elementos correlacionados de los dos conjuntos de objetos de la red de comunicaciones y los requisitos de dotación. La invención también tiene la ventaja de proporcionar múltiples herramientas de soporte de decisión a los operadores, estando integradas estas herramientas en una interfaz única de hombre ordenador que se ha diseñado desde el comienzo en base a los requisitos operacionales. También tiene la ventaja de dar mejor control a los usuarios sobre la planificación de presupuestos ya que la definición de los requisitos de dotación se construye en la fase de especificación. El sistema también es muy flexible y versátil ya que la mayor parte de los parámetros de organización pueden configurarse por los usuarios y en algunos casos puede hacerse de forma dinámica.

La invención se entenderá mejor y sus diversas características y ventajas se harán más evidentes a partir de la descripción en delante en este documento de algunas de las posibles realizaciones y a partir de los dibujos adjuntos, entre los cuales:

- la Figura 1 ilustra la disposición de un sistema de seguridad y protección;
- la Figura 2 es un diagrama lógico del funcionamiento de un sistema de seguridad y protección en una realización de la invención;
- la Figura 3 ilustra la arquitectura de procesamiento de información en una realización de la invención;
- las Figuras 4A, 4B, 4C, y 4D son diagramas lógicos del funcionamiento de una detección de anomalías y la función de manejo en varias realizaciones de la invención;
- las Figuras 5A y 5B ilustran el funcionamiento de una violación de una función del área designado en una realización de la invención;
- la Figura 6 es un diagrama lógico de una función de análisis de la cinemática esperada de acuerdo con una realización de la invención;
- las Figuras 7A y 7B ilustran el funcionamiento de una función de análisis de la huella histórica de los seguimientos de acuerdo con una realización de la invención;
- las Figuras 8A, 8B y 8C ilustran el funcionamiento de una función de análisis de riesgos tácticos de acuerdo con una realización de la invención;
- la Figura 9 ilustra el funcionamiento de una función de análisis del patrón de comercio de acuerdo con una realización de la invención;
- las Figuras 10A, 10B y 10C ilustran el funcionamiento de la función de manejo de inteligencia de acuerdo con una realización de la invención;
- las Figuras 11A y 11B ilustran la operación de la función de distribución de inteligencia de acuerdo con una realización de la invención;
- las Figuras 12A y 12B ilustran la organización de conjuntos de trabajo de acuerdo con una realización de la invención;
- la Figura 13 es un diagrama lógico del procedimiento de especificación de acuerdo con la invención;
- la Figura 14 ilustra la especificación de pantallas de dibujos operacionales de acuerdo con una realización de la invención.

En la memoria descriptiva, las reivindicaciones y dibujos, las abreviaturas y acrónimos tienen el significado indicado en la tabla inferior, excepto si se indica otra cosa en el texto.

Abreviatura	**Significado**
AIS	Sistema de Identificación Automática
BU	Baliza
BUC	Caso de Uso de Negocios

(continuación)

Abreviatura	**Significado**
C4ISR	Comandos, Control, Comunicaciones, Ordenadores, Inteligencia, Vigilancia y Reconocimiento
CONOPS	Concepto de Operaciones
COP	Cuadro Operacional Común
COTS	Comercial Fuera de la Plataforma
CPA	Punto más Cercano de Enfoque
CSSS	Sistema de Seguridad y Protección Costera
CW	Aguas Costeras
EA	Electro Acústico
EEZ	Zona Económica Exclusiva
EO	Electro Óptico
ETA	Tiempo de Llegada Estimado
GIS	Sistema de Información Geográfica
GNSS	Sistema Global de Navegación por Satélite
GPS	Sistema de Posicionamiento Global
GUI	Interfaz Gráfica de Usuario
HCI	Interacción Humano Ordenador
IMO	Organización Marítima Internacional
LRIT	Identificación y Seguimiento de Largo Alcance
MITL	Hombre en el Bucle
MMSI	Identidad del Servicio Móvil Marítimo
NOC	Centro de Operaciones Nacional
NUC	No Bajo Comando
POA	Puerto de Llegada
POD	Puerto de Partida
RD	Sensor de Radar
ROC	Centro de Operaciones Regional
ROP	Cuadro Operativo Regional
RDF	Buscador de Dirección Radial
RF	Radio Frecuencia
RSD	Desarrollador de Software Racional
SAR	Radar de Apertura Sintética
SAT	Satélite
SUC	Caso de Uso del Sistema

TTW	Aguas Territoriales
UML	Lenguaje de Modelado Unificado
VoIP	Voz sobre IP
VTMIS	Sistema de Información de Gestión de Tráfico de Barcos
VTS	Servicios de Tráfico de Barcos

La invención puede aplicarse a diferentes tipos de áreas, terrestres o navales, pero su realización preferida es un sistema de seguridad y protección costera (CSSS) o un sistema combinado terrestre y marítimo de seguridad y protección, En partes específicas del mundo como en los mares Mediterráneo, Negro, Rojo y Caribe, así como en Gibraltar, Malaca y estrechos similares, las actividades ilegales tales como el contrabando de drogas y falsificaciones, la inmigración ilegal, las actividades terroristas son bastante sustanciales y tienen la oportunidad de mover un tráfico comercial encubierto muy significativo. Esta clase de contexto es muy exigente en los términos del funcionamiento del sistema que debe poder extraer bajas señales de mucho ruido y correlacionar múltiples fuentes de información. Esto es por lo que esta invención está específicamente dirigida a estas aplicaciones, Pero nada impide aplicarla en otros contextos, aunque la mayor parte de la memoria descriptiva está dedicada a estos.

La Figura 1 es una disposición ilustrativa de un sistema de seguridad y protección costeras (CSSS). El propósito de un CSSS es dar a la autoridad encargada información suficiente y oportuna para contrarrestar las actividades ilegales y dirigirse a una diversidad de amenazas, posiblemente dirigidas a sitios sensibles. Las actividades ilegales tales como el tráfico de drogas, falsificaciones o tráfico de inmigrantes a menudo usan las costas para introducir sus cargas de contrabando en un país porque pueden encontrar en estas, numerosos sitios de escondite y almacenamiento. Amenazas asimétricas específicas pueden dirigirse a puertos, bases navales, plataformas marítimas. En la semántica posterior al 11/9, las amenazas se califican como asimétricas cuando un pequeño número de personas y pobremente equipados, pueden causar un daño significativo a un alto número de personas altamente equipadas. Los escenarios típicos incluirán un pequeño barco pesquero explotando una plataforma marítima de extracción de petróleo o una fragata anclada. La protección frente a amenazas asimétricas es altamente difícil porque nada específico distinguirá a un pequeño barco pesquero tripulado por terroristas cargados con explosivos de las docenas de los barcos vecinos tripulados por un pescador y cargados con peces.

Se han desarrollado varios equipos y sistemas para asegurar la protección frente a riesgos ambientales y la violación de los límites marítimos y para contrarrestar las amenazas asimétricas.

Para monitorizar los barcos comerciales, la Organización Marítima Internacional ha desarrollado un conjunto de normativas con normas de identificación obligatorias y equipos orientados a controlar esta identificación. Estas herramientas se conocen como los Sistemas de Identificación Automática (AIS), 160: el barco 200 está equipado con un transceptor de RF que difunde de forma regular en un ancho de banda asignado señales que transportan datos formateados. El rango de un AIS es de 30-40 kilómetros. Una primera parte de los datos es constante y se introduce manualmente, tal como: la Identificación del Servicio Móvil Marítimo (MMSI) – un identificador único de 9 dígitos de los equipos de RF a bordo, el número IMO, el signo y el nombre de llamada, eslora y manga, una antena fija de localización de posición sobre el barco. La segunda parte de los datos es una entrada variable y se recoge automáticamente por el AIS, en su mayoría a partir de los datos del Sistema Global de Navegación por Satélite (GNSS): la posición del barco con indicación precisa y estado de integridad, sello de tiempo de posición, curso y velocidad sobre la tierra, encabezado, tasa de giro, estado de navegación (tales como No Bajo Comando o NUC, anclado, etc.), con datos adicionales opcionales sobre los ángulos de escora, cabeceo, y balanceo y datos de sensores adicionales a bordo. Una tercera parte se refiere a datos del viaje y a discreción del patrón o cuando se requiera por la autoridad competente: calado del barco, carga peligrosa (tipo y otros datos, como se requiera por la autoridad competente), destino, Tiempo Estimado de Llegada (ETA), puntos de ruta y, opcionalmente, plan de ruta (último campo no proporcionado en el mensaje básico).

Otro tipo de sistema de información cooperativa es la Identificación de Largo Alcance y Seguimiento (LRIT), 150. Este se desarrolló bajo los auspicios de la IMO para proporcionar a través de una red de proveedores del servicio datos de posicionamiento e identificación a los miembros de la red de ámbito mundial. Este será obligatorio para ciertas categorías de barcos el 1 de Junio de 2008.

También se proporcionan diferentes sensores para adquirir datos de seguimiento no cooperativo de barcos por encima o por debajo del agua y aeroplanos. Estos comprenden sensores electromagnéticos, principalmente radar, radar fijos normalizados (RD), 110, radar en vuelo, sensores electro ópticos (EO), 120, tales como dispositivos de láser o de infrarrojos, fijos, transportados por aire o en barcos, dispositivos de búsqueda de la dirección de radio (RDF), 140, sensores electro acústicos (EA), 130, tales como los sonar que también pueden ser fijos o transportados por barco o helicóptero. Los satélites de vigilancia (SAT) equipados con Radar de Apertura Sintética (SAR), 170, pueden también proporcionar información de seguimiento. También las balizas (BU), 180, transportando diversos sensores de corto alcance (pequeños RD, EA) pueden desarrollarse como parte de la vigilancia de sitios sensibles o

reemplazar o suplementar sensores costeros de más largo alcance. La cobertura asegurada por los diversos sensores será una función de su funcionamiento, características del terreno a cubrir (obstáculos naturales, tales como el relieve y los bosques, obstáculos construidos por personas tales como edificios o interferencias de RF) y enlaces de comunicaciones disponibles. Estos factores determinarán la localización óptima de los sensores.

Los datos de los sensores deben procesarse a continuación antes de presentarse a los operadores encargados de interpretarlos. Esto puede hacerse en un equipo de interfaz conectado directamente al sistema y puede haber diferentes localizaciones del extremo de entrada de acondicionamiento / procesamiento de señales / procesamiento de datos de las salidas de los sensores dependiendo del caudal de las señales y la distancia entre los sensores y los centros de operación (Centros de Operaciones Regionales o ROC). Una parte de la especificación del sistema será para seleccionar las herramientas de fusión y clasificación de los datos de los sensores como una función del tipo de objetivos a detectar, identificar y seguir. El funcionamiento de estas herramientas es una parte importante del funcionamiento del sistema como un conjunto pero no un objeto de la presente invención.

Los ROC se atienden por las personas encargadas de correlacionar los datos de seguimiento de los sensores en su área de responsabilidad, integrar estos datos con la información recibida de los subsistemas y fuentes de inteligencia y decidir sobre las acciones a tomar, en base a esta información.

Una primera clase de subsistemas específicamente relevante para un CSSS comprende los Servicios del Tráfico de Barcos (VTS). Los VTS siguen el movimiento de los barcos en un área del puerto y presentan y registran la identificación, transporte, velocidad, ETA, ETD y otros datos relativos a estos seguimientos. Una segunda clase de sub-sistemas que pueden alimentar los datos de seguimiento dentro de un ROC comprende el Sistema de Información de Gestión del Tráfico de Barcos (VTMIS). El VTMIS cubre áreas marítimas mayores y proporciona información más sofisticada tal como la fusión de seguimientos de una pluralidad de sensores (de la misma categoría – es decir radar posicionados en diferentes localizaciones – o de diferentes categorías RD y EA, RD y RDF por ejemplo), cuando capturan el mismo objetivo, integrando datos del radar y del AIS, por ejemplo.

Las fuentes de inteligencia proporcionarán información sobre posibles eventos tales como barcos sospechosos de violaciones pasadas de regulaciones ambientales, fechas esperadas de suministros, localizaciones y actores de operaciones de contrabando, posible acción terrorista. Dependiendo del tamaño y configuración del área a monitorizar, múltiples ROC pueden controlarse ellos mismos por un Centro de Operaciones Nacional (NOC). Será cometido de los operadores de los ROC y NOC correlacionar la información que reciben desde las diferentes fuentes de información para tomar el curso adecuado de acción. Es el objeto de esta invención proporcionar a los operadores de los ROC y posiblemente NOC, con herramientas para automatizar este procedimiento de correlación de fuentes de información.

Como se ilustrado por la parte superior derecha del diagrama lógico de la Figura 2, un sistema de seguridad de área de acuerdo con esta invención procesará los datos de los sensores (procedentes de los sensores RD, RDF, EO, EA, AIS, SAT, BU) 1i0 que se califican como datos de "seguimiento instantáneo" 300 en el sentido de que suministran al sistema, coordenadas y velocidad en 3D del objetivo en tiempo real y presente. Algunos detectores también suministrarán un resultado de la clasificación. Y el AIS 160 dará una identidad supuesta del barco. Estos datos se almacenan temporalmente en una base de datos DB1 y se usan para presentar los seguimientos de objetivos sobre la consola de los operadores en los niveles de VTS, VTMIS, ROC y NOC. Mediante los procedimientos específicos 700, estos datos de seguimiento instantáneo se acondicionan y se almacenan en otra base de datos DB2. Se observará que la DB1 puede ser físicamente la misma base de datos incluso si los datos de seguimiento instantáneo y de seguimiento no instantáneo son lógicamente distintos. Los procedimientos de acondicionamiento tienen el propósito de preparar los datos para su uso en los procedimientos de correlación y evaluación del nivel de amenaza y se describirán adicionalmente con estos procedimientos. En el lado izquierdo del diagrama de la Figura 2, se representa el procesamiento lógico de los datos adquiridos desde las fuentes de inteligencia 400. Dichos datos generalmente vendrán de las agencias de inteligencia bajo una autoridad común con la autoridad que controla los ROC y el NOC, por ejemplo la Armada o los Guardacostas. Pero también pueden venir de agencias bajo la autoridad de otra armada o desde la Junta de Jefes de la Oficina de Personal o de agencias civiles o incluso de fuentes internacionales. Los datos se presentarán en informes escritos de inteligencia 500. Algunos informes pueden ser estructurados, por ejemplo, cuando tratan con eventos bien definidos tales como el suministro de una carga que pueden ser de varios tipos (armas, munición, drogas…) por un barco que puede identificarse exactamente (nombre, bandera, propietario, tripulación…) o identificarse por sólo un subconjunto de estas características. Estos campos pueden introducirse directamente de forma automática en la base de datos DB2. Más frecuentemente, los informes serán no estructurados, es decir con campos de datos no identificados que pueden introducirse automáticamente en una base de datos sin un procesamiento intermedio específico. Se han desarrollado procedimientos de extracción de información y herramientas para este efecto. Tales herramientas se describen en la solicitud de patente EP1364316 asignada a Thales. Dichas herramientas son capaces, después de un procedimiento de aprendizaje, de seleccionar automáticamente los contextos de ejemplos de clases/entidades de información a extraer y también para identificar las relaciones existentes en el texto entre las entidades relevantes. La información puede almacenarse a continuación en una base de datos estructurada por clases de información y/o relaciones. Estas herramientas usarán semánticas y algoritmos de análisis morfo sintáctico con máquinas de estados finitos o transductores. Por supuesto, parte de los informes de inteligencia se introducirán manualmente dentro de la DB2 y se comprobará la consistencia de la entrada automática de datos bien sistemáticamente para algunos campos de datos sensibles o

estadísticamente de modo que el procedimiento de aprendizaje puede mejorarse. El procedimiento de extracción de información 800 comprende tanto subprocesos manuales como automáticos. Podemos ver en la Figura 2 que algunos subsistemas pueden proporcionar dos clases de datos: de seguimiento instantáneo y de seguimiento no instantáneo. Éste es el caso para el VTMIS ya que tales sistemas normalmente registran todos los seguimientos para propósitos de auditoría y esta información puede usarse para alimentar los datos de seguimiento histórico directamente a la DB1. Éste es también el caso del Enlace 11, el Enlace 16, el Enlace 22, el Enlace Y u otro subsistema de enlaces de datos. Estos sistemas de comunicaciones de flota transmiten tanto datos de seguimiento instantáneo como no instantáneo adquiridos por los miembros de la flota para su centro de comandos. Estos datos se almacenarán bien en la DB1 o en la DB2 de acuerdo con las normas prefijadas. Esta variación en la arquitectura y localización de algunas de las funciones no alteran la diferencia en la naturaleza entre los datos de seguimiento instantáneo y no instantáneo y los procedimientos que a continuación interrelacionan a ambos.

Loa procedimientos de correlación 900 se correrán entre la DB1 y la DB2. Pueden usarse diversos tipos de procedimientos de correlación. Un primer tipo de correlación es muy simple, cuando están presentes los mismos datos de identificación en las dos bases de datos. Este es el caso para los datos del AIS, LRIT, VTS, y VTMIS presentes en la DB1 y la DB2 que se califican como "declaratorios". Puede ser el caso para datos de seguimiento instantáneo y datos casi instantáneos, es decir para un barco seguido para el cual los datos serán los mismos en las dos bases de datos para cada uno de los instantes dentro de una estructura de tiempo prefijada. En este caso, los datos se extraerán de la DB2 para correr la comprobación de consistencia descrita en este documento más adelante. También puede ser el caso para otros datos de sensores donde los objetivos tienen una firma no ambigua y pueden identificarse con certeza, por ejemplo por el VTMIS que comprende por sí mismo un procedimiento de firma y de identificación. Un segundo tipo de procedimiento es un procedimiento de clasificación donde los datos de seguimiento instantáneo pasados a la DB1 contienen el tipo de objetivo seguido por el sensor. La clase de objetivo se cotejará con las clases presentes en la DB2 para correr procedimientos de detección de anomalías y manejo que están basados en la desviación del comportamiento normalizado de una clase, tal como las cinemáticas, los riesgos tácticos, las huellas de la historia de seguimientos, la desviación del seguimiento, la evaluación del patrón de comercio, la desviación de los procedimientos de seguimiento normalizados descritos en este documento más adelante. Por supuesto, puede haber diferentes tipos de procedimientos que corren en el propio nivel del ROC dependiendo de qué clase de procedimientos de correlación y fusión están corriendo en el nivel de los subsistemas. Por ejemplo, un VTMIS normalmente proporciona un único seguimiento por objetivo y puede identificar el seguimiento correlacionando dicho seguimiento, posiblemente ayudado por otro tipo de sensor dedicado (EO, EA, IR) con una base de datos de firmas. Pero los mismos procedimientos pueden correr directamente en el nivel del ROC para los datos adquiridos desde sensores conectados directamente a dicho ROC y no a través de un VTMIS. Un tercer tipo de procedimiento es el dedicado a la correlación de los datos de las fuentes de inteligencia y los datos de seguimiento instantáneo. Es posible que los datos de las fuentes de inteligencia contengan datos de identificación no ambiguos, pero raramente éste es el caso. En la mayor parte de los casos, tendrá que correrse un procedimiento de correlación específico. Cuando las fuentes de inteligencia suministran información relacionada con un seguimiento, campos de datos tales como el tipo de transporte, destino esperado, ruta esperada, ventana de tiempo de la llegada esperada en un punto de la trayectoria estarán presentes en la DB2. Los datos de los sensores suministrarán los campos de datos correspondientes. El procedimiento de correlación coteja los campos de datos correspondientes con los soportes de confianza definidos por el usuario y el número de resultados de coincidencia y establece enlaces relacionales entre los informes de inteligencia coincidentes y los seguimientos. Cuando las fuentes de inteligencia suministran datos relacionados no con el seguimiento, el procedimiento de correlación es similar a un procedimiento del segundo tipo descrito en este documento anteriormente pero pueden correr de dos formas: se selecciona una clase de datos de inteligencia y se conectan las clases de seguimientos al mismo; o se selecciona una clase de seguimiento y las clases de informes de inteligencia se conectan al mismo. Se dan ejemplos adicionales en la descripción de los procedimientos de manejo de la inteligencia y distribución.

El nivel de confianza para el resultado del procedimiento de correlación a pasar al procedimiento de análisis del nivel de amenaza se define por el usuario. Se corre un procedimiento de puesta a punto de vez en cuando para asegurar que el nivel de confianza puede garantizarse.

El procedimiento de análisis del nivel de amenaza 100A se corre sobe el subconjunto de los registros de la DB1 que se han correlacionado con los registros de la DB2. Es parte del diseño del sistema asegurar que se capturan todas las amenazas potenciales en escenarios para los cuales la base de datos de seguimientos no instantáneos DB2 comprende los datos de clasificación frente a los cuales pueden compararse los datos de seguimiento instantáneo sobre registros de la DB1. Esta es una ventaja del procedimiento de la memoria descriptiva que se proporciona como parte de la presente invención para proporcionar herramientas para asegurar que esta cobertura de los riesgos es suficiente, no sólo en términos de los sensores sino también en términos del análisis de las categorías de riesgos y objetivos a controlar.

La Figura 3 representa una arquitectura del procesamiento de información en una realización de la invención. La arquitectura comprende tres capas.

El nivel 1 está constituido por los "activos de contribución", es decir las fuentes de datos de seguimiento instantáneo y de seguimiento no instantáneo a utilizar para evaluar el nivel de las amenazas de los diversos objetivos. La lista de estas fuentes de datos de seguimiento instantáneo y no instantáneo se da sólo para propósitos de ilustración:

incluye los sensores in situ, 1i0, VTS, VTMIS, unidades desarrolladas a través las comunicaciones de un enlace 11, 22, ó Y, estaciones terrestres de satélite, centros de análisis, bases de datos, etc.

El nivel 2 se está constituido por la infraestructura o Info-espacio del CSSS. Esta capa proporciona la columna vertebral de distribución de la información, los modelos de datos, una caja de herramientas de conversión de datos, una herramienta de extracción de información, funciones de seguridad (confidencialidad, disponibilidad, integridad), segregación física, cortafuegos, gestión de acceso, certificación e identificación de usuarios (descrita con más detalle en la parte de descripción dedicada a la distribución y manejo de inteligencia), fuentes autorizadas de información, correlación de datos y caja de herramientas de agregación (descritas anteriormente en este documento y facilidades de sistemas tales como la planificación de recursos, gestión y soporte logístico. Una parte de esta capa 2 es de acceso abierto. Otras partes estarán restringidas bien a una lista de usuarios o a clases de usuarios. Como se ha explicado con las normas para la distribución de inteligencia, estas restricciones pueden cambiar dinámicamente, dependiendo de la situación en la cual se opera el CSSS (normal, alerta, intervención…).

El nivel 3 es la capa de aplicación. Esta capa por si misma puede dividirse entre los servicios centrales disponibles para todas las clases de usuarios a través de las diferentes organizaciones de entre las cuales se despliega el CSSS y los servicios específicos de usuario con diferentes tipos de aplicaciones para diferentes clases de usuarios. Por ejemplo, puede ser muy bien que los riesgos ambientales, rescates, anti-contrabando, antiterrorismo, se dirijan por diferentes organizaciones con su propia estructura de ROC y NOC pero que usan los mismos activos de contribución (capa 1) y la misma infraestructura (capa 2). Como se explica más adelante adicionalmente en la descripción tales servicios específicos del usuario pueden implementarse fácilmente en una realización de la invención basada en la definición de conjuntos de trabajo. Pero pueden ser posibles otras implementaciones. Ejemplos de servicios centrales que pueden proporcionarse a todas las clases de usuarios (incluso si el acceso a la propia información puede restringirse) son: soporte de mapas y el sistema de información geográfica (GIS); voz sobre IP (VoIP); difusión de mensajería y alertas. Una parte esencial de los servicios centrales es el Cuadro Operacional Común (COP), la construcción del cual se explica con detalles adicionales más adelante en este documento; en esencia el COP da a los usuarios conocimiento de "quién está dónde" y "quién está haciendo qué" en cualquier sector marítimo (el "quien" que se declara o se detecta), posiblemente con varios indicadores de niveles de amenaza diferentes calculados de acuerdo con la invención; el COP puede incluir la división de la información de la embarcación y del contexto indexado geográficamente entre información permanente (características del barco, rutas de navegación, etc.), información semipermanente (es decir con un ciclo de refresco no en tiempo real tal como la carga, el viaje, la meteorología, zonificación, etc.) e información instantánea (mensajes, fotografías, etc.).

Esta arquitectura está bien adaptada para implementar el procedimiento de calcular los niveles de amenaza a partir de la salida de los procedimientos de correlación descritos anteriormente en este documento.

Puede usarse más de un procedimiento, independientemente o en combinación, para analizar el nivel de amenaza a atribuir a un seguimiento. Una secuencia lógica de un primer tipo de procedimiento basado en la detección de las desviaciones de los comportamientos normalizados se representa sobre las Figuras 4A, 4B y 4C. Como se ve en la Figura 4A, la secuencia operativa global incluye una función de detección de anomalías que dispara en paralelo una función de alerta y una función de análisis de riesgos. Esta función de análisis de riesgos dispara a su vez una lista de acciones. Una de las acciones sistemáticas en la lista es la investigación adicional que vuelve sobre la detección de anomalías bien para confirmar la alerta o para cancelarla, y en este caso posiblemente la actualización de parámetros que han disparado la anomalía. Ejemplos de anomalías incluyen: un barco está en un sitio equivocado; un barco envía una información de AIS incorrecta; un barco de pesca está pescando en un área, dónde, desde inteligencia se sabe que no hay peces; un barco que no se ha visto nunca antes en cierta localización con esa velocidad específica; un barco que no sigue los patrones históricos. Ejemplos de tipos de investigaciones adicionales son: llamar al barco; despachar un observador; realizar una investigación de inteligencia. Como se ilustra en la Figura 4B, la función de detección de anomalías consiste de una diversidad de sub-funciones independientes que tienen todas el mismo propósito, es decir la detección del comportamiento del seguimiento anormal. El comportamiento anormal puede ser un indicador de un ataque terrorista, una actividad de contrabando de drogas u otra actividad ilegal. Esta calificación activa una acción para tomar un vistazo más próximo. Las sub-funciones operan con diferentes entradas y escalas de tiempo. Además de la lista de anomalías el procedimiento produce una medida de la cantidad de trabajo que tiene que hacer un operario. En una situación muy confusa aconsejará añadir un nuevo operario. Puede haber situaciones donde la ausencia de información puede disparar una alerta, Un ejemplo es un perfecto día de pesca sin barcos de pesca. Esto activará una alerta general, no relacionada con un seguimiento. Como se ilustra en la Figura 4C, se detectan anomalías en los datos de enterada por medio de diferentes agentes que trabajan con diferentes datos de entrada y que trabajan sobre una escala de tiempo diferente. A veces, la escala de tiempo es directa (por ejemplo un seguimiento de violación de un área). Otras veces la escala de tiempo es más larga (por ejemplo, barco de pesca han desaparecido en el cuadro de vigilancia). Todos los agentes de detección de anomalías suministran indicadores que pueden estar basados en vectores de probabilidad y analizarse por medio de un motor de razonamiento. La entrada de la función de razonamiento son los indicadores proporcionados por los diferentes agentes. Por ejemplo el indicador de apariencia es un vector de probabilidad para la extrañeza basada en la aparición de un seguimiento. El motor de razonamiento también se proporciona con matrices de mapeo. Un ejemplo de matrices de mapeo se da por la Figura 4D. Estas matrices proporcionan la relación de un indicador con las estimaciones. Por ejemplo, la observación de un seguimiento se expresa en probabilidades P (e | normal) y P (e | ┐ normal). En otras palabras, la probabilidad de que el evento sea

normal y la probabilidad de que el evento no sea normal. A partir de este indicador se deduce la estimación para la anomalía = P (e | A). Esto se hace con la ayuda de las matrices de mapeo.

Las definiciones de las matrices de mapeo son:

P (normal | A) Probabilidad de que un seguimiento con una alta indicación de anomalía tenga un indicador de aparición normal.
P (normal | ¬ A) Probabilidad de que un seguimiento con una baja indicación de anomalía tenga un indicador de aparición normal.
P (¬ normal | A) Probabilidad de que un seguimiento con una alta indicación de anomalía no tenga un indicador de aparición normal.
P (¬ normal | ¬ A) Probabilidad de que un seguimiento con una baja indicación de anomalía no tenga un indicador de aparición normal.

La estimación para la anomalía para el indicador de aparición es:

$$P (e | A) = P (e | normal) * P (normal | A) + P (e | \neg normal) * P (\neg normal | A)$$

$$P (e | \neg A) = P (e | normal) * P (normal | \neg A) + P (e | \neg normal) * P (\neg normal | \neg A)$$

De este modo para cada uno de los indicadores de los diferentes agentes se deduce una estimación de anomalía, llamada

$P (e_1 | A)$, $P (e_1 | \neg A)$, $P (e_2 | A)$, $P (e_2 | \neg A)$, $P (e_3 | A)$, $P (e_3 | \neg A)$, etc. La conversión de las diferentes estimaciones de anomalías a una única estimación se hace de acuerdo con:

$$P (e | A) = P (e_1 | A) * P (e_2 | A) * P (e_3 | A) * \ldots * P (e_n | A)$$

$$P (e | \neg A) = P (e_1 | \neg A) * P (e_2 | \neg A) * P (e_3 | \neg A) * \ldots * P (e_n | \neg A)$$

La estimación normalizada es = P (e | A) / (P (e | A) + P (e | ¬ A)). Se dan resultados de ejemplo en la tabla siguiente:

Indicadores	Observación	P (A)	P (no A)
Aparición	Normal	0,25	0,8
	Improbable	0,75	0,2
Cinemáticas	Larga	0,25	0,8
	Muy corta	0,75	0,2
En área	No en área	0,3	0,9
	En área	0,7	0,1

El resultado representa la probabilidad de un comportamiento anormal para este seguimiento con estos indicadores.

También es posible evaluar un nivel de alerta general. Esta estimación es una medida general de la dificultad de la situación táctica. Por ejemplo, en el caso de seguimientos que son maniobras alrededor del barco o se detectan muchas desviaciones de la huella histórica. Otra situación extraña es cuando una clase completa de objetivos está apareciendo o acaba de desaparecer en comparación con la información de la huella histórica.

Los indicadores para esta estimación son:

Confusión — Este es un indicador para la dificultad en la situación táctica.
Ambiental — Indicador para la situación ambiental
Historia — Indicador para la diferencia con la situación sobre un día normal.
En el caso de que haya una diferencia no esperada en la situación táctica (por ejemplo los botes de pesca han desaparecido, o llenos de turistas, etc.)

Las entradas de confusión son:

- Aparición media — Valor medio de las extrañezas de aparición de todos los objetivos.
- Cinemática media — Valor medio de las extrañezas de cinemáticas de todos los objetivos.
- Áreas — Valor total de todos los seguimientos, que están presentes en las áreas definidas.

Las entradas ambientales son:

- Estado del mar
- Visibilidad

Las entradas de historia son:

- Desviación del tipo de seguimiento: indica para cada uno de los tipos de seguimiento la extrañeza con una situación normal.

En una realización de un sistema de acuerdo con la invención, la función de detección de anomalías puede realizarse a partir de la entrada de una de las siguientes sub-funciones o agentes: comprobación de la validez de la información del AIS; violación de un área de alerta, un área de alarma, un área de exclusión; investigación de las cinemáticas; evaluación de la huella histórica; análisis de riesgos tácticos; desviación del plan de ruta; análisis del patrón de comercio; reconocimiento de encuentros; provocar reacción; desviación del seguimiento normalizado. Pueden añadirse otros agentes a esta lista pero sin embargo caen dentro del alcance de esta invención si funcionan a partir de la correlación de los datos del seguimiento instantáneo y no instantáneo y determinan un nivel de amenaza de un objetivo. La inconsistencia de la información del AIS puede conducir a un aumento en el nivel de amenaza asignado a un seguimiento. Algunos ejemplos de controles a realizar son: tipo de barcos frentes a eslora y manga; Puerto de Salida (POD) y Puerto de Llegada (POA) declarados usualmente no conectados por una ruta comercial; viabilidad del destino y el ETA con respecto al tipo de barco; desplazamiento del ETA (el AIS del barco A se desconecta durante un tiempo y la velocidad media de todo el viaje difiere de los datos calculados anteriormente y después del cierre); número de la IMO respecto al tipo del barco y el nombre del barco; posición del AIS frente a posición del radar; curso frente al plan de ruta; velocidad frente al tipo de barco; tasa de giro frente al tipo de barco; estado de navegación frente la posición y el tipo de barco; peligrosidad de la carga frente a la posición y el destino. Antes de la activación de un aumento en el nivel de la amenaza asignado al seguimiento, podría correrse un segundo control frente a las explicaciones lógicas de una inconsistencia, por ejemplo: errores de configuración; fallo de funcionamiento del equipo de GPS; equipo de GPS antiguo; posición equivocada debido al efecto de multi-trayectoria – especialmente en los puertos. Se marcarán inconsistencias, posiblemente por encima de un umbral definido por el usuario.

Un segundo procedimiento de detección de anomalías se corre frente a áreas prefijadas. Como se ilustra por las Figuras 5A y 5B, el usuario puede definir áreas de alerta, áreas de alarma y áreas de exclusión. Las áreas pueden referirse a un sitio fijo o a un objeto en movimiento. Una alerta se dispara cuando cualquier seguimiento o un seguimiento que se ha calificado como perteneciente a una lista prefijada de clases de seguimiento entran en el área predefinida. Tal evento activará diferentes tipos de acciones dependiendo del área que se viola. Una violación de un área de alerta sólo activará una señal para los operadores en el ROC. Una violación de una zona de peligro puede enviar un mensaje a los medios de intervención en dichas zonas. Un área de exclusión puede activar una intervención automática de medios de disuasión o de combate.

Un tercer procedimiento de detección de anomalías es el procedimiento de investigación cinemática representado en la Figura 6. En esta sub-función, se investigan tres aspectos de un seguimiento: ¿cuál es el comportamiento promedio?, ¿hay un cambio significativo?, ¿cuál es el pronóstico del seguimiento?. En otras palabras, se investigan el estado actual y futuro del seguimiento. Esta investigación involucra las siguientes acciones: evaluación del seguimiento promedio (para una clase determinada de seguimientos); evaluación de velocidad/curso actuales; cálculo del Punto de más Cercano de Aproximación (CPA) de colisión. La evaluación del seguimiento promedio compara la cinemática promedio de un seguimiento para una clase de barcos seleccionados a partir de la DB1 (inteligencia de Cinemáticas) como coincidencia de la clase de seguimientos de la DB2. Para cada una de las clases, está disponible la información concerniente al comportamiento de la cinemática "esperada". Por ejemplo, cuando un barco que pertenece a la clase de barcos de pesca tiene una velocidad promedio de 10 nudos y una máxima de 25 nudos, una velocidad promedio de 20 nudos para un seguimiento clasificado como un seguimiento de un barco de pesca activará un aumento en el nivel de amenaza para este seguimiento. La velocidad/curso actuales pueden evaluarse con respecto a la historia del seguimiento para detectar cambios cinemáticos. En combinación con la información de inteligencia de cinemáticas, un cambio observado puede indicarse como significativo o dentro de un comportamiento normal. Un avión de línea aérea haciendo una maniobra con una aceleración de 2g se considerará como anormal mientras que la misma maniobra por un caza de combate se considerará como normal. Las cinemáticas actuales también pueden compararse con los límites de frontera de una clase de seguimientos.

Un cuarto procedimiento de detección de anomalías es la historia de huellas del procedimiento de investigación de seguimientos que se pone de ejemplo por las Figuras 7A y 7B. Esta es un medio para capturar y aprender los patrones de comportamiento normal y comparar el comportamiento real de un seguimiento frente al comportamiento normal basado en la historia. Por ejemplo, es conocido en qué posiciones aparecen normalmente los seguimientos por primera vez (puerto o rompiente del mar de playa); Un seguimiento que aparece en primer lugar en otra localización se considerará anormal (véase la Figura 7A). Para comparar el comportamiento de un seguimiento con los patrones locales, se crea una huella y se almacena en la DB2. Esta huella (véase la Figura 7B) es un mapa digitalizado, llamado huella histórica, que contiene información sobre los seguimientos observados en el área de interés. El área se divide en células cuadradas, por ejemplo de 250 metros de lado. Cada una de las células contiene por ejemplo información de los promedios y las desviaciones estándar, el número de apariciones de

seguimientos, velocidad, curso y apariciones de seguimiento iniciales. Esta información se proporciona para cada una de las clases de barcos (mercante, de pesca, de vela u otro tipo de barco). La huella histórica de los seguimientos se mantiene automáticamente por el almacenamiento del procedimiento de datos de seguimientos históricos y no requiere ningún apoyo por el operador. La huella histórica contiene información de todos los seguimientos en el área de interés y de este modo es una fuente dinámica de inteligencia. El sistema proporciona indicaciones sobre la madurez (número de cambios) y estado de carreras (número de mediciones más altas que un umbral). Los datos de los seguimientos históricos se usan para determinar las siguientes indicaciones: la probabilidad de que los seguimientos puedan estar presentes en cierta posición; la probabilidad de que los seguimientos puedan verse por primera vez en una cierta posición; la posición cinemática normal en una cierta posición. El procedimiento compara las cinemáticas actuales con la huella histórica y determina: la aparición del seguimiento (cuán extraño es encontrar un seguimiento en una cierta posición, en base a la comparación con varios seguimientos grabados en la huella histórica); la aparición inicial del seguimiento (cuán extraño es detectar un seguimiento sobre una cierta posición, en base a las áreas de detección grabadas en la huella histórica); apariencia del curso (cuán extraño es un curso de seguimiento en esa posición, en base al curso medio y la desviación estándar); apariencia de la velocidad (cuán extraño es una velocidad de seguimiento sobre esa posición, en base a una comparación para la velocidad media y la desviación estándar).

Un quinto procedimiento de detección de anomalías es un análisis de riesgos tácticos ilustrado por las Figuras 8A, 8B y 8C. Tomamos el ejemplo de un ataque terrorista, probablemente se realizará al amparo de objetos naturales o de oportunidad de modo que el descubrimiento del ataque sea lo más tarde posible. Detrás de estos objetos, la probabilidad de detectar un seguimiento ciertamente es mucho más pequeña. El área detrás de tal objeto se identifica como una zona ciega. Una vez que el seguimiento deja la zona ciega, está a vista abierta y visible por los sensores. Por esta razón el sistema asigna sistemáticamente zonas de peligro a las que están alrededor de una zona ciega. Los objetos usados como zonas ciegas pueden ser un seguimiento o una parte de un entorno natural. Se corre un procedimiento específico para cada una de las clases de objetos; todos los procedimientos se basan en el análisis de mapas y el análisis de seguimientos. El análisis de mapas se basa en los mapas náuticos digitales disponibles y los mapas terrestres. Cuando se detecta una zona ciega tal como una montaña, el área próxima a la zona ciega se marca como una zona peligrosa. El tamaño de una zona de peligro se determina por los ajustes por defecto. Cuando se observa un seguimiento, el procedimiento de análisis del seguimiento evalúa si este objeto puede usarse como cobertura por otro objeto. El seguimiento encubierto puede estar detrás del primer objeto, enmascarado bien físicamente o electromagnéticamente. Puede definirse una o más zonas de peligro para un seguimiento definido.

Un sexto procedimiento de detección de anomalías es la desviación del plan de ruta. Por supuesto, éste sólo está disponible para objetivos que han transmitido un plan de ruta. La transmisión generalmente se hará a través del AIS como se indicó anteriormente en este documento. El procedimiento compara la posición esperada del seguimiento y la real. La desviación puede ser una diferencia en el tiempo (el seguimiento es correcto pero retardado debido a una salida posterior o a una diferencia de las condiciones en la ruta). También puede ser una diferencia en la posición aunque la ruta se ha seguido con puntualidad hasta un momento en el tiempo.

Un séptimo procedimiento de detección de anomalías es el análisis de patrones de comercio. Este procedimiento se basa en la comparación de los datos del seguimiento instantáneo con los patrones de comercio almacenados en la DB2 para varias clases de barcos que transportan una cierta carga. Como se ilustra en la Figura 9, el sistema produce un histograma que comprende los puertos de origen y destino, la carga, el número de barcos que transportan esta carga. El histograma depende de la estación para reflejar el hecho de que el comercio es por sí mismo estacional. Un octavo procedimiento de detección de anomalías es el reconocimiento de encuentros. Esta funcionalidad determina la probabilidad de seguimientos que tienen un encuentro. Un encuentro en el mar puede usarse por los contrabandistas de droga para cargar las drogas desde un barco más grande a un barco más pequeño que puede aproximarse más fácilmente a la costa o transferir su carga a otro barco. Es probable un encuentro en una de las siguientes circunstancias: barcos que están juntos; barcos que tienen la misma velocidad; barcos que tienen la misma dirección; velocidad decreciente y/o cambio de curso en un sitio pasado de otro recorrido.

Un noveno procedimiento de detección de anomalías es la obtención de reacción. En casos en los que un operador despacha a un observador a cierta localización en la forma de un activo propio (bote inflable, helicóptero, aeroplano, barco de la armada, etc.), el sistema soporta la evaluación por el operario de la reacción de los seguimientos. Una reacción normal es ningún cambio de comportamiento a la vista de un vehículo de patrulla. Un cambio en el comportamiento (cambio de curso o de velocidad) se considera anormal a primera vista.

Un décimo procedimiento de detección de anomalías es la desviación del patrón de seguimiento estándar. Las clases de barcos siguen diferentes tipos de seguimientos. Por ejemplo un barco de pesca sigue las trayectorias conocidas de los peces, un ferri tiene una trayectoria fija y un horario; un barco de vela vira frente al viento. El seguimiento de un objetivo que se considera que pertenece a una clase con un patrón de seguimiento estándar coincidirá con el estándar y se analizará la desviación. Para realizar esta función, puede ayudarse de la clasificación de objetivos mediante sensores por otros procedimientos de correlación tales como: la altura del barco desde la distancia de la primera aparición; la posición del barco con respecto a la huella histórica; la falta de información del AIS, etc.

Después de que se ha realizado un procedimiento de detección de una anomalía, se corre un procedimiento de análisis de riesgos. Este procedimiento analiza el daño potencial en el caso de un seguimiento que tiene intenciones hostiles. Esto se combinará con el nivel de confianza de la identificación y la intención. Por ejemplo, si es un barco conocido que se ha comprobado con certeza que no hay ninguna posibilidad de que se haya secuestrado debido a un contacto de radio reciente no ambiguo, el nivel de amenaza concerniente a explosión se marcará como bajo, incluso si el nivel de daño posible causado en el caso de una explosión puede ser muy alto. La salida de este procedimiento es una lista de seguimientos clasificados por el nivel de amenaza para cada una de las categorías de amenaza (violación de la ley de varios tipos, ataque terrorista; peligro ambiental, etc.). A cada una de las categorías puede otorgarse una ponderación diferente en diferentes circunstancias (es decir: los informes de inteligencia llaman la atención de posibles eventos específicos, el nivel de alerta general basado en amenazas esperadas, etc.) y la lista variará consecuentemente. Los seguimientos amenazadores de mayor prioridad merecerán una investigación más cercana para alcanzar un nivel más alto de confianza para la información de identificación, intención y antecedentes. El operador en el ROC será capaz de este modo de centrarse en las tareas prioritarias y seleccionar más fácilmente una de las acciones a su disposición: llamar al barco por radio, despachar un observador, realizar una investigación de inteligencia.

Como ya se ha mencionado, los procedimientos de detección de anomalías pueden realizarse bien individualmente o secuencialmente o en paralelo. En los dos casos últimos, los resultados de cada uno de los agentes individuales de detección de anomalías y procedimientos de análisis de riesgos se combinarán usando el motor de razonamiento descrito anteriormente en este documento.

Otra categoría de procedimiento de análisis del nivel de amenaza está basado en los informes de inteligencia y la información extraída de los mismos. El manejo de la información de inteligencia y su uso en el procedimiento del análisis del nivel de amenaza puede variar enormemente de una realización a otra por diferentes razones, determinadas significativamente por la organización de las funciones de seguridad y protección en el país donde se despliega el sistema. La Figura 10A ilustra un sistema con varios ROC (ROC1, ROC2, … ROCn) coordinados por un NOC con agencias externas proporcionando información de inteligencia a diversos niveles (Regional, nacional) y Compiladores de Comms/Intel encargados del manejo de la información de inteligencia. Como ya se ha mencionado, los informes de inteligencia pueden introducirse manualmente en la DB2 o los registros de datos a almacenar en esta base de datos se extraen automáticamente a partir de los informes usando algoritmos dedicados a la extracción de información desde un texto estructurado o no estructurado. En el contexto de la extracción automática, el compilador se encargará con el establecimiento de los parámetros y el control del nivel de confianza de los resultados de la extracción de información. Las fuentes de inteligencia pueden ser bastantes diversas: correos electrónicos, voz, bases de datos internas o externas, Internet, agencias externas, fotografías, imágenes de satélite, noticias. Desde el punto de vista del diseño del sistema, la principal consideración será entonces conocer si los datos de inteligencia a utilizar dependen del seguimiento o no. El manejo de la información relacionada con el seguimiento se ilustra en la Figura 10B. Cada uno de los seguimientos en la DB1 está enlazado a una estructura en la DB2 donde se almacena la información de inteligencia para el seguimiento correlacionado. La definición de esta estructura se hace por un mantenedor que tiene uno de los papeles definidos en los ROC y el NOC (véase más adelante en este documento). En este caso, se establecerán los enlaces entre los seguimientos y los datos de inteligencia relacionados. La información enlazada con los seguimientos puede filtrarse sobre cualquiera de los campos de datos almacenados (fuente de datos: frescura, categoría de amenaza, etc.). El manejo de la inteligencia no relacionada con los seguimientos se ilustra en la Figura 10C. Normalmente, esta categoría de datos proporciona más información de antecedentes acerca de la situación táctica. Algunos ejemplos son: se ha robado el barco de pesca "Liberar a Whilly"; se ha informado de un transporte de droga, cuidado con el buque cisterna Exxon Valdez…El operador puede parametrizar una petición automática o definirla manualmente para buscarla en la DB2 para cierta información definida como parámetros de alerta, por ejemplo: tipo de eventos ilegales o amenazadores que se supone que ocurren en el área monitorizada en una ventana de tiempo; todos los barcos sospechosos, los barcos sospechosos de un cierto tipo… Y los resultados de estas peticiones se enlazarán con los seguimientos correspondientes que coinciden en los campos de inteligencia. Por supuesto, la información de inteligencia no relacionada con el seguimiento es dependiente del tiempo y debe retirarse cuando está anticuada.

El nivel de amenaza puede calcularse a continuación en base sólo a los datos de inteligencia enlazados a los seguimientos o en base a estos datos en combinación con cualquiera o todos los procedimientos de detección de anomalías descritos anteriormente. La posible combinación se realiza también por un motor de razonamiento, considerando las diversas fuentes de inteligencia consideradas relevantes para el seguimiento como un agente que saca indicadores al motor.

Cuando se manejan datos de inteligencia u otra clase de datos sensibles, es importante implementar normas de distribución que se definen por la autoridad suprema que controla el sistema. En realizaciones específicas de esta invención se definen normas de distribución tanto en base a los criterios geográficos que definen las áreas de responsabilidad y las áreas de interés como en base a los atributos de los propios datos. Los criterios geográficos se ilustran por la Figura 11A. Las áreas de interés son solapantes porque la información acerca de los barcos entrantes puede ser de interés para más de un ROC al mismo tiempo, incluso aunque la responsabilidad de las acciones a dirigir sea sólo para uno de ellos. Cada una de las áreas de interés se define por un polígono y la correspondiente política de distribución se implementa por medio de un filtro. El filtro de los atributos de la información se ilustra por la Figura 11B. El filtro se basa en una matriz con la lista de usuarios del sistema como primera coordenada y una

lista de atributos de información como una segunda coordenada. Los atributos de información relevante pueden ser los propios puntos de cruce de otra matriz que comprende como primera coordenada el tipo de información y como segunda coordenada la fuente de información. En realidad, algunas fuentes de inteligencia sólo aceptan distribuir su información bajos la condición de que su distribución se controla incluso dentro de la organización de un receptor permitido. El filtro se implementa en base a la combinación de células de la matriz. Las células de la matriz pueden incluir valores dinámicos definidos como una función, por ejemplo, de modos de operación. De este modo, las áreas de interés y la distribución selectiva serán diferentes entre un modo de monitorización normalizado, un modo de alerta general y un modo de intervención de crisis. Pueden definirse otras normas de distribución dinámicas.

Cuando el procedimiento de análisis del nivel de amenaza ha suministrado sus resultados, los datos fijados para construir el Cuadro Operativo Común (COP), 200A están completos. El COP es un cuadro operativo del área compuesto por ordenador. Se observará que el procedimiento de construcción del COP es un procedimiento dinámico. Un primer COP estará listo para presentarse a los operadores incluso antes de que se hayan completado todos los procedimientos de correlación y el análisis del nivel de amenaza. El COP se actualiza bien cuando están disponibles resultados frescos o periódicamente. Una variable definida por el usuario puede fijar el nivel de cambio en los parámetros claves de cada una de las situaciones que activará un refresco del COP, de modo que la tasa de cambio no cree inestabilidad de los datos y las representaciones. Otra variable definida por el usuario puede fijar el nivel de amenaza mínimo a presentar como parte del COP como una función del ordenador disponible y las capacidades de representación.

En una de las realizaciones de la invención, se presentarán los subconjuntos del COP en pantallas para los diversos tipos de operadores en los niveles del ROC y NOC. Como se explicará adicionalmente cuando se presente el diseño y el procedimiento de la memoria descriptiva para construir un sistema de acuerdo con la invención, los papeles de los operadores son un elemento clave que define una lista de tareas a cumplir por los diversos operadores con papeles atribuidos para cumplir una misión. El diseño de las pantallas se deduce a partir del Concepto de Operaciones (CONOPS) que saca varios Modos de Funcionamiento y un Concepto de Dotación para el funcionamiento del sistema. En base a la Misión Operacional y el análisis de Tareas, se definen los Papeles de los Operadores y a continuación se mapean a los Modos de Operación aplicables. El CONOPS también define un mapeo entre los Papeles de los Operadores y las Tareas Operacionales. En base a este mapeo, las Funciones del Sistema se asignan a los Papeles de los Operadores, definiendo de este modo qué operador necesitará qué funciones. En la práctica, los temas de autorización pueden implicar que cierta información y funciones se restrinjan a Papeles específicos o incluso se limiten a circunstancias operacionales específicas. Todos estos factores determinan los parámetros de los Conjuntos de trabajo 300A. Por consiguiente, el análisis operacional también da la penetración cuando un operador necesita información y las funciones del sistema. A pesar de todos los esfuerzos durante este análisis inicial, la práctica diaria puede mostrar que la carga de trabajo no está equilibrada suficientemente entre los Papeles. También, la organización puede cambiar con el tiempo e introducir nuevos Papeles o cambios de responsabilidades de los existentes. Por estas razones, el sistema de acuerdo con la invención comprende varios mecanismos flexibles a concertar con una nueva organización, nuevos requisitos de autorización o una nueva división de tareas entre los operadores. En un modo estándar, los usuarios del sistema tienen que registrarse por su nombre de usuario y contraseña. Estas pueden reemplazarse por una tarjeta inteligente con un código pin o con un dispositivo de control de acceso biométrico (huella dactilar, reconocimiento de cara o de pupila o similares). También pueden combinarse el código pin con la biométrica. Cualquier procedimiento del control de acceso que se realice, el registro de entrada determina que Papeles pueden realizarse por el operador. Después del registro de entrada, el sistema permite al usuario sólo uno seleccionado de los Papeles para el cual está autorizado. El sistema permite la definición flexible de esta autorización del usuario. Cuando un usuario ha seleccionado un Papel, el sistema configura su entorno de trabajo proporcionando varios Conjuntos de trabajo. Cada uno de los Conjuntos de trabajo es un conjunto coherente de funciones y de información que necesita un usuario para cumplir una tarea específica o conjunto de tareas. Estas funciones están dispuestas sobre la pantalla de un modo que fija el flujo de trabajo de las tareas soportadas. El sistema permite la asignación de Conjuntos de trabajo a los Papeles. La organización puede usar el sistema en diferentes Modos Operacionales, como el Modo Normal, el Modo de Emergencia, el Modo de Entrenamiento y el Modo de Mantenimiento. El Modo Operacional seleccionado determina qué Papeles están disponibles sobre el sistema y cuáles no. El número de Modos Operacionales puede extenderse definiendo un nuevo Modo Operacional y asignando un conjunto de Papeles a este modo. Esto permite a la autoridad gestionar el sistema para predefinir configuraciones organizativas para diversas clases de situaciones operacionales. Usando este mecanismo, ilustrado por la Figura 12A, la organización puede adaptarse por sí misma a la carga de trabajo actual. En los diferentes Modos Operacionales, la Asignación de Tareas a los Papeles (y de este modo los Conjuntos de trabajo a los Papeles) puede diferir para distribuir siempre el trabajo sobre los operadores en un modo equilibrado. La organización flexible del sistema permite el equilibrio de la carga de trabajo por la selección del estado de acción apropiado, añadiendo operadores extra que usan consolas separadas o seleccionando diferentes papeles que proporcionan la división requerida de tareas en la situación actual. La información que se usa para estas decisiones puede ser por ejemplo: el número actual y tipo de seguimientos en el área de interés, el número actual, el tamaño y la naturaleza de los incidentes actuales; la anticipación basada en el tiempo del día (datos históricos acerca del número esperado de seguimientos e incidentes); la anticipación en base a los datos de inteligencia (tipo esperado y tamaño de los incidentes). En centros con una fuerte carga de trabajo, esta función de equilibrado de las cargas de trabajo será propiamente un Papel definido con un Conjunto de trabajo atribuido. Las funciones pueden asignarse a los Conjuntos de trabajo. En esta definición, las posiciones de las

pantallas de las ventanas principales y sub-ventanas también pueden especificarse. La representación de la función sobre una pantalla puede establecerse que sea bien automática o manual. En una realización diferente, las funciones pueden asignarse directamente a un Papel y seleccionarse independientemente de los Conjuntos de trabajo actuales. Estos modos diferentes de asignación de los Conjuntos de trabajo se ilustran en la figura 12B.

La Figura 13 ilustra el procedimiento por el cual la invención está mejor especificada y diseñada. Este procedimiento se basa en el enfoque del Concepto de Operaciones (CONOPS) pero es único en el sentido de que junta todos los aspectos operacionales y de alto nivel técnico que son importantes para los usuarios del sistema para poder juzgar el sistema propuesto sobre criterios tales como: idoneidad para todos los propósitos pretendidos; cobertura de todos los propósitos pretendidos; consecuencias organizativas de la introducción del sistema; requisitos de dotación; entrenamiento y esfuerzos logísticos. En una realización específica del procedimiento de acuerdo con la invención la documentación de CONOPS incluye los elementos listados en la Figura 13.

Los capítulos principales del CONOPS, que pueden verse como muchas fases o etapas de la especificación del sistema serán: el Establecimiento del Proyecto, la Solución Propuesta, el Entorno de Soporte Propuesto, el Concepto Operativo y los escenarios Operacionales. Puede usarse otra redacción por ejemplo si el procedimiento de acuerdo con la invención se usa para describir un sistema existente como un modo de invertir el ingeniero su especificación en el contexto de una evaluación de su eficacia operativa antes de que se tome la decisión de corregir o rediseñar el sistema existente.

Se observará que los diferentes procedimientos detallados pueden usarse para recoger las entradas necesarias para alimentar estos capítulos, deducir conclusiones y tenerlos validados por los representantes autorizados de los usuarios. La información a introducir se puede recoger bien mediante un cuestionario, mediante un cara a cara o entrevistas telefónicas. También puede introducirse directamente por los usuarios dentro de un sistema de ordenador proporcionado con una interfaz y controles adecuados. La salida generalmente se producirá manualmente por el personal de diseño del sistema. Pero algunas salidas, como los gráficos construidos directamente a partir de la entrada, pueden producirse automáticamente. La validación puede hacerse también mediante una entrevista o la entrada de algunos usuarios en el sistema de ordenador. Hay un orden lógico usado para realizar las etapas del procedimiento, que se describen sobre la Figura 13. El orden es principalmente secuencial, con la advertencia de que la Solución Propuesta puede afinarse después de que los usuarios hayan revisado los Escenarios Operacionales. En la descripción de las etapas del procedimiento de acuerdo con la invención que sigue, el "subsistema" debe entenderse que comprende sensores, VTS, VTMIS, Enlaces y centros de control.

La etapa de Exposición del Proyecto comprende sub-etapas tales como:

- Misiones: todas las misiones para las cuales la organización al cargo del sistema es responsable;

- Situación actual: Organización (estructura actual de la organización y relaciones con las organizaciones externas que están involucradas en el cumplimiento de las misiones). El equipo legado (resumen de la infraestructura actual y el equipo que está disponible y debería posiblemente integrarse en el nuevo sistema); Activos Propios (resumen de los activos actuales que están disponibles o que se comprarán independientemente por la organización); Entorno (aspectos ambientales como el Clima y la Geografía); Antecedentes (política relevante y aspectos industriales): evaluación de la situación Operacional (resumen de áreas relacionadas geográficamente y amenazas que son importantes con respecto a las Misiones definidas); Asunciones (realizadas por las soluciones Propuestas); Limitaciones (alcance que se aplica a las soluciones Propuestas, por ejemplo la exclusión de algunas áreas); efectos Esperados (beneficios para los usuarios del sistema, en comparación con la situación actual).

La etapa de las soluciones Propuestas comprende sub-etapas tales como:

Propósito (Papeles del sistema);

- Organización propuesta (descripción de la estructura de la organización propuesta con sus nodos operacionales principales tales como los ROC, NOC, sus relaciones y responsabilidades);
- Sistema propuesto (descripción de los tipos de sistema y subsistema, tales como los diferentes tipos de sensores y VTMIS, y funcionalidades);
- Localizaciones (de subsistemas y de centros de operaciones; esta parte incluye los resultados del estudio de cobertura por sensores);
- Tipos de configuración del subsistema (configuración exacta del subsistema);
- Asignaciones del tipo de subsistema (asignación de los subsistemas, a saber sensores, para las localizaciones seleccionadas);
- Conectividad del Nodo Operacional (identificación de las relaciones y flujos de información entre los Nodos Operacionales);
- Fases del proyecto (descripción del escalonamiento propuesto de la introducción del nuevo sistema).

La etapa del concepto de Operación comprende sub-etapas tales como:

- Operaciones del sistema (resumen de las principales operaciones que están provistas realizar por la organización que usa el sistema);
- Análisis de la organización y las tareas: el análisis de la organización (para cada una de las regiones en el área a cubrir por el sistema, se identifican los Nodos Operacionales, agencias y organizaciones externas y activos involucrados en el funcionamiento de cada una de las Misiones); Tareas Operacionales (descripción de las diferentes fases del trabajo y etapas del procedimiento en la realización de una misión); Tareas para las asignaciones a los Nodos (Tareas que se realizarán para conseguir una misión que está asignada a los Nodos Operacionales identificados y las fases de trabajo identificadas); Papeles de los Operadores (identificación de los diferentes tipos de operadores en la nueva organización); Tareas para las asignaciones de Papeles (asignación de las Tareas Operacionales identificadas a los Papeles de los Operadores);
- Modos de Operación: descripción de los Modos (identificación de los diferentes modos de operación en los que la organización estará usando el sistema; esta definición puede combinar estados de alerta operacionales de la organización con estados del sistema; concepto de Dotación (descripción de las configuraciones de dotación necesarias en los diferentes modos de operación identificados);
- Temas esperados y planes de reserva (descripción de las configuraciones de dotación necesarias en situaciones más extraordinarias, por ejemplo un Nodo Operacional reemplazando otro Nodo Operacional que ha pasado a no disponible).

La etapa de soporte ambiental Propuesto comprende sub-etapas tales como:

- Logística (resumen de alto nivel del entorno de soporte logístico);
- Entrenamiento y soporte en operación (resumen de alto nivel de los conceptos de entrenamiento y soporte en funcionamiento)

La etapa de los escenarios Operacionales consiste principalmente en describir varios escenarios de operación que ilustran el papel de la organización y el sistema propuesto en la realización de las misiones identificadas.

Esta realización del procedimiento de la invención descrito anteriormente integra en la fase de especificación las necesidades organizativas y técnicas de los usuarios. Haciendo esto se posibilita al diseñador del sistema asegurar que los sensores, las fuentes de inteligencia, las herramientas de soporte de decisión, los conjuntos de trabajo, los Nodos Operacionales y el personal están planificados en el modo que corresponde a la cobertura de la misión pretendida. Más específicamente, el modelado combinado de las operaciones del sistema con la integración en una única HCI de la información de los sensores, las herramientas de inteligencia y de soporte de decisión, usando un grupo definido de tecnologías, permitirá a los usuarios entender cuál será el nivel de confianza que puedan alcanzar del procesamiento de datos automático en comparación con la interpretación de datos manual. A continuación podrán definir los Modos de Operación y los requisitos de personal correspondientes con un nivel de confianza inusual, cuando se compara con los procedimientos y sistema de la técnica anterior. Los requisitos de personal para los Nodos Operacionales y los subsistemas en cada uno de los Modos de Operación se determinarán a partir de las salidas de la sub-etapa de los análisis de la Organización y tareas tales como las matrices de asignación de las Tareas a los Nodos y de las Tareas a los Papeles. Estos serán la base para el presupuesto de los recursos humanos necesarios para atender los Nodos Operacionales y los subsistemas cuando se combina con las definiciones del tiempo necesario para realizar cada una de las Tareas y las restricciones del entorno de trabajo (horas de trabajo, asignación de vacaciones, etc.).

En una realización de la invención, las etapas específicas se realizan para definir la HCI del sistema. La invención como conjunto es única en el sentido de que enfoca los aspectos operacionales del sistema en vez de la arquitectura hardware y software como los procedimientos de la técnica anterior. La parte de la HCI del procedimiento de especificación se ilustra en la Figura 11. Comienza a partir de las salidas de la etapa de la Declaración del Proyecto de realización del procedimiento de acuerdo con la invención descrita anteriormente en ese punto. El procedimiento usa diagramas del Lenguaje de Modelado Unificado (ULM) bien conocidos por los especialistas en la técnica de diseño de software. El procedimiento encaja en el concepto de definición de una interfaz de usuario flexible. El modelo resultante representa un sistema genérico con todos los subsistemas y funciones disponibles. Por supuesto, para un sistema específico a suministrar a un conjunto definido de usuarios, algunos de los subsistemas y funciones disponibles pueden dejarse fuera cuando no son aplicables a los requisitos o la configuración del usuario sin eliminarse del modelo. El modelo consiste de una parte genérica y partes específicas de programa que representan la configuración específica del sistema. La parte específica del programa puede reestructurarse en cada nivel: pantallas, ventanas, sub-ventanas, contenidos de las ventanas, paneles con pestañas. La estructura versátil del procedimiento y la herramienta para soportarlo brinda mucha eficacia al procedimiento de diseño de la HCI en esta realización de la invención.

El procedimiento de diseño de HCI en esta realización de la invención comprende cuatro etapas.

La primera etapa es el Análisis del Negocio que comprende las siguientes sub-etapas:

- Hacer Diagramas del Caso de Uso de Negocios (BUC): Los BUC al más alto nivel se deducen a partir de las Misiones, Objetivos, Tareas de la organización de los usuarios; los Actores de los Negocios son entidades que quieren conseguir el BUC, contribuyen a conseguir el BUC o están influenciados por el BUC; los

diagramas pueden descomponerse en diagramas BUC de niveles más bajos bajando a un nivel que permite a los BUC describirse por un Diagrama de Actividad de Negocio;

- Dibujar los Diagramas de Actividad de Negocio: tales diagramas muestran el flujo principal de las actividades que se realizan por la organización para conseguir cada uno de los BUC;
- Desarrollar un Mapa de Papeles: tal mapa permite a todos los trabajadores en la organización (Papeles) que contribuyen a los BUC; el Mapa de Papeles muestra los tipos de trabajadores y su estructura de organización;
- Dibujar los Diagramas de Carriles para cada uno de los BUC: Un Diagrama de Carriles muestra varias columnas (carriles), representando cada uno de los actores o trabajadores que están involucrados en el BUC; las actividades identificadas para el BUC se asignan a estos carriles en base al flujo cronológico en los Diagramas de Actividad; Los Diagramas de Carriles también pueden mostrar Entidades (por ejemplo información o artículos) que se producen, consumen o intercambian entre los carriles; si se identifican muchas entidades que se relacionan entre sí, puede producirse una mapa de Entidades para mostrar estas relaciones.

La segunda etapa es el Análisis de Tareas que comprende las siguientes sub-etapas:

- Crear un Caso de Tareas (también llamado Caso de Uso del Sistema) para cada una de las Actividades de Negocios que se soportará por el sistema. Los diagramas de carriles de los BUC muestran qué trabajadores en la organización realizan estas Actividades de Negocios. Al nivel del Caso de Uso del Sistema (SUC), para cada uno de los trabajadores se identifica un Papel. Para cada uno de los Papeles se realiza un diagrama SUC, que muestra todos los SUC realizados por ese Papel. Si hay muchos SUC, pueden dividirse en varios diagramas, por ejemplo, en base a su coherencia operacional (véase también la siguiente etapa);
  -Ensamblar los Mapas de Casos de Tareas: estos mapas están estructurados en base a las tareas relacionadas; muestran relaciones entre tareas y jerarquía de las tareas; en esta etapa, se corre una comprobación para verificar que no hay ninguna tarea perdida;
  pueden incluirse las tareas resultantes de los aspectos técnicos del sistema, como los parámetros de configuración o correr una comprobación;
- Producir un Diagrama de Interacción Lógico para cada uno de los Casos de Tareas: estos son diagramas de carriles con sólo dos carriles, uno para el sistema y uno para el usuario, que muestran la interacción entre el usuario y el sistema.

La tercera etapa es el Diseño de Interacción que comprende las siguientes sub-etapas:

- Definir Contextos de Interacción, es decir grupos de Interacciones que el sistema tiene que realizar para proporcionar al usuario la información y funcionalidad que se han especificado;
- Producir Mapas de Contenidos que representan disposiciones de pantallas conceptuales donde el espacio de la pantalla se asigna a los Contextos de Interacción, mostrando de este modo dónde estará disponible la información y funciones sobre las pantallas del usuario;
- Producir Mapas de Navegación que muestran cómo puede navegar el usuario entre grupos de funciones e información dentro de un Contexto de Interacción único;
- Modelar la información para el usuario en Diagramas de Clases de Fronteras; cada una de las clases de fronteras contiene la especificación del formato y los rangos de valores de cada uno de los elementos de información;
- Desarrollar el Diseño Físico de Interacción; el diseño puede hacerse usando un constructor de la GUI, produciendo un prototipo de alta fidelidad de la HCI;
- Producir Diagramas de Interacción Lógica que presentan la especificación detallada de la Interacción Física en la forma de una documentación de actividades; estos diagramas pueden suplementarse por los Diagramas de Estado que muestran cuándo las acciones específicas están habilitadas o deshabilitadas, cuándo se presenta la información, etc.

La cuarta etapa es la Validación del Usuario o Comprobación de la Facilidad de uso. Esto involucra a los usuarios finales reales en la validación de las soluciones de HCI. Los escenarios se especifican y se asignan tareas a los usuarios a realizar usando un prototipo de trabajo del sistema. Los eventos pueden iniciarse a partir de procedimientos de simulación y se monitoriza el funcionamiento del usuario y se graba para su evaluación posterior. También puede preguntarse a los usuarios para rellenar cuestionarios después de cada uno de los experimentos. Los resultados de estos test de la facilidad de uso fluyen de vuelta al procedimiento donde sea apropiado para mejorar las soluciones del sistema de HCI. La comprobación de la facilidad de uso no es el primer punto en el procedimiento donde los usuarios finales pueden involucrarse. Básicamente, cada una de las etapas de verificación puede tener lugar con usuarios finales. Los usuarios finales y los expertos en el dominio típicamente son necesarios durante el Análisis del Negocio.

La retroalimentación durante la etapa de Validación del Usuario de HCI puede volver al procedimiento del Análisis del Negocio y modificar el CONOPS sin demasiado rediseño porque ocurre bastante pronto en el procedimiento de desarrollo.

El procedimiento puede soportarse por un conjunto de herramientas. Por ejemplo pueden producirse diagramas, mapas y modelos con herramientas de ingeniería de software/sistemas como el Desarrollador de Software Racional

o Rosa (RSD) de Rational. Este conjunto de herramientas también incluye una herramienta para diseñar la GUI (Eclipse). Las librerías de los componentes de la GUI pueden encontrarse fuera de la plataforma (COTS) o desarrollarse por el desarrollador del sistema. La especificación presenta ejemplos de un sistema de defensa propuesto para un entorno costero. Aunque es evidente que la invención puede aplicarse a otros entornos terrestres o urbanos. El tipo de sensores será diferente y su cobertura también será muy diferente pero se aplicarán los mismos principios y herramientas. Además, los beneficios de la invención serán mayores ya que otros entornos probablemente serán más exigentes en términos de fusión de inteligencias porque el nivel de confianza que puede atribuirse a los sensores será menor, específicamente en los entornos urbanos o de bosques donde las multi-trayectorias arruinarán la integridad de los sensores electromagnéticos. También, el procedimiento de la memoria descriptiva de acuerdo con la invención no es específico del entorno. Por consiguiente, no hay ninguna limitación del dominio en la invención reivindicada.

REIVINDICACIONES

1. Un sistema de seguridad y protección para un área definida que comprende sensores (110, 120, 130, 140, 150, 160, 170, 180) adaptados para capturar un primer conjunto de datos de seguimiento instantáneo (300) sobre un primer conjunto de objetos (200) localizados en dicha área o en la proximidad de la misma, comprendiendo dicho primer conjunto de datos de seguimiento instantáneo al menos un vector de posición en tiempo real y datos de velocidad de al menos un sensor sobre al menos uno de los objetos de dicho primer conjunto de objetos, fuentes de información (400) adaptadas para capturar un segundo conjunto de datos de seguimiento no instantáneo (500) sobre un segundo conjunto de objetos (600), comprendiendo dicho segundo conjunto de datos de seguimiento no instantáneo al menos un elemento de información sobre uno de: identificación, historia de posición/comportamiento de al menos uno de los objetos de dicho segundo conjunto de objetos, estando dicho sistema **caracterizado porque** comprende además un conjunto de procedimientos de ordenador (900, 100A, 200A) adaptados para correlacionar elementos del primer conjunto de objetos (200) con elementos del segundo conjunto de objetos (600) y para calcular niveles de amenaza de los elementos del primer conjunto de objetos a partir de dichos primero y segundo conjuntos de datos asignados a dichos elementos correlacionados.

2. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** comprende además procedimientos de ordenador, bases de datos y redes adaptadas para gestionar la colección de datos de seguimiento instantáneo y seguimiento no instantáneo sobre dichos primero y segundo conjuntos de objetos desde dichos sensores y fuentes de información y la distribución selectiva de dichos datos para al menos un usuario del sistema.

3. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** dichos niveles de amenaza se calculan al menos en parte en base a los resultados de al menos un procedimiento adaptado para detectar y manejar anomalías en el comportamiento de dichos números correlacionados.

4. Un sistema de acuerdo con la reivindicación 3 **caracterizado porque** dicho procedimiento adaptado para detectar y manejar anomalías en el comportamiento de dichos elementos correlacionados que comprende un subprocedimiento de detección de anomalías que recibe como entrada un indicador de al menos un agente y al menos una matriz de mapeo y produce como salida al menos una información del grupo que comprende un informe de anomalías, alerta específica, asesoramiento de los operadores y alerta general.

5. Un sistema de acuerdo con la reivindicación 4 **caracterizado porque** dicho subproceso de detección de anomalías usa un motor de razonamiento.

6. Un sistema de acuerdo con la reivindicación 3 **caracterizado porque** dicho procedimiento adaptado para detectar y manejar anomalías en el comportamiento de dichos elementos correlacionados comprende un subproceso de análisis de riesgos que recibe como entrada al menos un cuadro de vigilancia y produce como salida una lista de acciones.

7. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende información recibida desde los transceptores a bordo de algunos elementos del primer conjunto de objetos y **porque** los niveles de amenaza de dichos elementos se calculan al menos parcialmente a partir de los valores de una variable que define la consistencia de la información recibida desde los transceptores con otros elementos del primero y segundo conjuntos de datos de dichos elementos.

8. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende la definición de zonas específicas dentro del área que se tiene en cuenta para calcular los niveles de amenaza de los objetivos que entran en dichas zonas.

9. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende los parámetros cinemáticos esperados para las clases de objetos y porque los niveles de amenaza de los elementos del primer conjunto de objetos que pertenecen a dichas clases se calculan al menos parcialmente a partir de los valores de al menos una variable que define la desviación de dichos patrones cinemáticos.

10. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende huellas históricas de seguimientos de clases de objetos y que los niveles de amenaza de los elementos del primer conjunto de objetos que pertenece a dichas clases se calculan al menos parcialmente a partir de los valores de al menos una variable que define una desviación de dichas huellas históricas de seguimientos.

11. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende la definición de zonas específicas dentro del área que se tienen en cuanta para calcular los niveles de amenaza de los objetivos procedentes desde dichas zonas.

12. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende planes de ruta para algunos elementos del primer conjunto de objetos y porque los niveles de amenaza de dichos elementos se calculan al menos parcialmente a partir de los valores de al menos una variable que define la consistencia de la información recibida a partir de los sensores con los planes de ruta para dichos elementos.

13. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende patrones de seguimiento para clases de objetos y porque los niveles de amenaza de los elementos del primer conjunto de objetos que pertenece a dichas clases se calculan al menos parcialmente a partir de los valores de al menos una variable que define una desviación de dichos patrones de comercio.

14. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende clases de patrones de seguimientos representativos de las clases de eventos etiquetados con un nivel de amenaza y porque los niveles de amenaza de los elementos del primer conjunto de objetos que siguen las pìstas pertenecientes a dichas clases de patrones se calculan al menos parcialmente a partir de los valores del nivel de amenaza asignados a la clase de eventos coincidentes.

15. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende clases de incidentes en seguimientos representativos de clases de eventos etiquetados con un nivel de amenaza y porque los niveles de amenaza de los elementos del primer conjunto de objetos que siguen las pìstas pertenecientes a dichas clases de incidentes se calculan al menos parcialmente a partir de los valores del nivel de amenaza asignados a la clase de eventos coincidentes.

16. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende clases de seguimientos estándar representativos de las clases de objetos y porque el nivel de amenaza de los elementos del primer conjunto de objetos que pertenecen a la clase definida y se desvían del seguimiento estándar atribuido a la clase de objetos se calculará al menos parcialmente a partir de dicha desviación.

17. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** el segundo conjunto de datos comprende información extraída de los informes de inteligencia y **porque** la correlación de los elementos del primer conjunto de objetos con los elementos del segundo conjunto de objetos se basa en una combinación de los parámetros de alerta definidos por el usuario.

18. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** la información extraída a partir del primero y segundo conjuntos de datos tiene atributos de distribución basados, al menos en parte, en parámetros de zonificación de interés y en atributos de la información.

19. Un sistema de acuerdo con la reivindicación 1 **caracterizado porque** los cuadros operacionales del área compuestos por ordenador se representan a conjuntos de operadores.

20. Un sistema de acuerdo con la reivindicación 19 **caracterizado porque** los cuadros operacionales del área compuestos por ordenador a representar a un conjunto definido de operadores se seleccionan y se agrupan en conjuntos de trabajo determinados, al menos parcialmente, como una función de los papeles definidos para dicho conjunto de operadores, teniendo cada uno de los papeles tareas atribuidas configurables para cumplir las misiones configurables atribuidas.

21. Un sistema de acuerdo con la reivindicación 20 **caracterizado porque** los conjuntos de trabajos se adaptan para estar dispuestos, al menos parcialmente, como una función de un flujo de trabajo entre los operadores.

22. Un sistema de acuerdo con la reivindicación 20 **caracterizado porque** los conjunto de trabajos están adaptados para hacerse dependientes de un conjunto de modos de operación dependientes del estado de alerta que impactan en la lista y la carga de trabajo de las tareas para al menos un papel.

23. Un sistema de acuerdo con la reivindicación 19 **caracterizado porque** los cuadros operacionales del área compuestos por ordenador a representar se componen al menos parcialmente como una función del nivel mínimo, definido por el usuario, de la amenaza a dirigir y del ordenador disponible y las capacidades de representación.

24. Un procedimiento para el diseño de la especificación de un sistema de seguridad y protección para un área que comprende las etapas de definir a través de al menos una interacción con algunos de los usuarios del sistema las misiones a realizar por el sistema y los recursos adaptados para el cumplimiento de dichas misiones **caracterizado porque** dichos recursos son de un tipo seleccionado a partir de un grupo que comprende al menos sensores adaptados para adquirir el vector de posición en tiempo real y los datos de velocidad de los objetivos, fuentes de información adaptadas para adquirir al menos un elemento de información sobre uno de: identificación, historia de posición/comportamiento de al menos un objeto, centros de operaciones adaptados para realizar los procedimientos de ordenador para correlacionar elementos de un primer conjunto de objetos con elementos de un segundo conjunto de objetos y para calcular los niveles de amenaza de los elementos correlacionados de los dos conjuntos de objetos, la red de comunicaciones y los requisitos de dotación.

25. Un procedimiento de acuerdo con la reivindicación 24 **caracterizado porque** los recursos son de un tipo seleccionado a partir de un grupo que comprende al menos requisitos de dotación y al menos otro tipo seleccionado a partir de un grupo que comprende al menos sensores, fuentes de información, centros de operaciones, red de comunicaciones.

26. Un procedimiento de acuerdo con la reivindicación 24 **caracterizado porque** las entregas a al menos algunos de

los usuarios del sistema comprenden una evaluación de la idoneidad del sistema para los propósitos pretendidos y de la cobertura de los mismos.

27. Un procedimiento de acuerdo con la reivindicación 24 **caracterizado porque** las entregas a al menos algunos de los usuarios del sistema comprende una evaluación del entrenamiento y esfuerzos logísticos para desplegar y mantener dicho sistema.

28. Un procedimiento de acuerdo con la reivindicación 24 **caracterizado porque** los requisitos de dotación se definen al menos parcialmente en base a los papeles para cumplir las misiones, estando definidos dichos papeles por conjuntos de tareas.

29. Un procedimiento de acuerdo con la reivindicación 24 **caracterizado porque** el conjunto de tareas atribuidas a al menos un papel puede variar, al menos parcialmente, como una función de los modos de operación, estando definido cada uno de los modos de operación para una combinación de un estado de alerta definido por el usuario y un estado del sistema.

30. Un procedimiento de acuerdo con la reivindicación 24 **caracterizado porque** comprende además etapas para definir las interfaces humano ordenador del sistema, comprendiendo dichas etapas entre otros la definición de los diagramas del caso de uso de negocio derivados de las misiones asignadas a los usuarios del sistema.

31. Un procedimiento de acuerdo con la reivindicación 28 **caracterizado porque** comprende además etapas para definir las tareas a realizar por el sistema para soportar las actividades que se seleccionan por al menos algunos de los usuarios a partir de la lista de casos de uso de negocio.

32. Un procedimiento de acuerdo con la reivindicación 28 **caracterizado porque** comprende además etapas para definir los contextos de interacción usados a continuación para definir las disposiciones conceptuales de pantalla pasados a un constructor de la interfaz gráfica de usuario para definir el diseño de la interacción física.

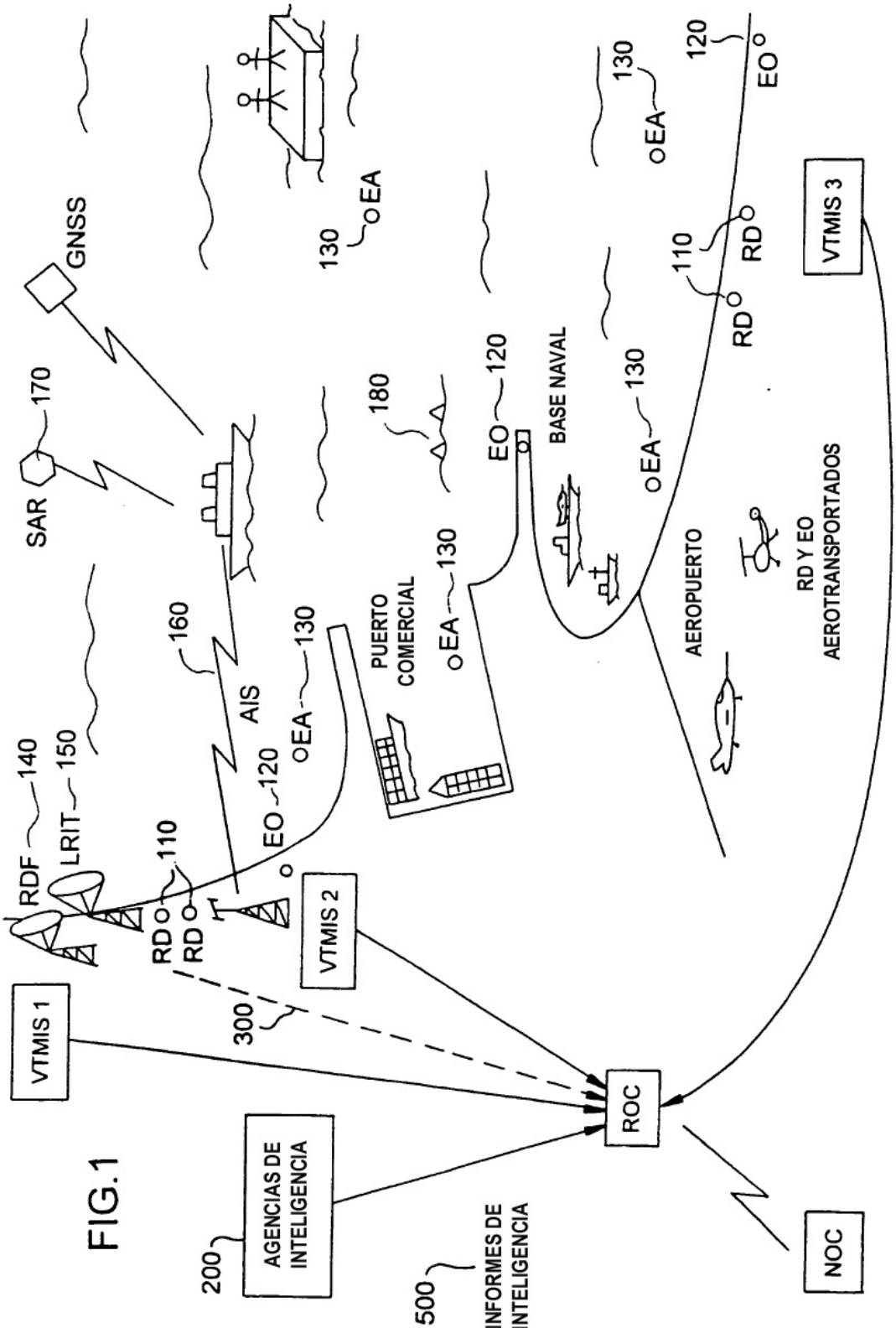
GNSS
SAR
170
RDF
140
LRIT
150
110
RD
RD
160
AIS
EO
120
EA
130
PUERTO COMERCIAL
180
BASE NAVAL
AEROPUERTO
RD Y EO AEROTRANSPORTADOS
VTMIS 1
VTMIS 2
VTMIS 3
300
ROC
NOC
AGENCIAS DE INTELIGENCIA
200
500
INFORMES DE INTELIGENCIA

FIG.1

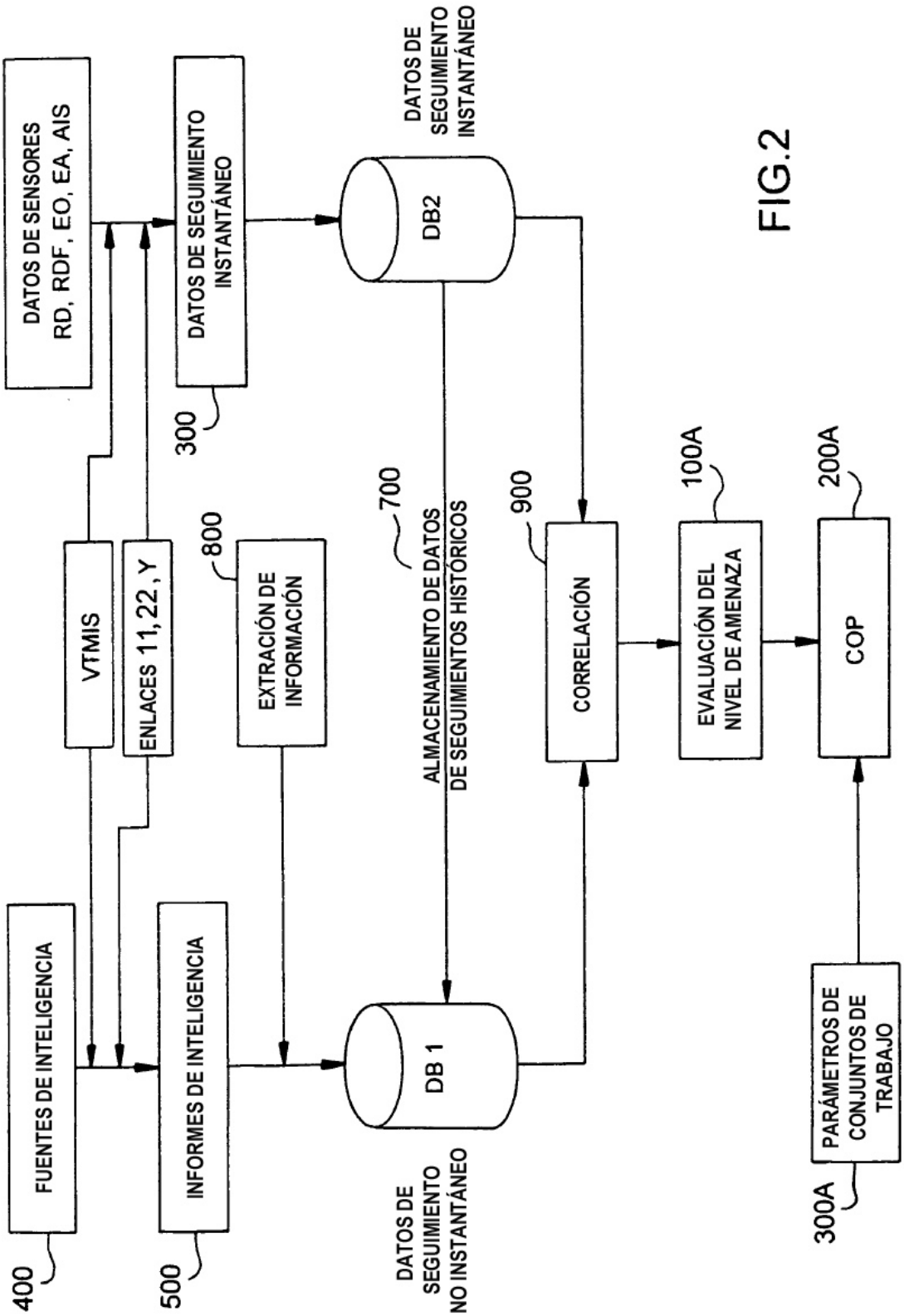
DATOS DE SENSORES RD, RDF, EO, EA, AIS
DATOS DE SEGUIMIENTO INSTANTÁNEO
300
DB2
DATOS DE SEGUIMIENTO INSTANTÁNEO
VTMIS
ENLACES 11, 22, Y
800
EXTRACIÓN DE INFORMACIÓN
700
ALMACENAMIENTO DE DATOS DE SEGUIMIENTOS HISTÓRICOS
900
CORRELACIÓN
100A
EVALUACIÓN DEL NIVEL DE AMENAZA
200A
COP
FUENTES DE INTELIGENCIA
INFORMES DE INTELIGENCIA
DB 1
PARÁMETROS DE CONJUNTOS DE TRABAJO
400
500
DATOS DE SEGUIMIENTO NO INSTANTÁNEO
300A

FIG.2

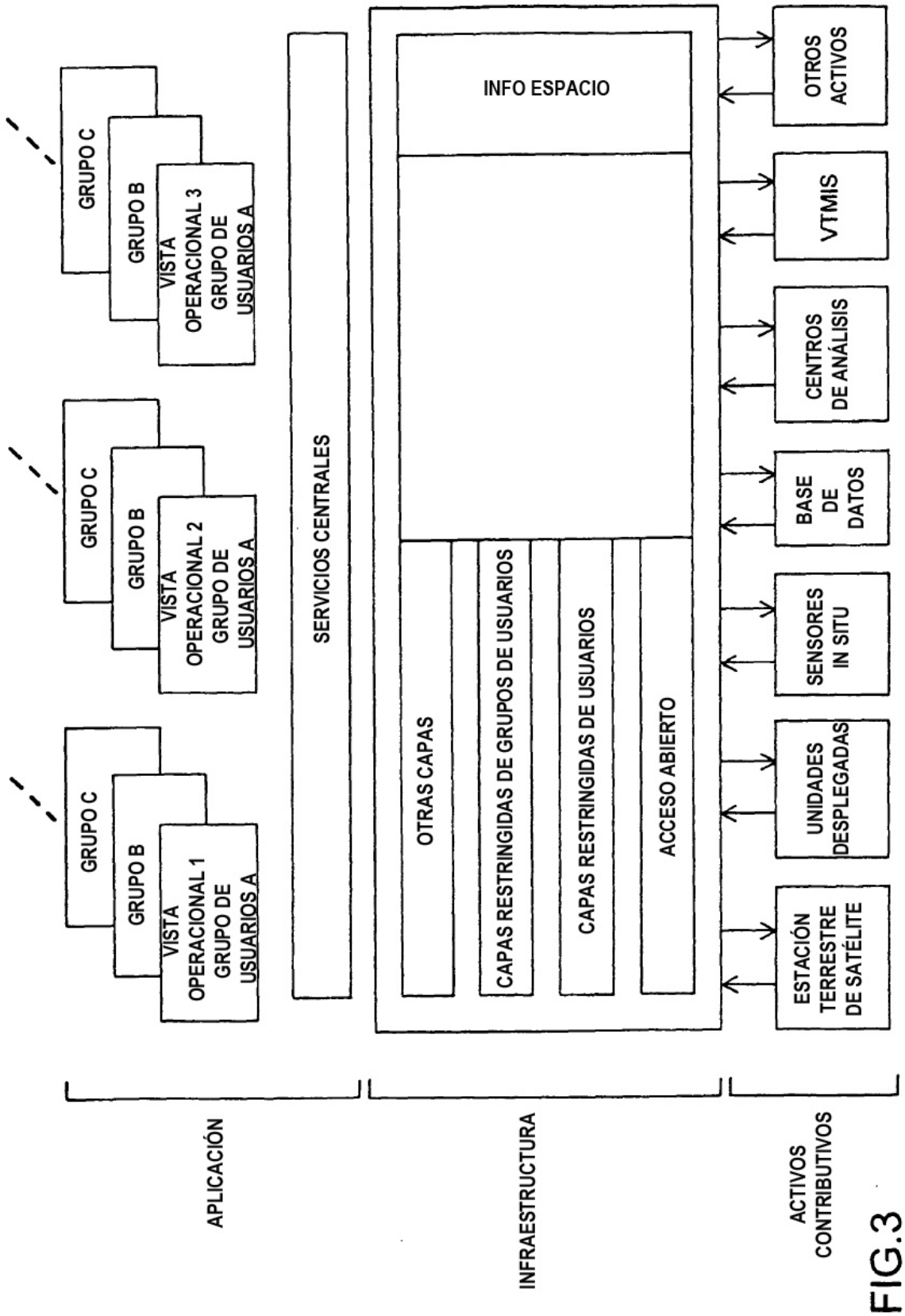
APLICACIÓN
INFRAESTRUCTURA
ACTIVOS CONTRIBUTIVOS
GRUPO C
GRUPO B
VISTA OPERACIONAL 1 GRUPO DE USUARIOS A
VISTA OPERACIONAL 2 GRUPO DE USUARIOS A
VISTA OPERACIONAL 3 GRUPO DE USUARIOS A
SERVICIOS CENTRALES
INFO ESPACIO
OTRAS CAPAS
CAPAS RESTRINGIDAS DE GRUPOS DE USUARIOS
CAPAS RESTRINGIDAS DE USUARIOS
ACCESO ABIERTO
ESTACIÓN TERRESTRE DE SATÉLITE
UNIDADES DESPLEGADAS
SENSORES IN SITU
BASE DE DATOS
CENTROS DE ANÁLISIS
VTMIS
OTROS ACTIVOS

FIG.3

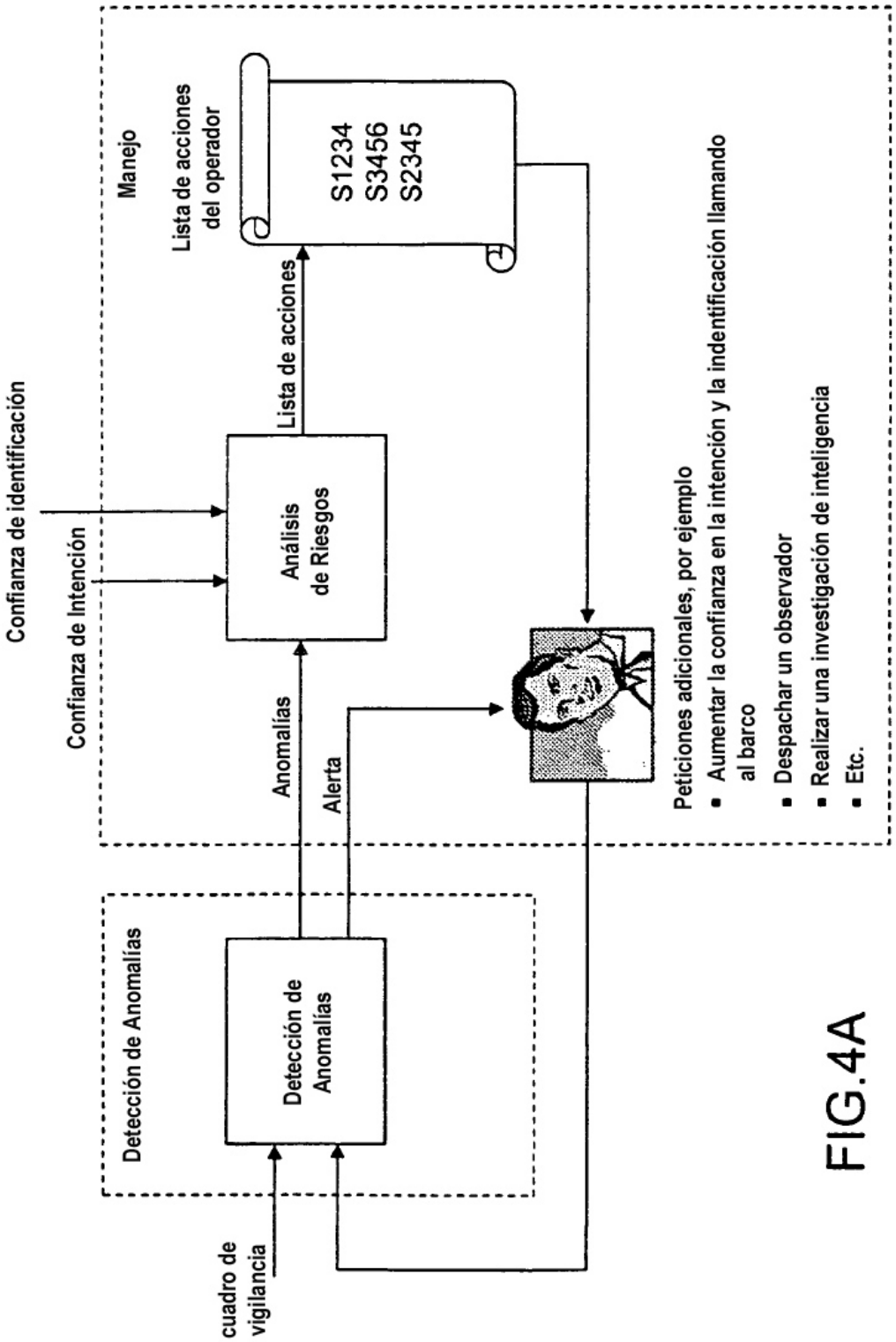
Manejo
Lista de acciones del operador
S1234
S3456
S2345
Lista de acciones
Análisis de Riesgos
Confianza de identificación
Confianza de Intención
Anomalías
Alerta
Detección de Anomalías
Detección de Anomalías
cuadro de vigilancia
Peticiones adicionales, por ejemplo
Aumentar la confianza en la intención y la indentificación llamando al barco
Despachar un observador
Realizar una investigación de inteligencia
Etc.

FIG.4A

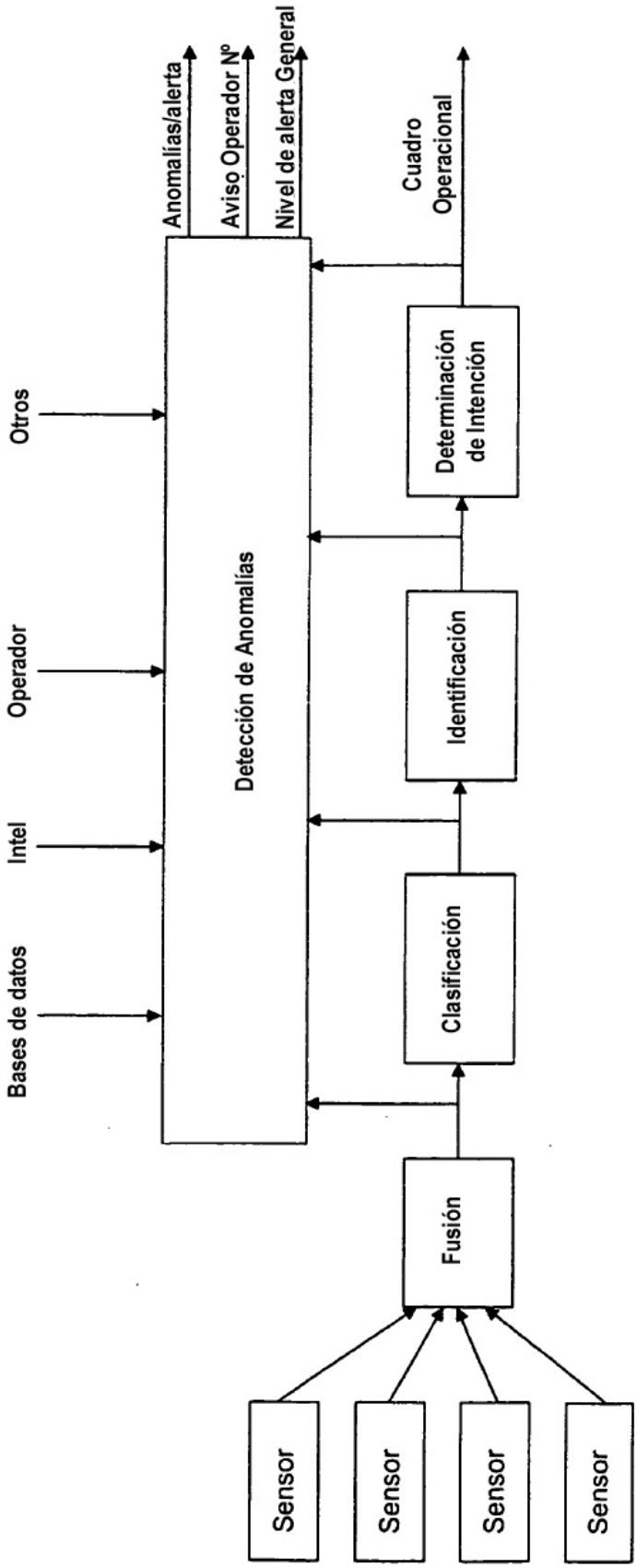
Anomalías/alerta
Aviso Operador Nº
Nivel de alerta General
Cuadro Operacional
Otros
Operador
Intel
Bases de datos
Detección de Anomalías
Determinación de Intención
Identificación
Clasificación
Fusión
Sensor
Sensor
Sensor
Sensor

FIG.4B

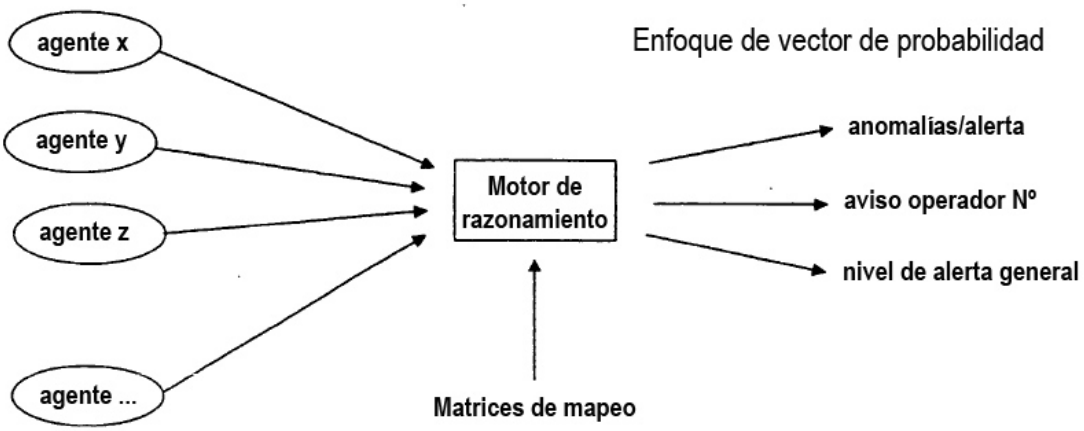

FIG.4C

		estimación	
Indicador	observación	Anomalía alta P(e|A)	Anomalía baja P(e|¬A)
aparición de seguimiento	P(e| normal)	P(normal | A)	P(normal | ¬A)
	P(e|¬normal)	P(¬normal | A)	P(¬normal | ¬A)

Matrices de mapeo

FIG. 4D

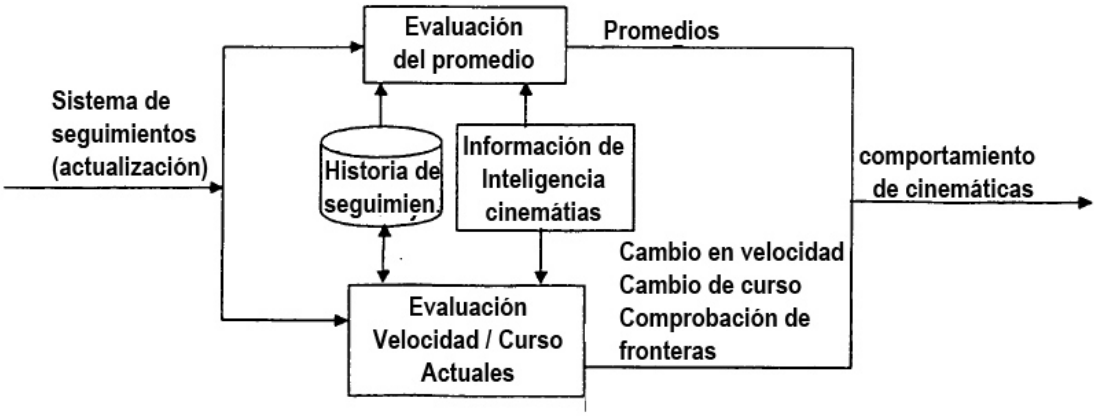

FIG.6

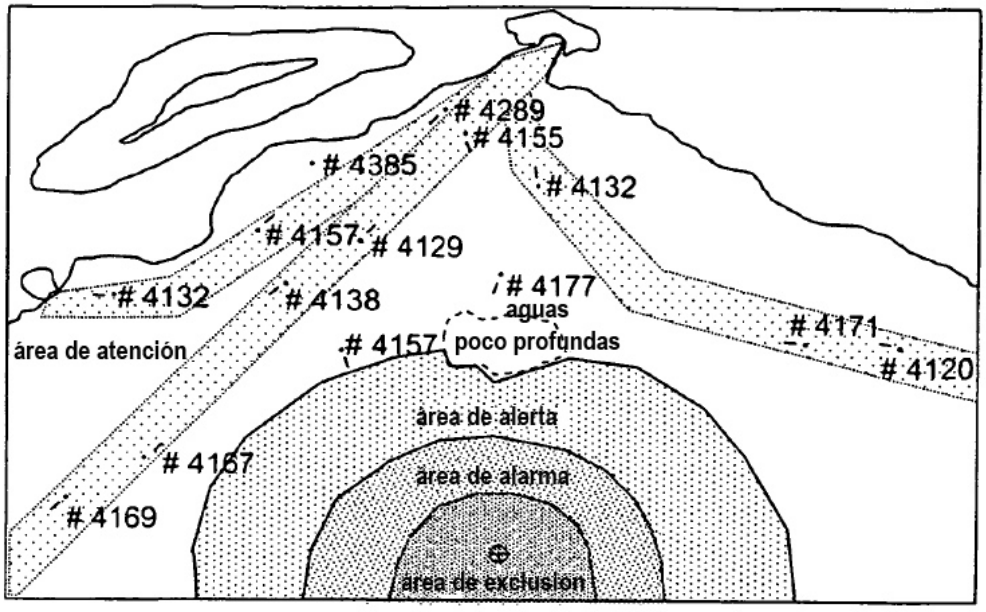
4289
4155
4385
4132
4157
4129
4132
4138
4177
aguas
poco profundas
4157
4171
4120
área de atención
área de alerta
área de alarma
4167
4169
área de exclusion

FIG.5A

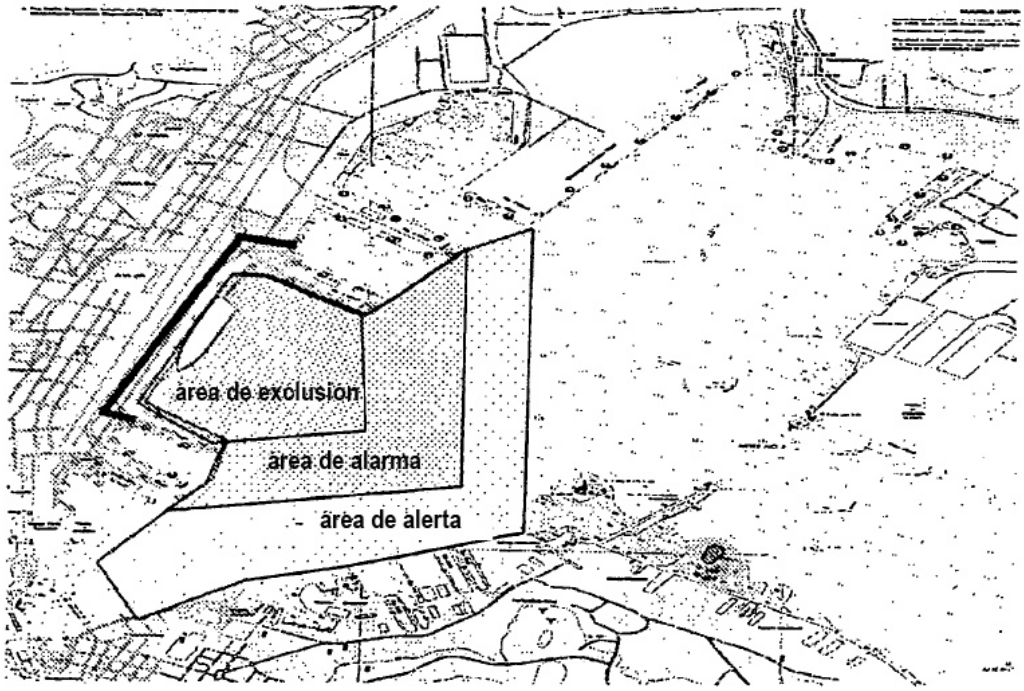
área de exclusion
área de alarma
área de alerta

FIG.5B

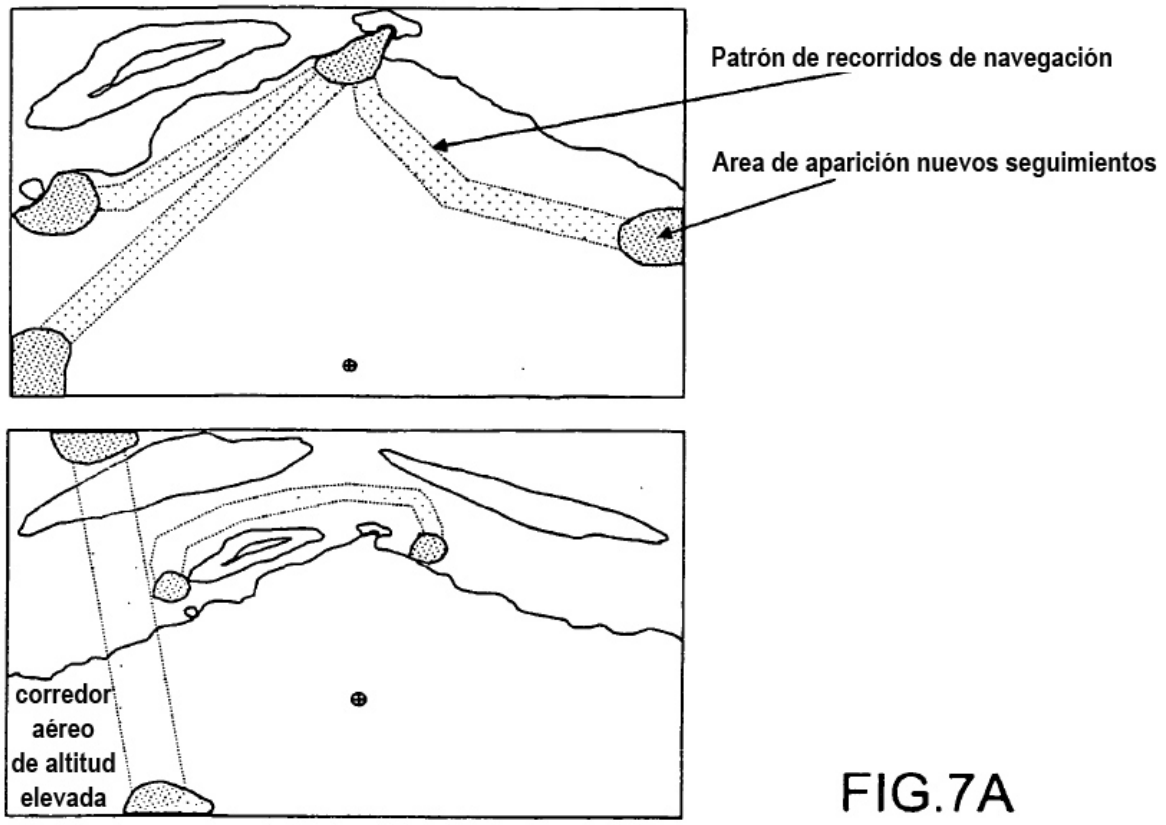
Patrón de recorridos de navegación
Area de aparición nuevos seguimientos
corredor aéreo de altitud elevada

FIG.7A

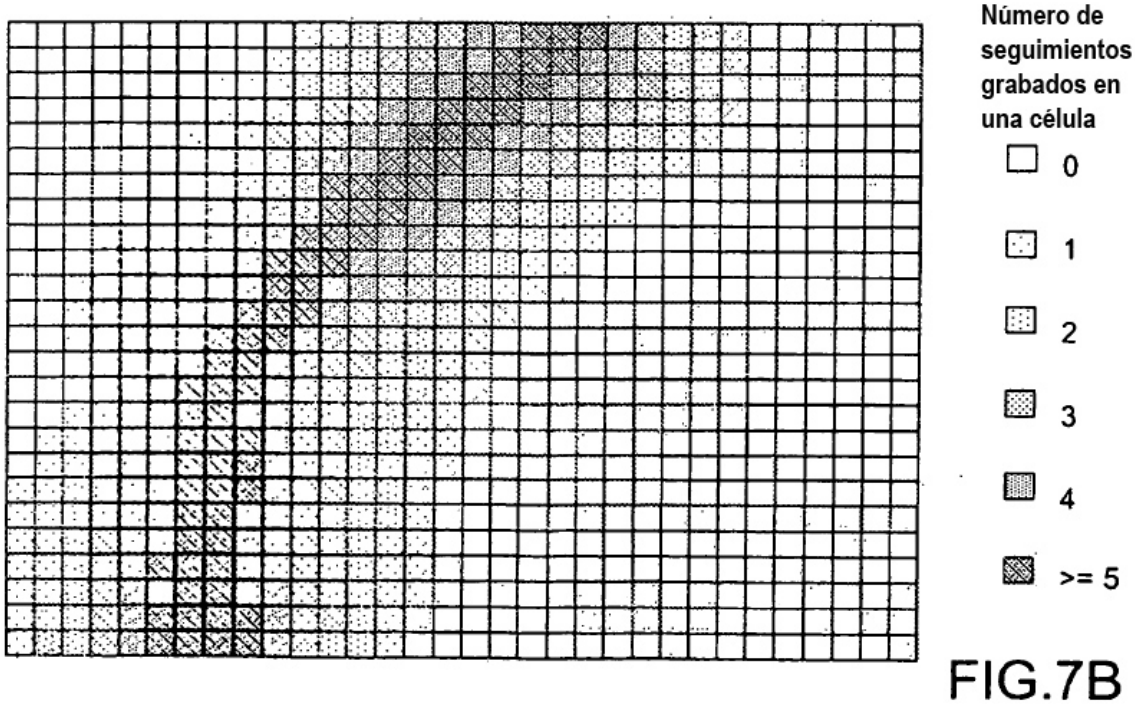
Número de seguimientos grabados en una célula
0
1
2
3
4
>= 5

FIG.7B

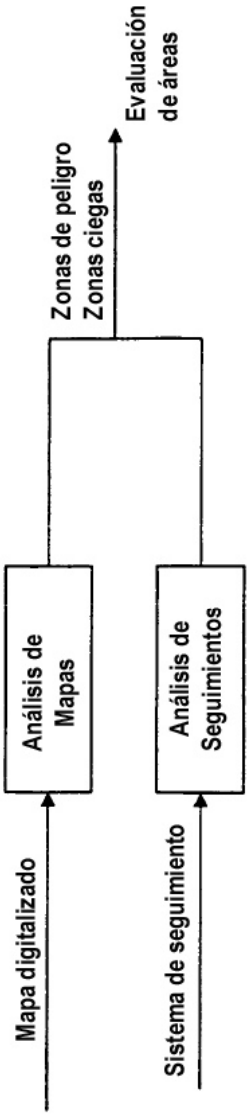

FIG.8A

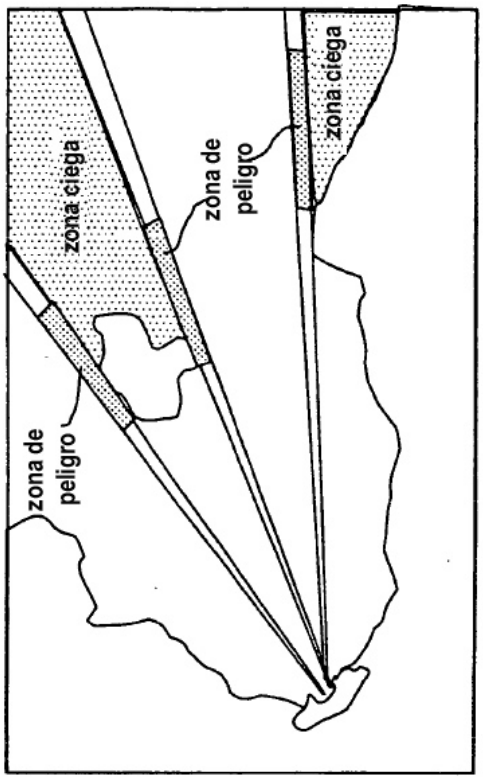

FIG.8C

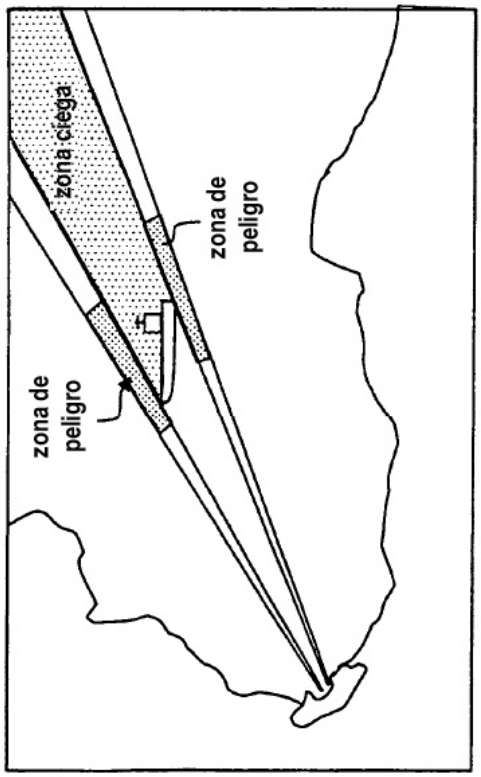

FIG.8B

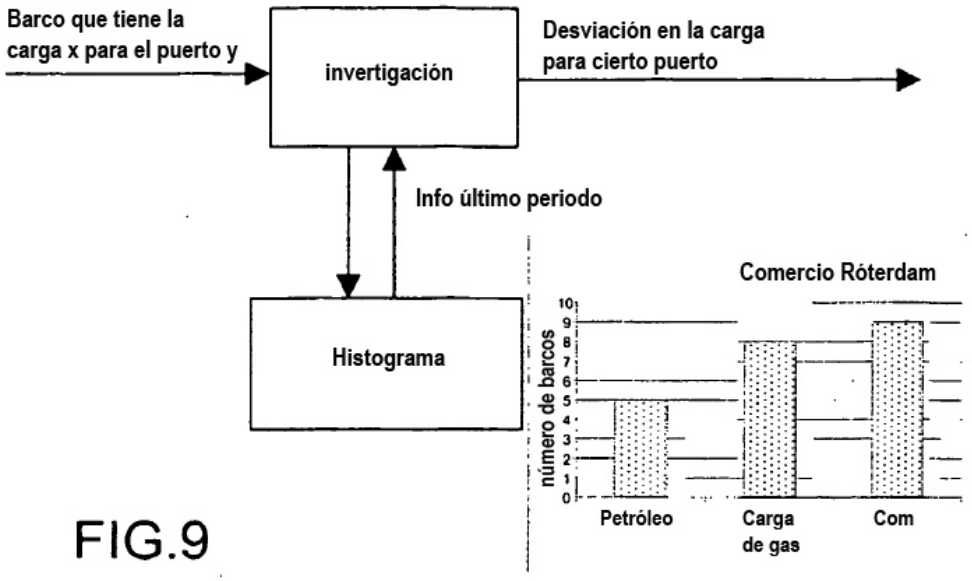
Barco que tiene la carga x para el puerto y
invertigación
Desviación en la carga para cierto puerto
Info último periodo
Histograma
Comercio Róterdam
número de barcos
Petróleo
Carga de gas
Com

FIG.9

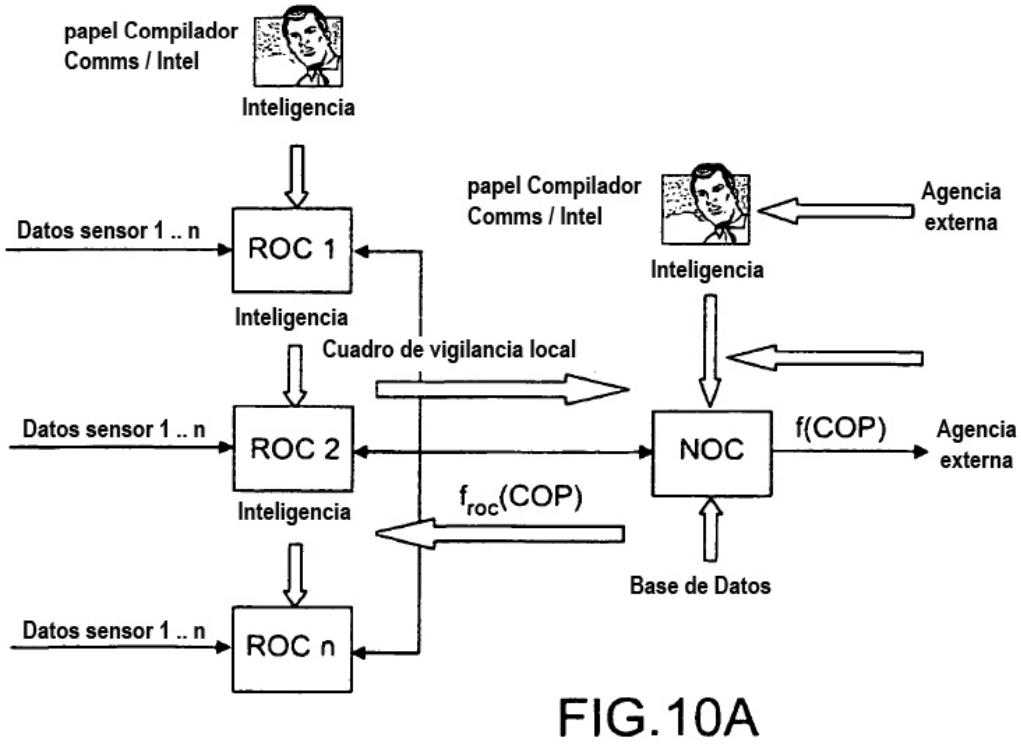
papel Compilador Comms / Intel
Inteligencia
Datos sensor 1 .. n
ROC 1
Inteligencia
papel Compilador Comms / Intel
Agencia externa
Inteligencia
Cuadro de vigilancia local
Datos sensor 1 .. n
ROC 2
Inteligencia
NOC
f(COP)
Agencia externa
f_{roc}(COP)
Base de Datos
Datos sensor 1 .. n
ROC n

FIG.10A

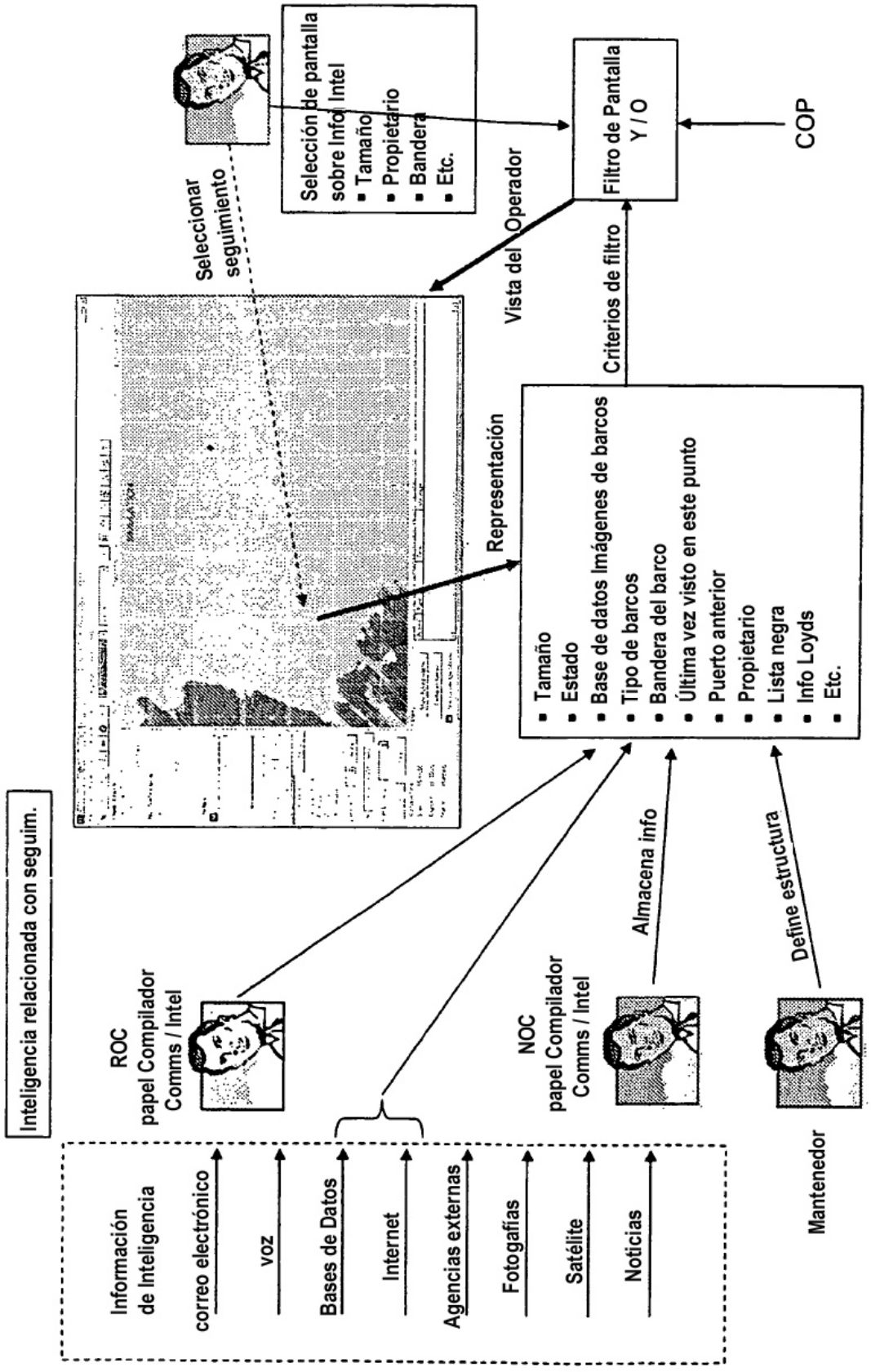
Inteligencia relacionada con seguim.
Información de Inteligencia
correo electrónico
voz
Bases de Datos
Internet
Agencias externas
Fotografías
Satélite
Noticias
ROC papel Compilador Comms / Intel
NOC papel Compilador Comms / Intel
Mantenedor
Almacena info
Define estructura
Representación
Tamaño
Estado
Base de datos Imágenes de barcos
Tipo de barcos
Bandera del barco
Última vez visto en este punto
Puerto anterior
Propietario
Lista negra
Info Loyds
Etc.
Criterios de filtro
Vista del Operador
Filtro de Pantalla Y / O
COP
Seleccionar seguimiento
Selección de pantalla sobre Info Intel
Tamaño
Propietario
Bandera
Etc.

FIG.10B

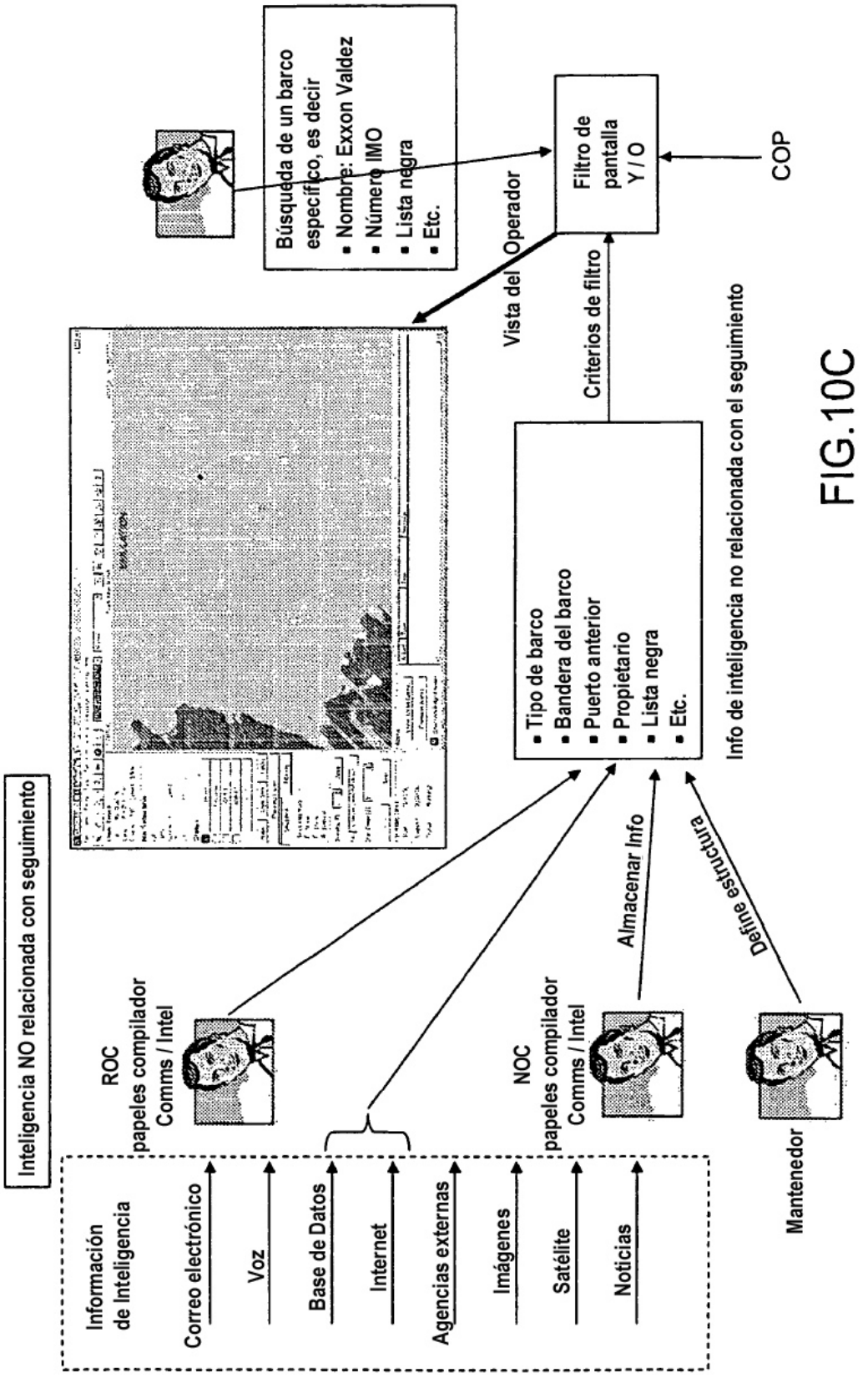
Inteligencia NO relacionada con seguimiento
Información de Inteligencia
Correo electrónico
Voz
Base de Datos
Internet
Agencias externas
Imágenes
Satélite
Noticias
ROC
papeles compilador
Comms / Intel
NOC
papeles compilador
Comms / Intel
Mantenedor
Almacenar Info
Define estructura
Info de inteligencia no relacionada con el seguimiento
Tipo de barco
Bandera del barco
Puerto anterior
Propietario
Lista negra
Etc.
Criterios de filtro
Vista del Operador
Filtro de pantalla Y / O
COP
Búsqueda de un barco específico, es decir
Nombre: Exxon Valdez
Número IMO
Lista negra
Etc.

FIG.10C

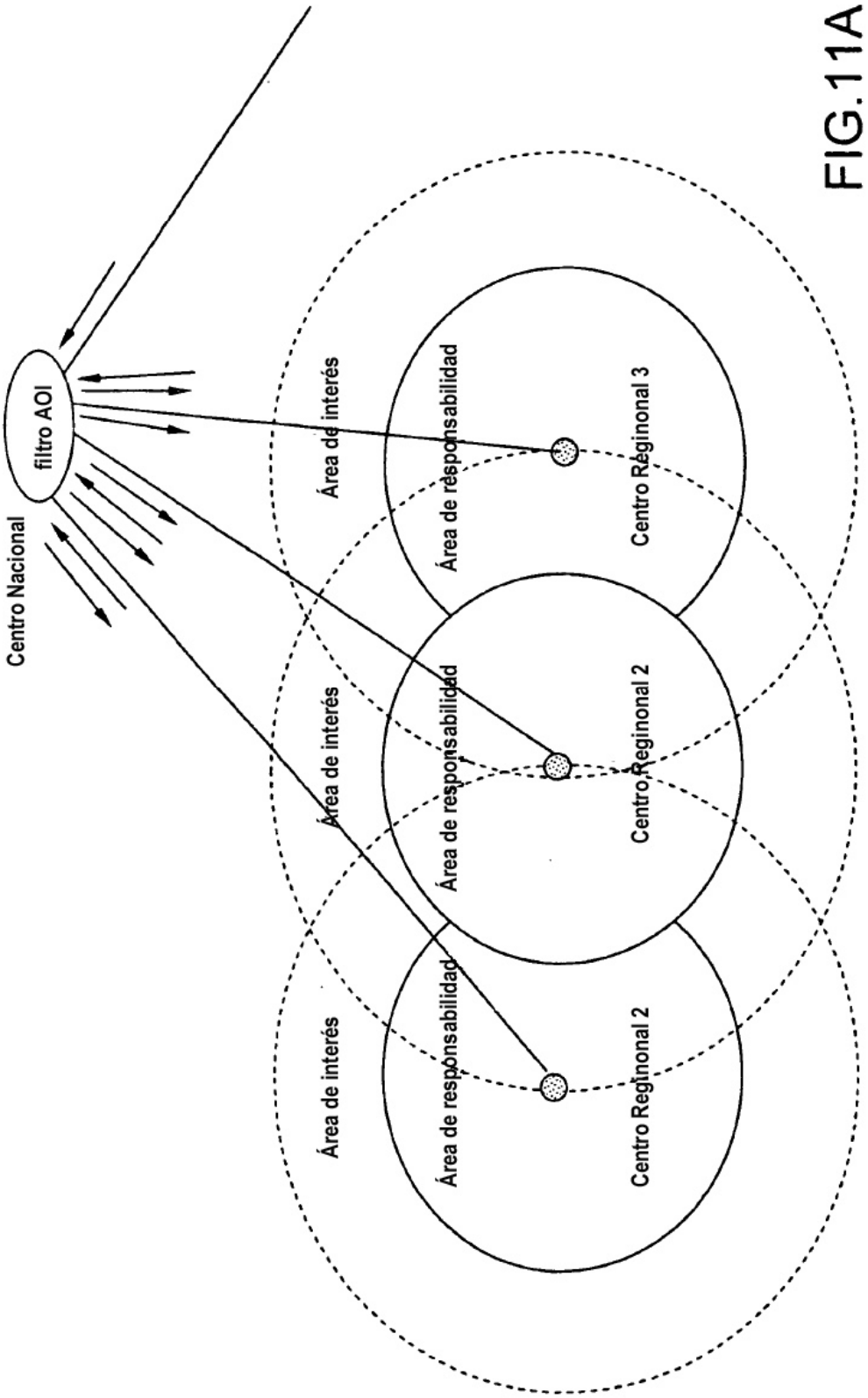
Centro Nacional
filtro AOI
Área de interés
Área de responsabilidad
Centro Regional 3
Área de interés
Área de responsabilidad
Centro Regional 2
Área de interés
Área de responsabilidad
Centro Regional 2

FIG.11A

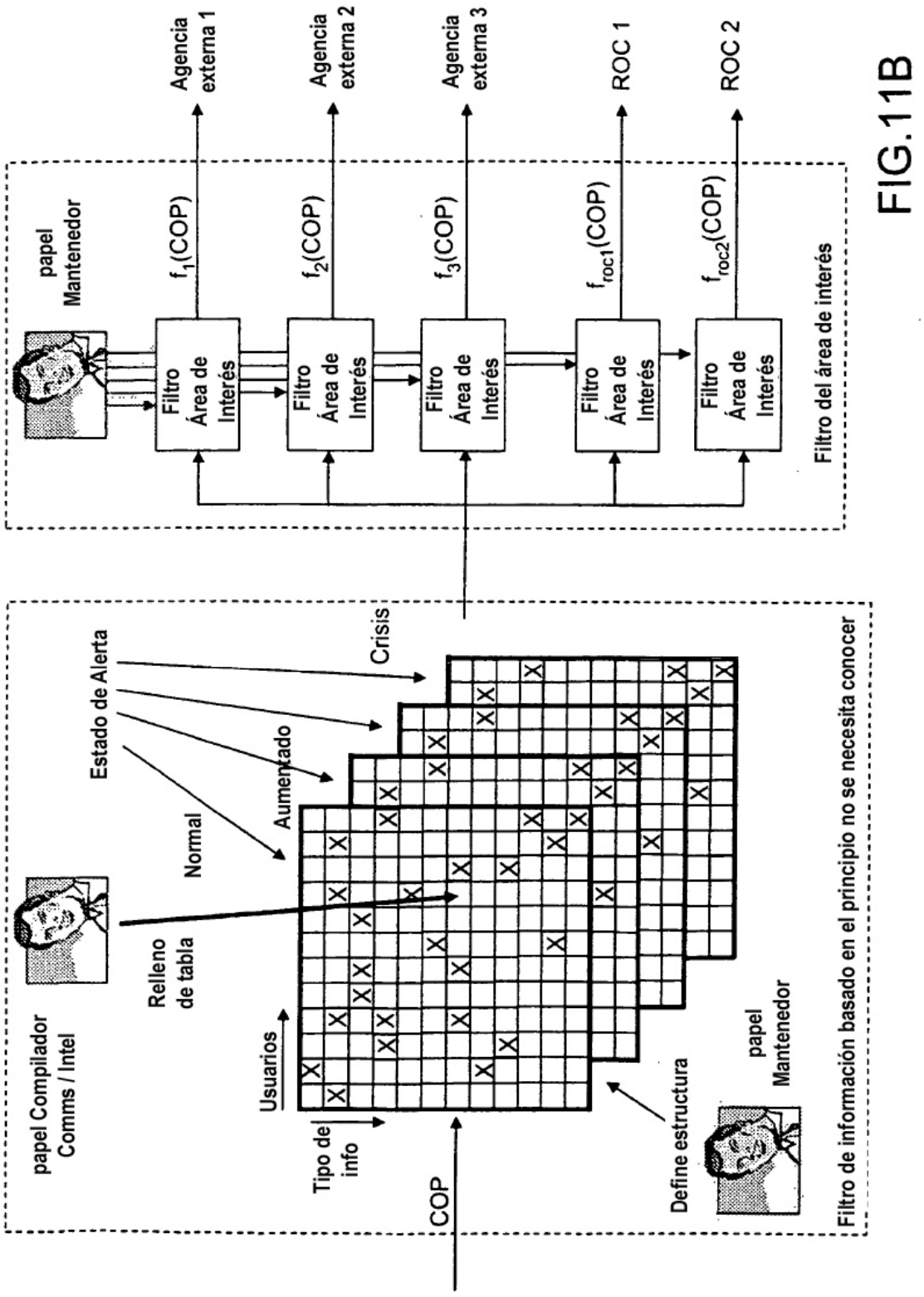
Agencia externa 1
Agencia externa 2
Agencia externa 3
ROC 1
ROC 2
papel Mantenedor
f_1(COP)
f_2(COP)
f_3(COP)
f_{roc1}(COP)
f_{roc2}(COP)
Filtro Área de Interés
Filtro del área de interés
Crisis
Estado de Alerta
Aumentado
Normal
Relleno de tabla
papel Compilador Comms / Intel
Usuarios
Tipo de info
COP
Define estructura
papel Mantenedor
Filtro de información basado en el principio no se necesita conocer

FIG.11B

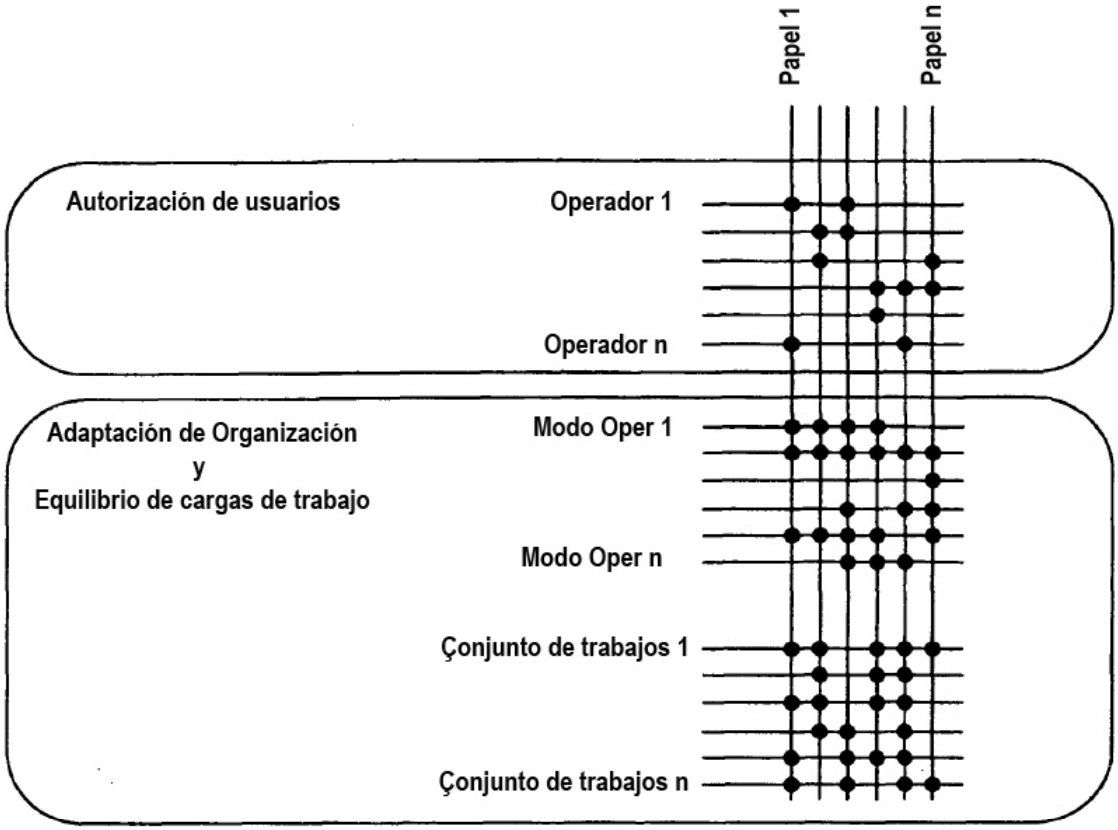

FIG.12a

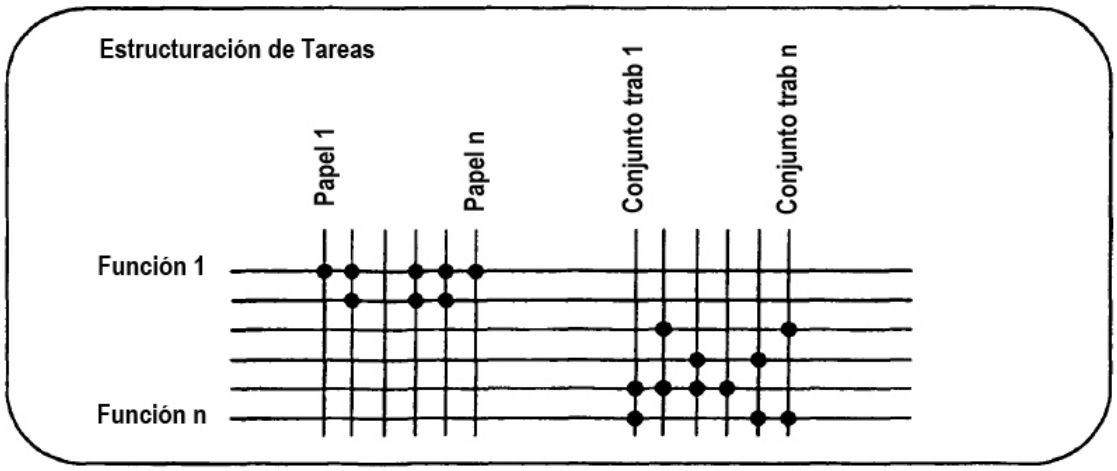

FIG.12b

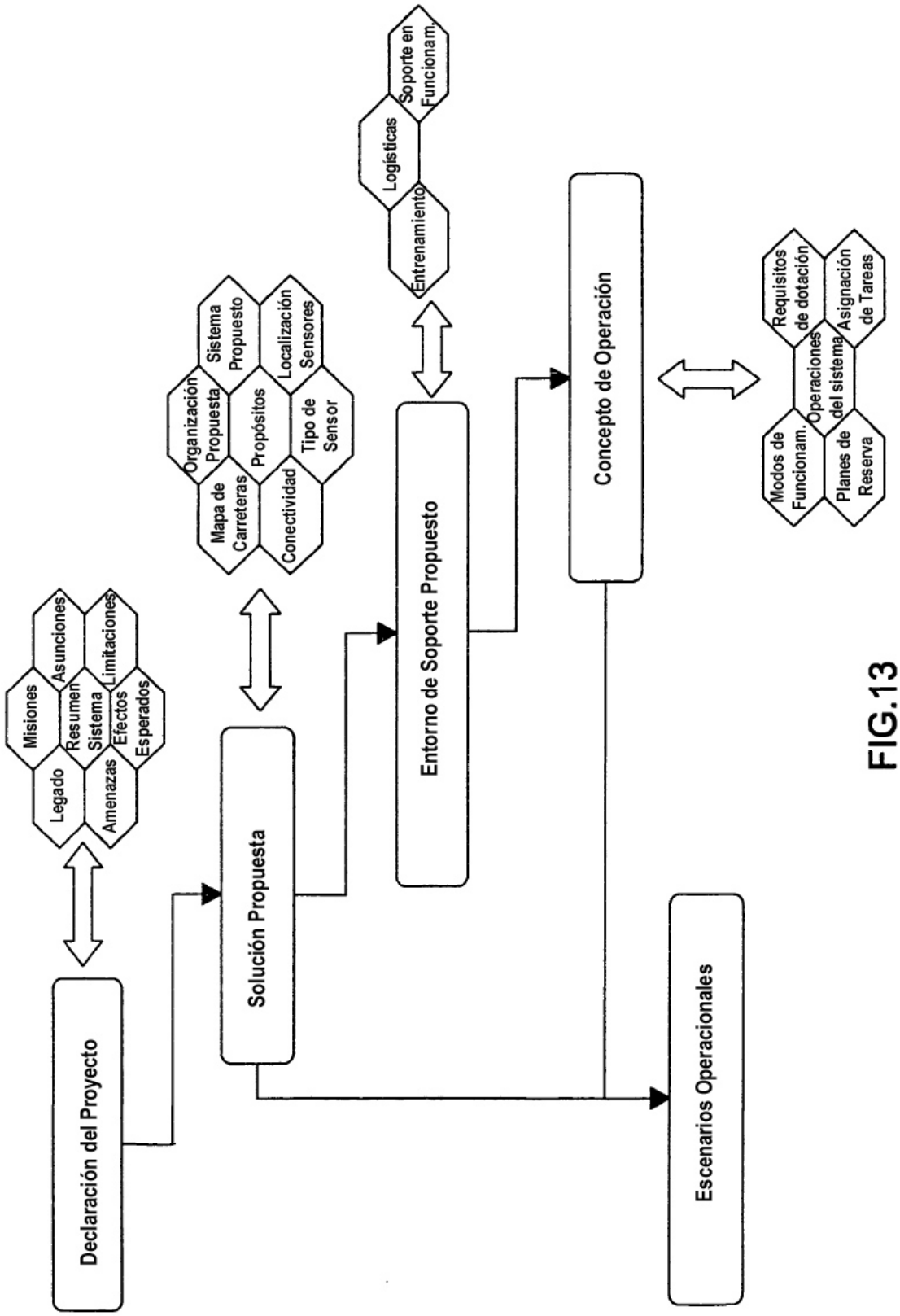
Declaración del Proyecto
Misiones
Asunciones
Limitaciones
Resumen Sistema
Efectos Esperados
Legado
Amenazas
Solución Propuesta
Sistema Propuesto
Localización Sensores
Organización Propuesta
Propósitos
Tipo de Sensor
Mapa de Carreteras
Conectividad
Entorno de Soporte Propuesto
Logísticas
Soporte en Funcionam.
Entrenamiento
Concepto de Operación
Requisitos de dotación
Asignación de Tareas
Operaciones del sistema
Modos de Funcionam.
Planes de Reserva
Escenarios Operacionales

FIG.13

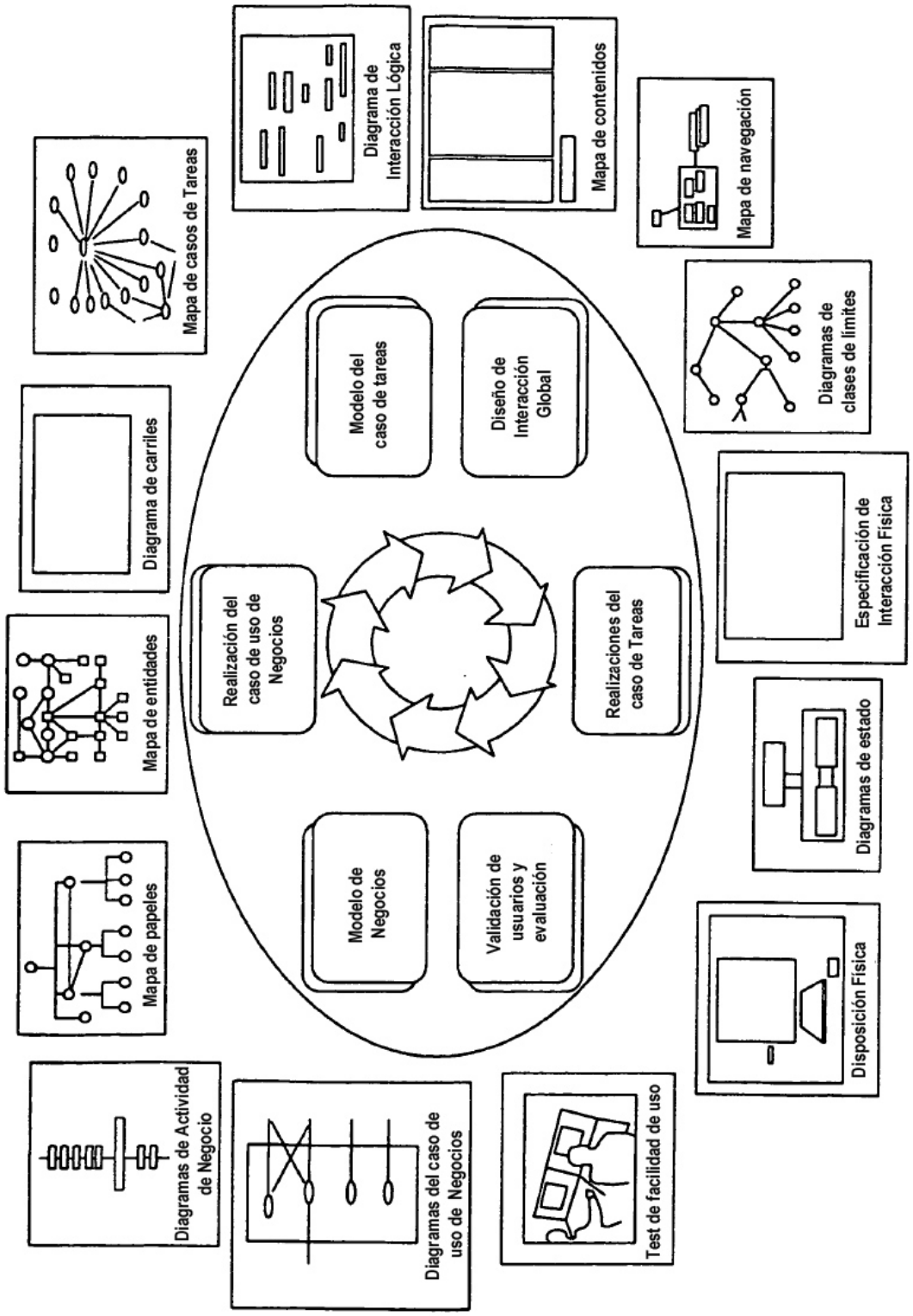
Diagramas de Actividad de Negocio
Mapa de papeles
Mapa de entidades
Diagrama de carriles
Mapa de casos de Tareas
Diagramas del caso de uso de Negocios
Test de facilidad de uso
Disposición Física
Diagramas de estado
Especificación de Interacción Física
Diagramas de clases de límites
Mapa de navegación
Mapa de contenidos
Diagrama de Interacción Lógica
Realización del caso de uso de Negocios
Modelo del caso de tareas
Diseño de Interacción Global
Realizaciones del caso de Tareas
Modelo de Negocios
Validación de usuarios y evaluación

FIG.14