(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 442**

(51) Int. CI.:

F41H 11/00 (2006.01)
G06N 5/02 (2006.01)
G08B 15/00 (2006.01)
G08B 13/12 (2006.01)
G08B 13/196 (2006.01)
G08B 25/00 (2006.01)
G08B 25/10 (2006.01)
G08B 31/00 (2006.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.06.2015 PCT/US2015/033878**

(87) Fecha y número de publicación internacional: **10.12.2015 WO15187768**

(96) Fecha de presentación y número de la solicitud europea: **03.06.2015 E 15802735 (9)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2019 EP 3164663**

(54) Título: **Método de defensa y rechazo**

(30) Prioridad:

03.06.2014 US 201462006976 P
09.03.2015 US 201562130367 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.07.2020

(73) Titular/es:

THE SECURITY ORACLE, INC. (100.0%)
1303 Lattimore Drive
Clermont, Florida 34711, US

(72) Inventor/es:

BUTLER, JR., CHARLES LANKFORD;
SMITH, SAMUEL MCARTHUR y
KIMBALL, VONTELLA KAY

(74) Agente/Representante:

BUENO FERRÁN , Ana María

DESCRIPCIÓN

Método de defensa y rechazo

Antecedentes de la invención

Campo de la invención

Realizaciones del método y sistema actualmente divulgadas incluyen una red de dispositivos informáticos, sensores y accionadores que operan de manera conjunta con un software de aplicación para detectar activamente, identificar y localizar amenazas y generar contramedidas en tiempo real diseñadas para retardar y/o mitigar el daño que puede provocarse por las amenazas.

Antecedentes de la técnica relacionada

El daño a activos físicos, tales como estaciones eléctricas o de suministros, puede resultar en una interrupción generalizada y un coste significativo. Por ejemplo, existen aproximadamente 55.000 subestaciones de energía eléctrica en los Estados Unidos y en cada caso los daños pueden costar entre unos pocos millones a decenas o cientos de millones de dólares en activos físicos perdidos e ingresos perdidos a partir de la interrupción de la energía. Además, los sistemas de protección pasivos actuales no pueden proteger contra ataques de estilo terrorista. Adicionalmente, los sistemas de protección pasivos actuales no cumplen con las regulaciones implementadas por la Comisión Federal Regulatoria de Energía (FERC) del 20 de noviembre de 2014, que ha generado un gran interés para encontrar una forma mejorada de evitar que los adversarios ataquen con éxito ciertas infraestructuras críticas, así como otras infraestructuras similares.

La técnica anterior en este campo consiste en seguridad física en forma de seguridad humana presencial y personal de respuesta. Sin embargo, la presencia de fuerzas estacionarias presenciales es prohibitivamente cara. Adicionalmente, las fuerzas de respuesta habitualmente tardan entre 3-5 minutos en el mejor de los casos y hasta 3 horas en llegar. Para entonces, el daño ya se ha hecho.

Otra forma de seguridad de la técnica anterior en este campo consiste en sistemas de protección física pasivos, tal como, por ejemplo, cámaras de detección, vallas de protección balística u obstáculos de acceso, etc. Sin embargo, los sistemas de protección física pasivos pueden superarse debido a una falta de resistencia activa del adversario. Tales sistemas también fallan al tomar otras medidas activas y/o contramedidas para mitigar y/o acabar con la amenaza expuesta al activo físico. Otra insuficiencia es el fallo de responder adaptativamente a un suceso, tal como un ataque de tipo terrorista, para coordinar respuestas, optimizar resultados y minimizar daños. Además de fallar en una resistencia activa del adversario, los sistemas de la técnica anterior no hacen nada para operar de manera conjunta con la seguridad física una vez que ésta llega.

El documento US 2006/0031934 A1 divulga un sistema que usa una red distribuida para evaluar la condición de una ubicación y generar informes relacionados con el nivel de seguridad de la ubicación. El sistema usa múltiples muestras de datos para generar una estimación de probabilidad de una amenaza de seguridad (es decir, un cambio en nivel de seguridad). Puede sonar una alarma en relación a la condición en una ubicación que la eleva a una condición de alerta.

EL documento US 2004/0257223 A1 divulga un sistema para supervisar un activo (ya sea fijo o móvil) que incluye un o más agentes asociados al activo para comunicar datos acerca de la seguridad del activo a una unidad de control maestra. Los agentes son sensores que detectan ciertas características de un entorno en el que se sitúa el activo. Aunque esta solicitud sí describe la respuesta a una amenaza identificada, la respuesta es una respuesta predeterminada almacenada en una base de datos y se basa solamente en el tipo de amenaza. El documento US 8 384 542 B1 divulga un sistema de seguridad para proteger una instalación en un área definida de una amenaza terrorista, presentando módulos y barreras de construcción blindados con túneles para proteger una vía de comunicación entre el sensor y el subsistema de contramedidas.

La incapacidad de la técnica anterior para interceptar inmediata, activa o físicamente adversarios, especialmente más allá del perímetro del área donde se ubica el activo físico, es una razón de por qué los adversarios pueden moverse rápidamente a través de su secuencia de ataque sin retraso o interrupción hacia su objetivo. La capacidad de un sistema para realizar una función de este tipo puede proteger no solo activos físicos de incidencias hostiles, sino que, cuando se implementa de acuerdo con el método divulgado, también puede cumplir con las regulaciones de la FERC.

Breve sumario de la invención

Los componentes del sistema pueden incluir un ordenador y una red de comunicaciones, un sensor, un accionador, software de aplicación, diversas interfaces y *human-in-the-loop* (presencia humana en el bucle). Operando de manera conjunta a través del software de aplicación, el sistema puede generar respuestas automatizadas a eventos (por ejemplo ataques, terrorismo, vandalismo, robo, eventos meteorológicos, etc.) que pueden variar de estar totalmente automatizadas a estar condicionadas a que un usuario ejecute las mismas. El sistema emplea sensores que detectan, identifican y localizan amenazas adversarias probables de modo que accionadores no letales pueden actuar automáticamente a distancia para debilitar al adversario y/o atenuar la amenaza que éste representa. Algunas realizaciones proporcionan un hardware de control remoto que puede ser usado por el *human-in-the-loop* para adquirir objetivos en remoto y ejercer a discreción en cuanto a si disparar ciertos accionadores para retardar al adversario. Un software adicional puede ayudar al *human-in-the-loop* para adquirir automáticamente objetivos y desarrollar respuestas en tiempo real basándose en escenarios aprendidos ejecutados por el sistema. El sistema utiliza un bucle de realimentación continuo para detectar dinámicamente y priorizar las amenazas a medida que se desarrollan y generar contramedidas para retardar activamente el efecto resultante de las mismas. En el caso de un ataque terrorista, el sistema puede usarse para retardar lo suficiente al terrorista en l consecución de sus objetivos lo suficiente como para habilitar la participación del personal de respuesta.

Como ejemplo, los sensores pueden detectar la presencia no autorizada de personal cerca de las instalaciones de una subestación de energía eléctrica y automáticamente dirigir las cámaras, iniciar secuencias de alarma, adquirir señales objetivo y apuntar armamento (no letal y/o letal) al personal. Un usuario puede a continuación ser capaz de tomar el control de ciertos componentes (remota o directamente) para administrar una medida no letal para repeler al adversario con el beneficio del ahorro de tiempo gracias a accionadores que ya están dirigidos a los adversarios. Pueden preferirse accionadores no letales, que pueden existir en forma de emisiones directas de luz, sonido, ondas magnéticas, químicos, etc. Tras la detección del adversario, el sistema puede ejecutar probabilidades de resultados basándose en datos en tiempo real y escenarios aprendidos para generar objetivos y otras secuencias de contramedida, de modo que los accionadores y sensores apropiados se implican inmediatamente en la respuesta. Estas secuencias de contramedidas pueden presentarse al *human-in-the-loop* mediante una interfaz en una pantalla de ordenador, habilitando así que el *human-in-the-loop* lleva a cabo la contramedida. Además, o como alternativa, pueden emplearse las secuencias de contramedida para preparar accionadores y sensores para una ejecución condicionada por *human-in-the-loop* y/o el sistema puede accionar automáticamente algunos o todos los componentes sin la ejecución condicionada por el usuario.

Puede usarse un software de control lógico para implementar algoritmos de toma de decisiones con el fin de iniciar secuencias preparatorias de la respuesta a la amenaza. Puede usarse un software de razonamiento automatizado para determinar (en tiempo real y/o mediante parámetros preprogramados) qué eventos aborda el sistema y hasta qué grado el sistema ordena y controla los componentes del sistema para generar una respuesta automatizada a la amenaza. El bucle de realimentación continuo habilita que el sistema determine casi instantáneamente la mejor forma de actuar, considerando factores de daño colateral, tiempo de respuesta de seguridad física, minimización de costes y daño físico en un conjunto de contramedidas que se amplían a una respuesta o una etapa preparatoria activa para la respuesta.

El cierre de los lapsos de tiempo entre detección, respuesta y neutralización de la amenaza permite la realización de mejoras de rendimiento que los sistemas de protección pasivos son incapaces de alcanzar y detiene de forma efectiva un ataque mientras cumple con las nuevas regulaciones de la FERC. Además, se generan eficiencias con respecto a las comunicaciones, el almacenamiento de datos y la reducción de infraestructura mediante la coordinación de actividades de los diversos componentes de acuerdo con escenarios aprendidos y secuencias de contramedidas, reducción de sistemas ineficientes y redundantes y asignación eficiente de recursos de cálculo y de almacenamiento de datos.

El método y sistema permiten frustrar ataques y/o provocar un retardo significativo a adversarios casi instantáneamente (por ejemplo, menos de aproximadamente 3 a 5 segundos) y se permite al *human-in-the-loop* la oportunidad de enfrentarse repetidamente al adversario, si es necesario desde una ubicación remota.

Mientras el método y el sistema se describen en relación con la protección de una subestación, la aplicación se extiende a cualquier situación en la que se espera un riesgo de daño a un activo físico y/o área, y son suficientes medidas no letales para abordar el riesgo, o incluso se prefieren. Se puede tratar, sin limitación, de casas, barcos, complejos industriales, aeropuertos, puertos de carga, etc. El sistema también puede emplearse en otras situaciones en las que pueden desarrollarse exigencias similares, tal como el control de multitudes y masas (por ejemplo salas de conciertos, lugares de protesta, disturbios, etc.).

Mientras que estas ventajas potenciales son posibles mediante las soluciones técnicas aquí ofrecidas, éstas no es necesario que se consigan. El sistema aquí divulgado puede implementarse para conseguir ventajas técnicas, tanto si se buscan o consiguen estas ventajas potenciales, individualmente o en combinación, como si no. La invención se define por las reivindicaciones adjuntas.

Otras características, aspectos, objetos, ventajas y posibles aplicaciones de la presente invención serán evidentes a partir de un estudio de las realizaciones ilustrativas y ejemplos descritos a continuación, en combinación con las Figuras, y las reivindicaciones adjuntas.

Breve descripción de las figuras

Los otros objetos, aspectos, características, ventajas y posibles aplicaciones anteriores de la presente invención serán más evidentes a partir de la siguiente descripción más detallada de los mismos, junto con las siguientes figuras, en las que:

Fig. 1: ilustra componentes que pueden usarse con el sistema de defensa y rechazo;
Fig. 2: ilustra una red informática que puede usarse con el sistema;
Fig. 3: diagrama de bloques de las etapas de decisión que pueden ser tomadas por el software de aplicación;
Fig. 4A y 4B: visualizaciones de un modelo simulado que puede ser generado por el sistema basándose en las reglas de decisión;
Fig. 5A y 5B: diagramas de flujo de bucles de realimentación continuos para una versión que usa un software de control lógico y una versión que usa un software de razonamiento automatizado, respectivamente, que pueden usarse con el sistema;
Fig. 6A-C: visualización de modelado de análisis de fallo, un informe coste-beneficio y un informe resumen de resultado, respectivamente, que pueden ser generados por el sistema;
Fig. 7A y 7B: visualización de un diseño de sistema protector físico pasivo con adversarios coordinando un ataque e ilustración del tiempo requerido para que el sistema supere el sistema protector físico pasivo, respectivamente;
Fig. 8A y 8B: muestran una disposición de sensores de múltiple fenomenología que puede establecerse por el sistema y un visualizador que demuestra las acciones coordinadas de los componentes del sistema para frustrar un ataque, respectivamente;
Fig. 9: diagrama de flujo para un método de utilización del sistema; y,
Fig. 10: Espectro de Amenaza Base de Diseño ilustrativo.

Descripción detallada de la invención

La siguiente descripción es de una realización aquí contemplada para la realización de la presente invención. Esta descripción no debe tomarse en un sentido limitante, sino que se hace meramente con el propósito de describir los principios generales y las características de la presente invención. El alcance de la presente invención debería determinarse con referencia a las reivindicaciones.

En referencia ahora a la Fig. 1, los componentes del sistema pueden incluir una red informática 100, al menos un sensor 10, al menos un accionador 20, un software de aplicación 30, un *human-in-the-loop* e interfaces de usuario que operan de manera conjunta, generando respuestas automatizadas a sucesos. Los sensores 10 pueden detectar, identificar y localizar amenazas probables representadas por los sucesos. El software de aplicación 30 determina la mejor forma de actuar (o múltiples formas de actuar con resultados probabilísticos) por la que se ejecuta una operación concertada de los componentes del sistema para abordar las amenazas. El sistema puede ejecutar probabilidades de resultados basándose en escenarios aprendidos y presentar éstos al usuario a través de un visualizador en un dispositivo informático 101 o ejecutar contramedidas y/o medidas preparatorias automáticamente. Algunas realizaciones permiten que un usuario ejecute contramedidas a través de los módulos 109 y/o paneles 110 (véase la Fig. 2) visualizados por el software de aplicación 30 a través de interfaces gráficas de usuario (GUI). Además, puede usarse un bucle de realimentación dinámico continuo para proporcionar respuestas en tiempo real dinámicas y adaptativas a medida que evolucionan los eventos.

Puede usarse la técnica de fusión de sensores y otras técnicas para comprobar si la presencia cerca de un área/activo protegido es una amenaza. Se generan respuestas medidas en forma de contramedidas mediante las cuales los accionadores 20 pueden usarse para actuar a distancia del activo físico/área con el fin de debilitar e incapacitar a los adversarios de manera no letal antes de que puedan moverse dentro de un alcance en el que puedan provocar daño al activo físico/área. Las respuestas son acordes al nivel de amenaza presentada. Por ejemplo, un activista que solo intenta hacer una declaración política allanando y entrando, puede ser sometido a una secuencia de avisos tras su detección antes de medidas que puedan provocar efectos debilitantes, mientras que a un adversario armado se le puede someter a medidas lesivas, aunque no letales, tras la detección.

Red informática

Haciendo referencia ahora a la Figura 2, la red informática 100 puede incluir una pluralidad de dispositivos informáticos 101, servidores informáticos 102, bases de datos 103, redes de comunicación 104 y rutas/conexiones de comunicación 108. Un usuario del sistema puede usar al menos un dispositivo

procesador 105, de almacenamiento de memoria 106a, 106b e interfaz de comunicaciones 107 para comunicar y ejecutar comandos. Cada servidor informático 102 puede conectarse a al menos una base de datos 103, en la que un software de aplicación 30 ejecutado por cada dispositivo informático 101 puede realizar funciones de almacenamiento, integración, configuración y transmisión de datos. El software de aplicación 30 puede almacenarse en cualquier tipo de medio o medios legibles por ordenador o adecuados. Éstos pueden ser un medio o medios legibles por ordenador no transitorios, tal como un medio de almacenamiento magnético, un medio de almacenamiento óptico o similar. Más adelante se analizarán posibles arquitecturas de sistema informático para la red informática 100.

El sistema puede incluir el control remoto de los diversos componentes por el *human-in-the-loop*. Esto puede conseguirse mediante un sistema de cableado eléctrico coaxial, por cable y/o líneas ópticas, yendo desde los diversos accionadores 20 y sensores 10 a los dispositivos informáticos (que pueden o no estar dentro de la sala de control). El control remoto también puede incluir comunicaciones inalámbricas en longitudes de onda infrarroja, ultrasónica, de radio y/u otras longitudes de onda electromagnéticas de transmisión de luz configuradas para transportar información codificada con el fin de ejecutar diversas funciones. Por ejemplo, un dispositivo informático 101 de la sala de control puede comunicarse a través de un sistema de transmisores, receptores y/o transceptores con los accionadores 20 y sensores 10 para dirigir la operaciones de los mismos (por ejemplo movimiento motriz de accionadores, sensibilidad de sensores, dirección de exploración de sensores, etc.).

El sistema puede operar con comunicaciones seguras vía encriptación. Por ejemplo, puede utilizarse una encriptación de curva elíptica de 2048 bits y 4096 bits sistémica a lo largo de toda la red informática 100 para protegerlo de una toma de control no autorizada, interrupción de componentes o interrupción del sistema en su totalidad. Esta tecnología de encriptado sistémico puede, en parte, usar microchips que soportan los algoritmos de encriptación embebidos en componentes del sistema configurados para transmitir datos y comunicarse mediante enlaces (por ejemplo a través de Ethernet, IP, SCADA, sistemas de control de automatización digitales, etc.). Además, pueden usarse conmutadores de ciberseguridad, tal como conmutadores de Ethernet ciber protegidos, gestionados, industriales de sistemas de control e información, para proporcionar protección multicapa. Un ejemplo de conmutador puede incluir el conmutador de ethernet de ciberseguridad Tungsten™ de Sensar. Los conmutadores de ciberseguridad pueden configurarse para supervisar la fibra frente a intentos de ataque (por ejemplo pirateo informático, escucha clandestina, manipulación, etc.) detectando cambios en la longitud de la fibra, cambios repentinos en la atenuación, etc., pudiendo el ciber conmutador interrumpir el enlace cuando se detecta un ataque. Reestablecer el enlace puede requerir rehabilitar el enlace manualmente.

Pueden utilizarse otras formas de supervisión y conmutación, según se establezcan mediante una política de seguridad programada en el sistema. Por ejemplo, la supervisión puede producirse en cada puerto, de modo que tras la detección de una brecha de seguridad producida en cualquier puerto, o cualquier elemento de red conectado al puerto, puede ejercerse una acción (por ejemplo crear un registro o incluso aislar un puerto). La detección de brechas puede conseguirse mediante la identificación de puertos silenciados, cambios en la longitud del cable, cambios en la atenuación de la fibra, cambios en el consumo de energía de PD de Alimentación a través de Ethernet (PoE), etc.

Sensor

Los sensores 10 pueden usarse para detectar ocurrencias y recopilar datos con respecto a las ocurrencias. Los datos de los sensores, accionadores y/o de contramedidas del sistema pueden transmitirse a un dispositivo informático 101, a otro sensor 10 y/o a un accionador 20. La transmisión puede producirse a través de uno de los esquemas de transmisión por cable o remotos descritos anteriormente y/o a través de cualquiera de las rutas/conexiones de comunicación 108 de la red informática 101. Además, algunos sensores 10 pueden conectarse al sistema mediante una configuración de sistema en circuito cerrado.

Los sensores 10 incluyen cualquier dispositivo que puede usarse para detectar y registrar características del entorno, que pueden incluir luz, movimiento, temperatura, presión, etc. Por ejemplo, un sensor 10 puede ser un dispositivo semiconductor que cambia la conductancia eléctrica basándose en cambios de luz, presión, etc., creando de este modo un conmutador condicionado. Pueden usarse otras técnicas de conmutación/sensor, que pueden incluir, sin limitación, sensores de campo visual, sensores sísmicos, sensores acústicos y de audio, sensores de reconocimiento de anomalías y patrones, sensores y conjuntos de detección de disparos, radares en fase de radiofrecuencia, etc.

Otros sensores 10 adicionales pueden incluir sensores de Radar de Vigilancia Horizontal (HSR) con un alcance operativo de hasta 360 grados de exploración continua y zonas de control programables ilimitadas para áreas en tamaño entre 4.050 metros cuadrados (1 acre) hasta más de 16 kilómetros cuadrados (10 millas cuadradas). Pueden emplearse LIDAR usando algoritmos analíticos de detección de anomalías y/o detectores de movimiento, junto con otros detectores que pueden detectar cambios en la geometría de un área de vigilancia.

Algunos sensores 10 pueden ser sensores activos que emiten frecuencias activas a lo largo de toda el área de vigilancia para activar/energizar transceptores pasivos, reflectores, etiquetas de RFID, etc. transportados por fuerzas amigas (por ejemplo, personal de seguridad física, personal de respuesta, etc.). Señales emitidas desde los transceptores pasivos son adquiridos y procesados por el sistema para distinguir y diferenciar entre adversarios y no adversarios. Por ejemplo, pueden configurarse transceptores pasivos para resonar y excitarse a las frecuencias transmitidas por los sensores activos 10, emitiendo así una señal que puede ser detectada por otros sensores 10 del sistema. Con el uso de tales sensores activos 10 y transceptores pasivos, el sistema puede usar un procesamiento de señales y técnicas de correlación para identificar las posiciones y movimientos de fuerzas amigas, identificando las fuerzas amigas como aquellas que emiten una señal firma desde un transceptor pasivo.

También pueden usarse diversas cámaras como sensores 10, que pueden emplearse con un software de reconocimiento de imágenes para ayudar a la identificación de objetos. Por ejemplo, una cámara puede ser un dispositivo de imagen térmica, que puede usar la formación de imágenes térmicas ferroeléctricas para detectar cambios en la capacitancia como intermedio para los cambios térmicos. Puede crearse un plano focal pixelado dentro de la cámara para detectar cambios en una matriz 2D con el fin de determinar un patrón de imagen térmica. A continuación, los datos del plano pixelado pueden procesarse, almacenarse y transmitirse de acuerdo con un software de reconocimiento, según se necesite. Otras cámaras pueden incluir cámaras de reconocimiento de objetos 3D. Tales cámaras habitualmente emplean un software de reconocimiento 3D que genera una imagen 3D de un objeto a partir de una representación 2D usando técnicas de representación de vectores latentes. Pueden usarse otras cámaras y técnicas de captura de imágenes, que pueden incluir, sin limitación, RADAR térmico, LIDAR, LADAR, ultrasónica, visión nocturna, etc.

Algunas realizaciones incluyen cámaras que emiten y detectan iluminación de IR a y por encima de 940 nm para habilitar la detección nocturna a través de la cámara sin emitir un haz de IR visible a simple vista. Otras cámaras pueden equiparse con una capacidad de procesamiento especial para generar imágenes durante el mal tiempo, tal como formación de imágenes controlada por alcance, formación de imágenes de tiempo de vuelo directo, etc. Por ejemplo, en la formación de imágenes controlada por alcance, una fuente láser puede iluminar el campo de visión mediante luz láser pulsada. Con la luz pulsada y una obturación controlada de la lente puede generarse una imagen libre de los reflejos que se provocarían de otra manera debido a objetos que dispersan luz en el campo de visión (por ejemplo nieve). Otras cámaras pueden incluir cámaras resistentes a explosiones y balas.

Los sensores 10 pueden incluir sensores telemétricos y de posición, que pueden emplean luz láser y optoelectrónica para comprobar la presencia de un diferencial en los impulsos de luz emitida y reflejada. El diferencial puede usarse para determinar la posición y el movimiento de un objeto. Los sensores telemétricos 10 pueden usarse junto con cualquiera de las cámaras anteriores para desarrollar una representación 3D de un área y cualquier objeto (por ejemplo, un adversario) en tiempo real, que puede visualizarse en uno de los dispositivos informáticos 101 a través de un módulo 109 y/o panel 110. Otras técnicas telemétricas y de detección de posición pueden incluir la detección de RADAR por radio o microondas.

Los sensores 10 pueden usarse de diversas formas. Por ejemplo, los sensores de campo visual 10 pueden usarse en conjunto con, o puede fijarse a, un accionador 20 para ayudar a apuntar al accionador 20. Los sensores sísmicos y de audio 10 pueden usarse para detectar sonidos u otros sucesos vibracionales indicativos de una actividad malintencionada o sospechosa. Como ejemplo, un sensor de audio 10 puede equiparse con una circuitería resonante y de excitación para resonar en un sonido sintomático de un disparo y transmitir una señal al sistema cuando se detecta un sonido de este tipo. Los sensores sísmicos 10 pueden configurarse de forma similar para detectar vibraciones indicativas de ciertos tipos de motores al ralentí cerca de un área de interés.

Pueden usarse una pluralidad de sensores 10 para generar una colección y correlación de datos, que pueden usarse para formular evaluaciones, mediante un software de aplicación 30, para identificar una amenaza y/o la gravedad de la amenaza que un suceso pueda representar. Por ejemplo, datos de sensor que detectan tres personas moviéndose en un movimiento concertado y en una formación particular pueden determinarse como adversarios, generando el sistema, mediante servo accionadores 20, contramedidas no letales pero debilitantes. Sin embargo, puede determinarse que los datos de sensor que detectan tres personas moviéndose cerca erráticamente son intrusos no hostiles, controlando el sistema mediante servo alertas de audio para informar a las personas que son intrusos y deberían salir de las instalaciones. En esta última situación, la respuesta también puede incluir un breve control mediante servo de un accionador cegador láser 20 para intensificar el aviso. El software 30 para realizar tales análisis y evaluaciones puede incorporarse en el motor de razonamiento automatizado y/o en el software de control lógico.

Además de las capacidades de detección de los sensores 10 y la analítica del software 30, pueden usarse otras técnicas para ayudar con la detección, identificación y localización de amenazas. Éstas pueden incluir

sensores inteligentes calibrados, fusión de sensores, analítica en tándem, interfaces programables de la aplicación (API), etc. La API habilita que el software de aplicación 30 del sistema, tal como el motor de razonamiento automatizado por ejemplo, actúe como una plataforma de red de software a través de programas de aplicación y componentes de hardware del sistema. Algunas de estas técnicas también pueden usarse para mejorar el funcionamiento de los componentes del sistema en ciertas condiciones. Por ejemplo, si el mal tiempo impide la detección mediante un cierto tipo de sensor, técnicas tal como fusión de sensores, por ejemplo, pueden habilitar la detección continuada aplicando estadísticas predictivas a datos correlacionados adquiridos de otros sensores 10.

Accionador

Los accionadores 20 pueden usarse para ejecutar las contramedidas ordenadas por el sistema a través del software de aplicación 30 y/o *human-in-the-loop*. Los accionadores 20 pueden estar en comunicación con un dispositivo informático 101, otro accionador 20 y/o un sensor 10 para recibir/transmitir datos de accionador, datos de sensor y/o datos de contramedidas desde el sistema. Puede conseguirse la transmisión de datos y comunicaciones entre el accionador 20 y componentes del sistema de manera similar a la de los sensores 10 descritos anteriormente, incluyendo el uso de API. El software con control de algoritmos y los algoritmos de toma de decisiones pueden procesar los datos de sensor y de accionador desde las API de sensores y APIS de accionadores para controlar activamente los sensores 10 y accionadores 20. En este sentido, algunos sensores 10 y accionadores 20 incluyen conjuntos de torreta, conjuntos de cardán y similares para habilitar un movimiento articulado.

Ejemplos de accionadores 20 pueden ser dispositivos que emiten luz, sonido, radiación de microondas, químicos, objetos en masa, etc. en una dirección deseada con una trayectoria deseada, que pueden procurarse de empresas tal como WatchStander® o Precision Remotes®. Los accionadores 20 se configuran para implementar contramedidas a amenazas de forma que las emisiones desde los mismos deberían provocar la interrupción, distracción, dolor, lesiones o incluso la muerte si es necesario. Por ejemplo, los emisores de luz pueden incluir deslumbradores láser para emitir luz visible dirigida hacia humanos, provocando una ceguera temporal, o una luz infrarroja dirigida hacia sensores y otra electrónica para interrumpir operaciones electrónicas que pueden ser empleadas por los adversarios. Los emisores químicos pueden incluir gas lacrimógeno y otros agentes pulmonares, nerviosos y/o irritantes. Otros emisores pueden incluir generadores de impulsos electromagnéticos, generadores sónicos o ultrasónicos, cañones de agua, armas de bolas de goma, armas de redes, armas de espuma, etc. Los efectos de las emisiones pueden provocar ceguera temporal, náuseas, vómitos, dolores de cabeza, pérdida auditiva, dolor subcutáneo, convulsiones, etc.

Otros accionadores 20 pueden incluir compuertas controladas remota y electrónicamente, puertas, barreras de personal y otros dispositivos que actúan como obstáculos de seguridad pasivos. Algunos de éstos pueden incluir dispositivos pasivos que ya son parte de un sistema físico pasivo existente, como el sistema de defensa y rechazo puede usarse para aumentar sistemas físicos pasivos (si ya están instalados o se instalan simultáneamente con el sistema de defensa y rechazo).

Las respuestas coordinadas administradas por los accionadores 20 son una contramedida usada para mitigar el daño presentado por un suceso y/o extinguir su amenaza. Una contramedida puede incluir una medida activa tomada en preparación de una ocurrencia prevista; por tanto, las contramedidas no se limitan solo a respuestas a un evento. Por ejemplo, escenarios aprendidos pueden informar al sistema que si se administra una contramedida particular, a continuación los adversarios intentarían realizar ciertos actos defensivos; por tanto, el sistema controlaría mediante servo automáticamente accionadores adicionales en preparación. Por tanto, generar una contramedida puede incluir el desencadenamiento concertado de una pluralidad de accionadores 20 para generar el resultado esperado.

Pueden emplearse diferentes secuencias y combinaciones de intensidad de respuesta de accionador y tasa de respuesta basándose en las circunstancias, según sea determinado por el software de aplicación 30 y/o el *human-in-the-loop*. Los accionadores 20 pueden trabajar independientemente o de una coordinada en este sentido. El efecto resultante en un adversario puede ser obstaculizar sus sentidos de vista, sonido y tacto al menos hasta que la seguridad física llega para enfrentarse al mismo. Por ejemplo, una contramedida puede incluir la actuación de un accionador de microondas 20 para producir una sensación de quemazón momentos antes de la actuación de un deslumbrador láser accionador 20, que puede ser seguido por una emisión ultrasónica, de modo que el adversario experimenta una cierta sensación psicofisiológica. Los accionadores no letales 20 pueden actuar sobre el adversario no solo para suprimirlo, sino también para interrumpir sus movimientos y frustrar su objetivo. Por lo tanto, el sistema no solo retarda al adversario lo suficiente como para ganar un tiempo muy necesario para que la seguridad física y el personal de respuesta se enfrenten, sino también frustra un ataque completamente sin la necesidad de una fuerza letal. Los sensores 10 y los accionadores 20 pueden colocarse para detectar y actuar sobre un adversario mucho antes de que el adversario entre en contacto con el perímetro del área física.

Software de aplicación

El software de aplicación 30 puede incluir un motor de razonamiento automatizado, software de control lógico y/u otro software (por ejemplo, software de conexión por interfaz, software de adquisición de objetivo, etc.). El motor de razonamiento automatizado emplea inteligencia artificial y el aprendizaje de máquina para generar automáticamente contramedidas y ejecutar respuestas. El software de control lógico emplea algoritmos de toma de decisiones para implementar secuencias de acuerdo con contramedidas, pero sin una ejecución automática de la respuesta. El sistema puede usar cualquier combinación del software descrito anteriormente para conseguir el grado de automatización deseado.

Motor de razonamiento automatizado

En referencia a la Fig. 3, el motor de razonamiento automatizado es un software que habilita la automatización de los componentes de sistema para generar contramedidas que analizan y responden adaptativamente al evento. Una integración sinérgica de sensores 10 identifica el evento, realizando un análisis de tipo DAFO (debilidades, amenazas, fortalezas y oportunidades) inmediato para localizar las potenciales amenazas que el evento representa. Un bucle de realimentación implementado por el motor de razonamiento automatizado (véase la Fig. 5B) usa los datos de sensor y del accionador para generar adaptativamente contramedidas en tiempo real y/o por comandos preprogramados para ejecutar respuestas automatizadas que se orquestan y se adaptan a los cambios en tiempo real.

Puede usarse inteligencia de máquina para identificar y localizar las amenazas representadas por un evento, de modo que pueden generarse contramedidas para minimizar daños. Las amenazas se determinan mediante el sensor de modelado y análisis y datos de accionador para comprobar el riesgo potencial que representa el evento. Si el evento genera un factor de riesgo por encima de un umbral, a continuación puede categorizarse como una amenaza. Por ejemplo, un evento puede ser la caída de una rama de árbol que el sistema ha detectado. Debido a que no se registra ninguna firma de calor (por ejemplo, sensores de infrarrojos), no se detecta movimiento adicional (por ejemplo, sensores de movimiento), no se detecta ningún arma (por ejemplo, frecuencias de RADAD reflejadas), y no se detecta ningún material explosivo (por ejemplo, sensores químicos, radiológicos, etc.), el sistema puede no clasificar este evento como una amenaza. Como otro ejemplo, un evento puede ser una persona caminando por una calle cerca del perímetro, que puede no clasificarse como amenaza si la persona continúa caminando. Si la persona se detiene durante un periodo de tiempo a lo largo de la valla del perímetro, este suceso puede clasificarse a continuación como una amenaza que justifica un aviso audible emitido desde un accionador 20. Si la persona continúa situándose cerca de la valla incluso después del aviso, la amenaza puede elevarse para justificar una contramedida mejorada. La interacción de componentes de sistema y la posible respuesta pueden ilustrarse con los siguientes dos escenarios producidos en una subestación de transmisión de energía eléctrica situada en un punto relativamente bajo en un valle fluvial rural caracterizado por suaves colinas y terreno irregular. Cada escenario incluye una situación en la que la vegetación en el área que rodea inmediatamente la subestación se limita a hierba corta, existe una entrada de coches de 300 metros que conduce al lado norte de la subestación desde una carretera secundaria al norte, el momento es media tarde y no hay nadie presente en la subestación que está en modo seguro.

En un primer escenario, un cazador se aproxima a la vecindad de la subestación a pie avanzando de este a oeste a lo largo del lado norte de la subestación. Sensores de cámara térmica equipados con analítica de vídeo y sensores de radar en fase de RF detectan esta actividad, y el sistema de defensa y rechazo clasifica al cazador como el nivel más bajo de amenaza por la que se sitúa en observación activa. En esta etapa, un sistema de gestión de video de seguridad (VMS) notifica la amenaza al control de seguridad a través de una GUI de VMS para observación (que puede ser parte de la GUI de comando y control 60 - véanse las Figuras 8A y 8B). Los sensores de cámara térmica equipados con analítica de vídeo y los sensores de radar en fase de RF continúan notificando a un coordinador inteligente (IC) la posición relativa del cazador con la subestación, y una vez que el cazador ha progresado a dentro de 300 metros de la subestación (u otra distancia predeterminada), el sistema de defensa y rechazo reclasifica al cazador como una amenaza media y el VMS de seguridad notifica este aumento de amenaza al control de seguridad a través de la GUI de VMS para observación donde el personal de sala de control de seguridad determina que el cazador está portando un rifle de gran calibre.

El cazador a continuación dispara un único tiro a un ciervo y dentro de uno o dos segundos el sensor de sistema de detección de disparos de analítica de audio integrado de defensa y rechazo geolocaliza el destello de boca del rifle y simultáneamente determina la trayectoria de la bala informando de esta información al IC. Basándose en la trayectoria de la bala, el IC mantiene clasificación del cazador en el nivel de amenaza media ya que no hay intención malintencionada aparente de provocar daño a la subestación.

De acuerdo con reglas de políticas de confrontación (a través de reglas de decisión programadas en el software de aplicación), el IC dirige un accionador integrado de sistema de defensa y rechazo presencial, equipado con un foco de 129 millones de lux (12 millones de fc), un deslumbrador láser, y LRAD para enviar

un mensaje de aviso de seguridad grabado al cazador a un nivel de volumen que se ajusta para la distancia al cazador, de modo que el mensaje alcanza al cazador en un estado claramente audible, pero no tan alto como para asustar al cazador. El mensaje de aviso de seguridad insta a prácticas de caza seguras, incluyendo evitar trayectorias que pondría en riesgo balas impactando infraestructura de subestación.

En el segundo escenario, un adversario se aproxima a la vecindad de la subestación a pie avanzando de este a oeste a lo largo del lado norte de la subestación. Sensores de cámara térmica equipados con analítica de vídeo y sensores de radar en fase de RF detectan esta actividad, en los que el sistema de defensa y rechazo clasifica el adversario como el nivel más bajo de amenaza y le sitúa bajo observación activa. En esta etapa, el VMS notifica la amenaza al control de seguridad a través de la GUI de VMS para observación. Sensores de cámaras térmicas equipados con analítica de vídeo y los sensores de radar en fase de RF continúan notificando al IC la posición relativa del adversario con la subestación, y una vez que el adversario ha progresado a dentro de 300 metros de la subestación (u otra distancia predeterminada) el sistema de defensa y rechazo reclasifica el adversario como una amenaza media y el VMS notifica este aumento de amenaza al control de seguridad a través de la GUI de VMS para observación donde el personal de sala de control de seguridad determina el adversario está portando un rifle de gran calibre.

El adversario comienza a correr hacia la subestación y después de entrar dentro de, por ejemplo, 100 metros de la subestación adopta una posición prona con un rifle apuntando a la subestación. Basándose en la velocidad del adversario y que está acortando la distancia entre él mismo y la subestación, el IC le reclasifica a un nivel de amenaza media alta. El adversario a continuación dispara un único tiro a la infraestructura de subestación (depósito de aceite refrigerante de transformador), y dentro de uno o dos segundos el sensor de sistema de detección de disparos de analítica de audio integrado de defensa y rechazo geolocaliza el destello de boca del rifle y simultáneamente determina la trayectoria de la bala informando de esta información al IC. Basándose en la trayectoria de la bala, el IC reclasifica el adversario en el nivel de amenaza más alto y como un francotirador implicado en el acto de disparar con intención de provocar daño a la subestación.

Para distraer inmediatamente al francotirador y degradar su capacidad de disparar con precisión al sitio protegido, el IC dirige un accionador integrado de sistema de defensa y rechazo presencial, equipado con un foco de 129 millones de lux (12 millones de fc), un deslumbrador láser y LRAD para enfrentarse al francotirador enviando primero un sonido grabado de un explosivo seguido de un breve destello del foco de 129 millones de lux (12 millones de fc) aproximadamente 1/4 de segundo más tarde de modo que ambos alcanzan al francotirador simultáneamente. El francotirador se debilita temporalmente y no dispara un disparo posterior.

Para debilitar, distraer y retardar adicionalmente al francotirador y degradar su capacidad de disparar con precisión al sitio protegido, el IC dirige un accionador integrado de defensa y rechazo presencial, equipado con un foco de 129 millones de lux (12 millones de fc), un deslumbrador láser y LRAD para enfrentarse de nuevo al francotirador disparando el deslumbrador láser para cegar temporalmente al francotirador y proyectar un sonido grabado de lamentos de alto nivel de decibelios simultáneamente al francotirador, que debería provocar que el francotirador se retire y se marche.

También puede usarse inteligencia de máquina para diferenciar entre adversarios y no adversarios de modo que las contramedidas pueden controlar los servo accionadores 20 para apuntar y actuar sobre adversarios, pero no sobre no adversarios (por ejemplo, fuerzas azules). Puede detectarse un no adversario empleando sensores activos 10 que emiten frecuencias activas a lo largo de toda el área de cobertura de detección para energizar transceptores pasivos o reflectores portados por los no adversarios, diferenciando así a éstos de adversarios y protegiéndolos de ser atacados por un accionador 20. Tras identificar las amenazas y no amenazas, el sistema desarrolla un conocimiento de la situación por el cual se generan contramedidas. La priorización de amenazas y los resultados probabilísticos son factorizados por el software de razonamiento automatizado. Pueden generarse contramedidas para influenciar la observación, orientación, toma de decisiones y bucle de acción del adversario durante un ataque. Esto puede incluir interrumpir las maniobras del adversario abrumando, distrayendo y/o suprimiendo al adversario. Mientras uno de los principales parámetros operativos del motor de razonamiento automatizado es generar contramedidas para provocar un retardo, de modo que se otorga un tiempo adicional para que llegue la seguridad física y el personal de respuesta, puede emplearse cualquier interrupción de la operación prevista del adversario que socava su capacidad para lograr un objetivo y proporcionar al personal de seguridad físico ventajas añadidas cuando lleguen.

Por ejemplo, el motor de razonamiento automatizado puede programarse para generar una contramedida para suprimir el movimiento en una dirección, para alentar el movimiento en otra dirección, para forzar al adversario a buscar cobertura en un área en la que representan la menor amenaza de daño al activo físico. Una vez que el personal de seguridad físico llega, el sistema puede cambiar adaptativamente para generar contramedidas que de nuevo fuercen a los adversarios a buscar cobertura en un área, de forma que el personal de seguridad física tiene la ventaja táctica y/o estratégica cuando se enfrenta a éstos. Tal acción

concertada por el sistema dependería del conocimiento de la situación actualizado continuamente a través del bucle de realimentación.

Se programan reglas de decisión en el software 30 para determinar cuándo un evento justifica la generación de una contramedida y qué tipo de contramedida generar. Cuando son aplicados por el sistema, las reglas de decisión factorizan los parámetros y variables derivados de los análisis de conocimiento de la situación, análisis de contingencias, análisis máximo y mínimo relacionado con el activo físico/área y activos colaterales, análisis de coste-beneficio de tomar acción/sin acción, etc. Las reglas de decisión pueden recurrir a tácticas, tal como el control mediante servo de un conjunto de accionadores 20 para forzar al adversario a moverse a diferentes ubicaciones donde aumenta la efectividad de un segundo conjunto de accionadores 20 o disminuye la posibilidad de ataque del adversario.

También pueden usarse reglas de decisión para programar el sistema con fines de seguridad y cumplimiento con reglas de confrontación. Por ejemplo, el software 30 puede programarse de modo que los accionadores 20, cuando apuntan en la dirección de un adversario que está entre los accionadores 20 y una carretera, pueden no disparar al adversario si la trayectoria de los haces está en línea con moristas que pasan. Otros ejemplos de reglas de decisión podrían incluir cómo los accionadores 20 podrían enfrentarse a múltiples objetivos eficientemente factorizando la amenaza representada por cada adversario individual y modificando el comportamiento de confrontación de objetivo del accionador mediante el bucle de realimentación continuo. El bucle de realimentación continuo de información desde los sensores 10 y accionadores 20, junto con el flujo de proceso continuo de la Fig. 3, determina inmediatamente qué contramedidas están teniendo el efecto más deseado en una situación fluida dada y se adapta en consecuencia.

Las reglas de decisión podrían codificarse usando reglas de producción de restricciones de la forma: si objetivo está EN LÍNEA con carretera ENTONCES INHIBIR disparar. En la que EN LÍNEA es una restricción establecida en las posibles ubicaciones objetivo e INHIBIR es una restricción en la acción de disparar. Otra regla podría ser de la forma: si el objetivo está CERCA de un activo crítico ENTONCES el nivel de amenaza es ALTO. En la que CERCA es una restricción sobre la ubicación relativa del objetivo y ALTO es una restricción sobre nivel de amenaza. Puede resolverse a continuación un conjunto jerárquico de estas reglas de producción de restricciones usando uno de los varios algoritmos de toma de decisiones de múltiples atributos bien conocidos para producir las reglas de decisión.

Haciendo referencia ahora a las Fig. 4A y 4B, se divulga un modelo simulado que puede generarse por el sistema basándose en reglas de decisión. Las reglas de decisión pueden programarse para depender del área/activo a proteger y las ocurrencias esperadas a las que el área/activo se expondría para definir amenazas de ocurrencias. Esto puede conseguirse asociando las amenazas con un contexto mediante factores de contexto. Los factores de contexto pueden incluir, sin limitación, factores políticos, ambientales, tecnológicos y sociales. Los factores políticos pueden incluir límites legales de uso de una contramedida, el tipo de área/activo y el nivel de respuesta permitida por la ley para proteger el área/activo u otro activo. Los factores ambientales pueden incluir la topografía del sitio a proteger, la geografía del área, si es de día o de noche, el daño colateral que puede producirse al área/activo u otro activo. Los factores tecnológicos pueden incluir las limitaciones de los accionadores 20 y sensores 10, la disponibilidad de seguridad física, restricciones impuestas por las capacidades de seguridad física y personal de respuesta, etc. Los factores sociales pueden incluir la propensión para provocar daño involuntario a otros, la proximidad a áreas pobladas, etc. Los resultados pueden visualizarse a través de la GUI de factores de contexto 40 mostrada en la Fig. 4A. El razonamiento automatizado y otra programación de software inteligente se describe a continuación y se implementa basándose en las reglas de decisión. Por ejemplo, puede programarse un factor de contexto en las reglas de decisión para evitar el control mediante servo de un accionador emisor de microondas 20 que, si se acciona, puede extenderse más allá de un perímetro predefinido, independientemente del efecto de minimización que pudiera tener del daño presentado por el evento.

Las reglas de decisión forman un conjunto jerárquico de restricciones en el espacio de decisión. Las restricciones se normalizan como metas. Una restricción inhibitoria se normaliza de modo que la inhibición es la inversa lógica de autorización. Una inhibición tiene un grado bajo de autorización. Una meta tiene un alto grado de autorización. La toma de decisiones incluye agregar la autorización de todas las restricciones (metas e inhibiciones) y, a continuación, buscar las regiones en el espacio de decisión con el grado más alto de autorización. Estas, a continuación, se convierten en el conjunto de decisiones. Por ejemplo, supóngase que una regla de objetivo produce una restricción de la forma, el objetivo está en la ubicación X con precisión Y. Esto pone una restricción precisa en la solución de disparo para una decisión de disparo. Otra restricción es de la forma, si campo visual despejado desde accionador hasta el objetivo. Para crear una restricción de campo visual despejado, pueden aplicarse restricciones inhibitorias para todos los obstáculos que podrían cruzar una línea desde el accionador hasta el objetivo para determinar la autorización de campo visual despejado.

De acuerdo con el segundo escenario descrito anteriormente, lo siguiente es un ejemplo que muestra el

uso de las reglas de decisión para generar un bucle de realimentación de decisión del sistema de defensa y rechazo. En el segundo escenario, el adversario es un francotirador terrorista con conocimiento interno de la instalación que ataca la instalación, usando el sigilo y la fuerza para infligir un daño incapacitante a la subestación. Un escenario de este tipo puede encajar dentro de amenaza n.º 1 usando el análisis de Amenaza Base de Diseño (véase la Fig. 10), que se describirá en más detalle a continuación.

Progresión de Eventos

1. El adversario está caminando en paralelo a la línea de la valla del lado norte de la subestación avanzando de este a oeste. La trayectoria del adversario está a más de 300 metros de la valla (u otra distancia predeterminada).

Detección y clasificación

Los sensores de radar en fase de RF pueden producir un evento de movimiento detectado por radar, donde el radar proporciona el alcance, rumbo, la velocidad y el tamaño de objetivo. La ubicación del objetivo puede calcularse a partir del alcance y rumbo en relación con la ubicación y orientación de la antena de radar.

Los sensores de cámara de imágenes térmicas también pueden producir un evento de objeto térmico detectado. El software de detección de cámara de imágenes térmicas puede precalibrarse registrando objetos existentes en el campo de visión. Exploraciones posteriores pueden comparar los objetos detectados en la actualidad con los objetos prerregistrados. Cualquier nuevo objeto detectado puede desencadenar un evento de objeto térmico detectado. Los sensores de cámara de imágenes térmicas pueden proporcionar alcance, rumbo, tamaño y caracterización del objetivo. La ubicación del objetivo puede calcularse a partir del alcance y rumbo en relación con la ubicación y orientación del sensor de cámara térmica. Un software de clasificación asociado a la cámara térmica puede clasificar los objetos como humanos, perro, coche, etc. A corto alcance, el software de clasificación también puede determinar si un humano está de pie, sentado o tumbado. A muy corto alcance, el software de clasificación también puede realizar reconocimiento facial en un objetivo humano.

Los sensores del sistema de detección de disparos pueden producir un evento de disparo detectado, en el que software puede detectar y ubicar la ubicación en la que se ha producido el disparo y la dirección del disparo a partir de la onda de choque acústica.

Reglas de decisión

Si evento-de-evento-de-movimiento-detectado-por-radar con ubicación LEJOS de valla y HUMANO (velocidad, tamaño, etc.), entonces disparar evento-humano-lejos-fuera-de-valla.

Si evento objeto-térmico-detectado conubicación LEJOS de valla y objeto HUMANO, entonces disparar evento humano-lejos-fuera-de-valla.

LEJOS se define como un intervalo (nítido, impreciso o probabilístico) entre 300 metros y 500 metros más allá de la valla (u otra distancia predeterminada).

Si evento humano-lejos fuera de valla generado por radar y térmicamente coubicado, entonces disparar evento amenaza-de-nivel-muy-bajo.

Si evento amenaza-de-nivel-muy-bajo, entonces responder notificando a gestión de seguridad detalles del evento de amenaza de nivel muy bajo y controlar mediante servo sensores de cámara de alta resolución la ubicación de la amenaza. Tras la recepción del evento de amenaza de nivel muy bajo, el software de sistema de gestión de seguridad puede visualizar las imágenes de radar, térmicas y de cámara de alta resolución en las GUI de comando y control 60 (véanse las Fig. 8A y 8B). Puede requerirse al personal de sala de control de seguridad para que observe los eventos de amenaza de nivel bajo.

2. El adversario gira caminando hacia la valla norte hasta que está a menos de 300 metros de la valla (u otra distancia predeterminada).

Reglas de decisión

Si evento de movimiento-detectado-por-radar con ubicación MEDIA a valla y humano (velocidad, tamaño, etc.), entonces disparar evento humano-media-fuera-de-valla.

Si evento de objeto-térmico-detectado con ubicación MEDIA a valla y objeto humano, entonces disparar evento de humano-media-fuera-de-valla.

MEDIA se define como un intervalo (nítido, impreciso o probabilístico) entre 100 metros y 300 metros más allá de la valla (u otra distancia predeterminada).

Si los eventos humano-media-fuera-de-valla generados por radar y térmicamente coubicados, entonces disparar evento de amenaza-de-nivel-bajo.

Si evento de amenaza-de-nivel-bajo, entonces responder notificando a gestión de seguridad con detalles del evento de amenaza de nivel bajo y controlar mediante servo cámaras de alta resolución la ubicación de amenaza.

Tras la recepción del evento de amenaza de nivel bajo, el software de sistema de gestión de seguridad puede visualizar las imágenes de radar, térmicas y de cámara de alta resolución en las GUI de comando y control 60. Puede requerirse al personal de sala de control de seguridad para que supervise los eventos de amenaza de nivel bajo.

3. El adversario corre hacia la subestación y, después de entrar 100 metros dentro de la subestación (u otra distancia predeterminada), adopta una posición prona con un rifle apuntando a la subestación.

Reglas de decisión

Si evento de movimiento-detectado-por radar con ubicación CERCA de valla y humano (velocidad, tamaño, etc.), entonces disparar evento de humano-cerca-fuera-de-valla.

Si evento de movimiento-detectado-por-radar con ubicación CERCA de valla y humano (velocidad, tamaño, etc.) y velocidad HACIA valla, entonces disparar evento de humano-se-aproxima-fuera-de-valla.

Si evento de objeto-térmico-detectado con ubicación CERCA de valla y objeto humano prono, entonces disparar evento de humano-cerca-fuera-de-valla y disparar evento de humano-prono.

CERCA se define como un intervalo (nítido, impreciso o probabilístico) entre 100 metros y 300 metros más allá de la valla (u otra distancia predeterminada).

Si los eventos humano-cerca-fuera-de-valla generados por radar y térmicamente coubicados y (evento de humano se aproxima cerca fuera de valla o evento de humano prono fuera de valla), entonces disparar evento de amenaza- de-nivel-medio.

Si evento de amenaza-de-nivel-medio, entonces responder notificando a gestión de seguridad con detalles del evento de amenaza de nivel medio y controlar mediante servo cámaras de alta resolución la ubicación de la amenaza. También difundir aviso audible al adversario para que se aleje de la valla.

Tras la recepción del evento de amenaza de nivel medio, el software de sistema de gestión de seguridad puede visualizar las imágenes de radar, térmicas y de cámara de alta resolución en las GUI de comando y control 60. El software de sistema de gestión de seguridad también puede hacer sonar una alarma audible en la sala de control. Puede requerirse al personal de sala de control de seguridad para que supervise los eventos de amenaza de nivel medio.

4. El adversario a continuación dispara un único tiro a la infraestructura de subestación.

Reglas de decisión

Si evento de movimiento-detectado-por-radar con ubicación CERCA de valla y humano (velocidad, tamaño, etc.), entonces disparar evento de humano-cerca-fuera-de-valla.

Si evento de objeto-térmico-detectado con ubicación CERCA de valla y objeto humano-prono, entonces disparar evento de humano-cerca-fuera-de-valla y disparar evento de humano-prono.

Si evento de disparo-detectado con ubicación CERCA de valla, entonces disparar evento de disparo-cerca-fuera-de-valla. CERCA se define como un intervalo (nítido, impreciso o probabilístico) entre 100 metros y 300 metros más allá de la valla (u otra distancia predeterminada).

Si eventos de humano-cerca-fuera-de-valla y evento de disparo-cerca-fuera-de-valla coubicados, entonces disparar evento amenaza-de-nivel-alto.

Si evento de amenaza-de-nivel-alto-con-disparo dirigido a infraestructura, entonces responder notificando a la gestión de seguridad con detalles del evento de amenaza de nivel alto y controlar mediante servo cámaras de alta resolución la ubicación de amenaza. También controlar mediante servo el foco de 129

millones de lux (12 millones de fc), deslumbrador láser y LRAD para apuntar a la ubicación del objetivo.

Si se habilita el autodisparo, entonces disparar el foco deslumbrador láser y LRAD al objetivo.

Tras la recepción del evento de amenaza de nivel alto, el software de sistema de gestión de seguridad puede visualizar las imágenes de radar, térmicas y de cámara de alta resolución en las GUI de comando y control 60. El software de sistema de gestión de seguridad también puede hacer sonar una alarma audible en la sala de control. El software de gestión de seguridad también puede visualizar las soluciones de objetivos. Puede requerirse al personal de sala de control de seguridad para que supervise los eventos de amenaza de nivel alto. Si el autodisparo está deshabilitado, entonces el personal de seguridad puede habilitar manualmente el autodisparo.

5. El francotirador empieza a alejarse de la valla.

Reglas de decisión

Si evento de movimiento-detectado-por-radar con ubicación CERCA de valla y humano (velocidad, tamaño, etc.), entonces disparar evento de humano-cerca-fuera-de-valla.

Si evento de movimiento-detectado-por-radar con ubicación CERCA de valla y humano (velocidad, tamaño, etc.) y velocidad ALEJADA de valla, entonces disparar evento de humano-se-marcha-fuera-de-valla.

Si evento de objeto-térmico-detectado con ubicación CERCA de valla y objeto humano de pie, entonces disparar evento de humano-cerca-fuera-de-valla y disparar evento de humano-de-pie.

Si evento de humano-cerca-fuera-de-valla y evento de humano-cerca-se-marcha-fuera-de-valla y evento de humano-de-pie-fuera-de-valla generados por radar y térmicamente coubicados, entonces disparar evento de amenaza-de-nivel-medio.

Si evento de amenaza-de-nivel-medio, entonces responder notificando a gestión de seguridad con detalles del evento de amenaza de nivel medio y controlar mediante servo cámaras de alta resolución la ubicación de la amenaza. También difundir un aviso audible al adversario para que se aleje de la valla.
Tras la recepción del evento de amenaza de nivel medio, el software de sistema de gestión de seguridad puede visualizar las imágenes de radar, térmicas y de cámara de alta resolución en las GUI de comando y control 60. El software de sistema de gestión de seguridad también puede hacer sonar una alarma audible en la sala de control. Puede requerirse al personal de sala de control de seguridad para que supervise los eventos de amenaza de nivel medio.

6. El francotirador se marcha.

Reglas de decisión

Si eventos de no-movimiento-detectado, entonces disparar evento de amenaza-sin-nivel.

Si evento de amenaza-sin-nivel, entonces restablecer sensores a la configuración de amenaza sin nivel.

Tras la recepción del evento de amenaza-sin-nivel, el software del sistema de gestión de seguridad puede visualizar que no existen amenazas actuales.

Diversas técnicas y métodos estadísticos y probabilísticos se incorporan en el motor de razonamiento automatizado. Éstos pueden incluir, sin limitación, lógica imprecisa, redes neuronales artificiales, razonamiento bayesiano, propagación de restricción elástica, toma de decisión de múltiples objetivos o múltiples atributos, mapeo y localización simultáneos, filtrado de Kalman, etc. Con el uso de cualquiera de las técnicas anteriores, el motor de razonamiento automatizado pondera las contingencias almacenadas (por ejemplo, 80% de escenario A se está produciendo ahora mismo, 10% de escenario B se está produciendo ahora mismo, existe una probabilidad del 20% de que se produzca el escenario D si las contramedidas "x" e "y" se ejecutan, etc.), y usa analítica de estadística predictiva para desarrollar resultados con ponderaciones probabilísticas a variables (por ejemplo, factores de contexto). Las contramedidas propuestas se generan basándose en estos resultados, para los que puede usarse un modelado de análisis de fallo para generar contramedidas con respuestas deseadas, o al menos aceptables. Los resultados pueden visualizare a través de la GUI de contramedidas propuestas 50 mostrada en la Fig. 4B.

Un ejemplo de una analítica estadística predictiva puede ser la generación de perfiles de escenarios modelados matemáticamente para los escenarios aprendidos (por ejemplo, escenario A, escenario B, etc.). A medida que sucede un evento, la colección de datos del sensor 10 puede generar un modelo matemático

del evento actual. Este modelo de evento actual puede generarse de forma iterativa para producir un perfil de ocurrencia actual. El perfil de ocurrencia actual puede a continuación compararse con los perfiles de escenarios modelados de forma estadística para desarrollar correlaciones, relaciones, indicadores de avance y retraso, etc. Con el fin de cuantificar el porcentaje de un escenario aprendido dado que la ocurrencia actual se está produciendo. El sistema puede usar a continuación la analítica, vía el motor de razonamiento automatizado, por ejemplo, para determinar la mejor contramedida. El perfil de ocurrencia actual resultante y los perfiles de escenario aprendidos modelados pueden visualizare en las GUI de factor de contexto y de contramedidas propuestas 40, 50.

Estas y otras GUI pueden visualizare en pantallas de visualización 113 de dispositivos informáticos 101 a través de módulos 109 y paneles 110. Un módulo 109 puede comprender una pluralidad de paneles 109 para visualizar datos y GUI de una manera jerárquica. Por ejemplo, un primer módulo 109 puede programarse para visualizar GUI de simulación y de modelado a través de una pluralidad de primeros paneles 110. Un segundo módulo 109 puede programarse para visualizar las GUI de comando y control 60 (véanse las Figuras 8A y 8B) a través de una pluralidad de segundos paneles 110. Otros módulos 109 y paneles 110 puede programarse para visualizar transmisiones de cámara, datos estadísticos acerca de componentes, información acerca de conmutadores de ciberseguridad, etc.

Un método para desarrollar reglas de decisión efectivas para mejorar el rendimiento del motor de razonamiento automatizado es exportar los resultados de informe de múltiples escenarios exhaustivos de simulación y modelado que pueden crearse durante el diseño del sistema de defensa y rechazo (véase la fase de Diseño de Sistema de Protección Física de utilización del sistema, a continuación). Pueden emplearse tácticas de respuesta y escenarios de ataque adicionales que se producen, y para los que no se ha modelado anteriormente (es decir, no se han introducido como escenarios aprendidos), para ejecutar informes de escenarios de simulación y modelado adicionales con el fin de actualizar las reglas de decisión. Tales actualizaciones se usan para mejorar el rendimiento del sistema vía el motor de razonamiento automatizado.

Un *human-in.the-loop* puede habilitar/deshabilitar la capacidad de cualquier componente del sistema antes, durante y/o después de que se detecte un suceso. Por ejemplo, un usuario puede evitar la actuación de un accionador 20 particular que puede estar programado de otra manera para controlar una contramedida o incluso evitar que el sistema realice una contramedida. En otras realizaciones, el usuario puede seleccionar de entre una pluralidad de contramedidas o incluso construir y almacenar contramedidas, que pueden realizarse antes de y/o tras la detección de un evento.

Puede visualizare una GUI de comando y control 60 a través de la que el *human-in-the-loop* puede controlar un componente del sistema transmitiendo y/o interrumpiendo datos de contramedidas (véase la Fig. 8B). La GUI de comando y control 60 puede programarse de modo que cada componente, representado en la GUI como un icono, es también una interfaz de usuario. Activar un icono permite que el *human-in-the-loop* interactúe selectivamente con el proceso de contramedida. Por ejemplo, el *human-in-the-loop* puede determinar qué componente activar/desactivar, discontinuo, repetido, etc. Puede activarse un icono mediante un dispositivo periférico, tal como un ratón de ordenador, un controlador informático de mano de tipo juego, un teclado, etc. para controlar el movimiento de un cursor en la pantalla de la GUI 60. Puede activarse un componente colocando el cursor sobre su icono representativo y activando el icono. Además, o como alternativa, la GUI de icono puede programarse para visualizar una caja de opciones tras la activación del icono GUI 60, que puede mostrar una lista de actividades interactivas entre las que elegir. Además, o como alternativa, puede usarse una función de arrastrar y soltar para habilitar arrastrar un componente encima de otro componente y/o adversario para activar el componente en relación al componente/adversario sobre el que se ha arrastrado. Por ejemplo, arrastrar un accionador sobre un adversario puede provocar que el accionador 20 controle mediante servo la dirección del adversario. Pueden utilizarse otras interfaces interactivas y GUI, que pueden ser programables y reprogramables, para la personalización de la GUI a discreción del usuario.

Se ha de observar que un usuario que habilita/deshabilita un accionador y/o contramedida no necesita deshabilitar el motor de razonamiento automatizado, sino que la interacción de usuario puede actuar para interrumpir selectiva y/o temporalmente datos de contramedidas transmitidas por el motor de razonamiento automatizado. En este sentido, el motor de razonamiento automatizado continúa operando y generando contramedidas de acuerdo con las reglas de decisión. Adicionalmente, el razonamiento automatizado y/o software de control lógico continúa ayudando al *human-in-the-loop*, incluso si existe una interrupción temporal de transmisión de datos de contramedidas, para que adquiera los objetivos dirigiendo automáticamente los accionadores a los objetivos. Por ejemplo, tras la detección de un disparo de arma, los accionadores de contramedidas pueden apuntarse a la ubicación del origen exacto del disparo, incluso si un usuario deshabilita el disparo automático del accionador 20 del sistema, ya que el software de aplicación 30 se sigue aplicando para localizar el alcance y el rumbo del disparo. El software de adquisición de un objetivo a bordo, en conjunto con el razonamiento automatizado y/o software de control lógico, puede conducir al accionador 20 a re-apuntar al adversario a medida que se mueve y/o si se detecta otro disparo

de arma en una ubicación diferente.

El software 30 está programado para generar un bucle de realimentación continuo dinámico con los componentes del sistema, adaptándose a los eventos a medida que se producen en tiempo real (véanse las Fig. 5A y 5B). La realimentación dinámica puede incluir un bucle que puede iterar continuamente las etapas de detección, procesamiento analítico, actuación y/o control de *human-in-the-loop* seguido por la actuación. El bucle de realimentación continuo y el flujo de proceso continuo de la Fig. 3 califica y clasifica las amenazas para generar contramedidas que se implementan automáticamente y/o son mostradas al *human-in-the-loop* a través de las GUI 40, 50, 60. En este sentido, las contramedidas no se eligen únicamente para minimizar daño, sino también para habilitar la generación de una respuesta con grados de severidad de impacto. Debido a que pueden generarse contramedidas con ponderaciones estadísticas asignadas a resultados probables, el humano puede proporcionar una guía y vigilancia como entradas de control tras la presentación de la contramedida en las pantallas de visualización 113. Las entradas de control pueden mejorar el rendimiento del sistema habilitando el ajuste en tiempo real de prioridades y/o la anulación de ciertas acciones por *human-in-the-loop*.

Los datos de sensor y accionador se adquieren a través de las API de los sensores 10 y accionadores 20 de modo que los parámetros operativos, tales como constantes temporales, tasas de actualización y datos característicos de los sensores 10, por ejemplo, pueden ajustarse dinámicamente basándose en las circunstancias. Por ejemplo, el alcance, la resolución y la tasa de exploración de un sensor 10 puede ajustarse para proporcionar una mejor precisión y una actualización más rápida en las áreas que tienen más actividad y una menor tasa de actualización en las áreas con poca o ninguna actividad. Además, cualquier parámetro de un sensor 10 y/o accionador 20 puede cambiarse adaptativamente basándose en el rendimiento/daño/degradación de un sensor 10 y/o accionador 20. La capacidad de ajustar dinámica y automáticamente los parámetros operativos es una forma en la que el sistema genera eficiencias mediante recursos de cálculo y de datos de almacenamiento asignados de forma eficiente. Adicionalmente, se requieren comunicaciones más eficientes, menos almacenamiento de datos y menos infraestructuras de las que se requerirían de otra manera.

En referencia ahora a las Fig. 6A-C, el sistema puede generar un modelado de análisis de fallo e informes de resumen de resultado para definir un nivel de capacidad de un área/activo dado, que puede basarse en los análisis de tipo DAFO. Ejecutando todos los escenarios aprendidos y contramedidas para refinar iterativamente respuestas de contramedidas hasta que se consigue el nivel de capacidad prevista, el sistema puede proporcionar un nivel cuantificable de preparación que los usuarios pueden usar para la toma de decisiones. Por ejemplo, un análisis de fallos puede proporcionar a un usuario diversos niveles de capacidad del sistema para frustrar un ataque y compararlos con niveles variables y con los tipos de componentes del sistema. Como se muestra en la Fig. 6A, la comparación del análisis de fallos entre una respuesta dada del personal a un ataque y una respuesta usando el sistema de defensa y rechazo revela que la respuesta del personal proporciona una seguridad inadecuada a un mayor coste. Con los diversos resultados del análisis de fallos para cada escenario, el usuario puede tomar una decisión informada y/o realizar un análisis de coste-beneficio en cuanto a cuántos componentes del sistema son necesarios para conseguir un nivel deseado de seguridad. Además, el software 30 puede realizar análisis de coste-beneficio para la selección óptima, la colocación e instalación de accionadores 20, sensores 10 y otros componentes, como se muestra en las Fig. 6B-C. Este análisis puede incluir análisis de coste-beneficio asociado con la reducción de guardias de seguridad como personal para las diversas configuraciones del sistema. Mientras esto puede ser particularmente beneficioso durante una configuración inicial, el software 30 puede ejecutar esta aplicación de forma continua o periódica después de la configuración inicial. La disposición de los sensores 10 y accionadores 20 puede proporcionar una protección exhaustiva aplicando la teoría de círculos concéntricos. Por ejemplo, pueden generarse círculos concéntricos de sensores 10 y accionadores 20, donde cada círculo puede proporcionar un nivel diferente de protección y/o generar una contramedida basándose en la distancia a la que está el círculo del activo físico/área. En este sentido, un accionador 20 dentro de un círculo más externo puede generar una emisión para evitar que un adversario se acerque (es decir, dentro de alcance para provocar daño), mientras que un accionador 20 en un círculo más interior puede generar una emisión para fijar al adversario en una cierta ubicación. Además, la intensidad y el efecto debilitante de los accionadores 20 puede aumentarse a medida que el adversario avanza a través de los círculos concéntricos. La descripción de los círculos concéntricos anterior no pretende ser limitante y se entiende que pueden utilizarse otros niveles de intensidad y respuestas de contramedidas diferenciadas.

Software de control lógico

El software de control lógico emplea algoritmos de toma de decisiones para implementar las secuencias de acuerdo con las contramedidas, pero sin ejecutar la respuesta. Si los accionadores 20 son o no letales, el *human-in-the-loop* puede tomar la decisión de implementar las contramedidas o no. Con el software de control lógico, el *human-in-the-loop* puede conocer la situación mediante una GUI geoespacial que informa al *human-in-the-loop* de que un ataque potencial de un adversario es inminente o está en progreso. Esto puede mostrarse al usuario a través de la GUI de comando y control 60 de la Fig. 8B. El *human-in-the-loop*

respondería tomando el control de los accionadores 20 a través de los iconos interactivos de las GUI mediante dispositivos de interfaz periféricos. Con el software de control lógico, una vez que se detecta un evento, el sistema prepara los componentes para la ejecución de una contramedida, pero reserva la ejecución de la misma para que sea llevada a cabo por el *human-in-the-loop*. Como se describe anteriormente, el software de control lógico puede usarse además de o como alternativa al motor de razonamiento automatizado.

Software de Sala de Control

El software de Sala de Control puede usarse para mostrar la situación de un evento y de las amenazas identificadas y presentar sugerencias y contramedidas, así como proporcionar el origen de la toma de decisión subyacente del software de aplicación 30. En una situación en la que el sistema no está totalmente automatizado, el usuario puede tener la opción de proporcionar una respuesta condicionada antes de que se lleve a cabo una contramedida. Ésta puede ser una simple respuesta de ir/no ir o puede requerir más implicación, con lo que el usuario selecciona las contramedidas y/o toma el control de accionadores los 20 y otros componentes. Esté totalmente automatizado o no, la visualización de la situación puede usarse para habilitar que un usuario (por ejemplo, un humano supervisor) tome una decisión. Tales decisiones pueden extenderse más allá de meramente controlar los componentes del sistema. Por ejemplo, el conocimiento de la situación puede ayudar al usuario en la toma de decisiones para su propia seguridad, contactar con el personal de emergencias apropiado, deshabilitar o bloquear ciertas operaciones de la instalación, etc. Esto puede incluir mostrar los escenarios aprendidos y otra información probabilística asociada a las contramedidas tomadas para abordar las amenazas a un usuario en el dispositivo informático 101. El software de simulación (por ejemplo, software PSIM) puede incluirse con el software de sala de control para visualizar la efectividad probable y los resultados previstos de diversos escenarios.

Puede usarse diverso software geoespacial para generar la GUI en un dispositivo informático 101 representativo de la simulación, que puede ser una representación 2D y/o 3D del paisaje y topología ilustrando con precisión la escena real en tiempo real. El software de simulación puede generar una GUI similar a la GUI mostrada en la Fig. 8B; sin embargo, se entiende que pueden usarse otras configuraciones de GUI que se adaptan mejor al sistema particular del usuario. El software de simulación puede incluir un software de control de interfaz hombre-máquina (HMI) con iconos en directo en un entorno de software geoespacial. La integración del software HMI puede lograrse a través de API, software de terceros, soporte intermedio o a nivel de código fuente de cualquiera y/o toda la gestión de alarma y control de acceso de seguridad electrónica (ACAMS), sistemas de gestión de información de seguridad física (PSIM), gestión de emergencias, sistemas de expedición asistidos por ordenador de seguridad pública, sistemas de gestión de evacuación, software de GIS y/o geoespacial, controles de sistemas digitales, controles de sistemas lógicos, software de adquisición de datos y controles de sistema y cualquier software de GUI asociado para estos componentes de software. En este sentido, el sistema recopila y correlaciona los eventos de los dispositivos de seguridad dispares existentes y de los sistemas de información (video, control de acceso, sensores, analítica, redes, sistemas de construcción, etc.) para aumentar adicionalmente la robustez, mejorar los tiempos de respuesta y generar eficiencia.

Aunque se muestra que el visualizador está dentro de una sala de control, el sistema no se limita ciertamente a esta configuración. Como se describirá más en detalle en la sección de arquitectura informática, puede usarse cualquier dispositivo de visualización informático capaz de habilitar entradas a través de un software de conexión por interfaz. Por tanto, pueden usarse dispositivos informáticos 101 fuera de la sala de control, dispositivos informáticos móviles y otros dispositivos informáticos conectados a la red informática 100 para controlar los componentes del sistema. Por ejemplo, un usuario puede ser el *human-in-the-loop* a la vez que está en un vehículo y usa un ordenador portátil. Adicionalmente, puede haber múltiples *human-in-the-loop* ejerciendo el comando y el control de diversas partes del sistema.

Como se describe anteriormente, el sistema de defensa y rechazo puede usarse para mejorar los sistemas físicos pasivos (si ya están instalados o se instalan simultáneamente con el sistema de defensa y rechazo) o puede usarse como un sistema autónomo. Cuando se mejora el sistema protector físico pasivo, el método puede incluir recoger las capacidades latentes de y añadir un potencial valor exponencial al sistema pasivo. Ya se mejoren los sistemas existentes o se usen como un sistema autónomo, las múltiples aplicaciones de seguridad no conectadas, los accionadores 20 y los sensores 10 pueden integrarse mediante una interfaz de usuario integral, creando así una relación integral entre los módulos de software existentes de los diversos fabricantes, que pueden dotar a los operadores del sistema de usuario final de la capacidad para tomar el control de los accionadores 20 remotos. Además de cerrar los lapsos de tiempo entre la detección, la respuesta y la neutralización, estas características también añaden robustez y dotan al sistema de una eficiencia adicional.

La Fig. 7A ilustra un diseño de sistema protector físico pasivo típico con adversarios coordinando un ataque y la Fig. 7B ilustra que superar los sistemas protectores físicos pasivos de saltar la valla y cortar el candado requiere únicamente 0,2 minutos. Después de superar los sistemas físicos pasivos, los adversarios pueden

lograr su objetivo en un tiempo tan corto como de 3 minutos.

Como se observa en la Fig. 8A, el sistema de defensa y rechazo puede usarse para establecer un conjunto de sensores de múltiples fenomenologías 10 que proporciona una cobertura de 360º comenzando desde dentro de la infraestructura crítica y extendiéndose hacia fuera, a una distancia que puede prescribirse/determinarse por el sistema y de acuerdo con el nivel de capacidad elegido del análisis de fallo. La infraestructura crítica y las vías probables de aproximación de los adversarios al sitio de la infraestructura crítica pueden comprobarse, así como las posibles zonas, puntos de embudo, lugares de ocultación naturales, posiciones de francotirador/distancia de seguridad, pasajes, etc. Puede configurarse la analítica de los sensores para establecer regiones de interés. Por ejemplo, puede aumentarse la sensibilidad de un sensor en una cierta zona porque sería una buena posición de francotirador para un adversario. Además, pueden identificarse diversos puntos de referencia que el adversario atravesaría probablemente mientras realiza en secuencias sus tareas de ataque y/o responde a las contramedidas, de modo que el software 30 puede programarse para concentrar la potencia de combate en esas áreas. La Fig. 8A muestra que el conjunto de sensores no deja ningún área sin observar, que áreas críticas tienen cobertura redundante con un coste mínimo y que pueden detectarse y enfrentarse a adversarios incluso más allá del perímetro de la instalación.

Puede usarse un API para integrar sensores 10 y accionadores 20 con el IC, de modo que el IC puede reaccionar a la información colectiva del sensor 10. La colocación de los sensores 10 y de los accionadores 20 puede diseñarse para crear círculos concéntricos de protección, proporcionando cada círculo un grado variable de protección. Con el método de implementación descrito anteriormente, la integración puede usarse para extender una protección no letal hasta tres kilómetros más allá del perímetro del área/activo, aumentando así potencialmente el tiempo que se retrasan los adversarios en un múltiplo de quizás diez o más. La implementación del sistema puede incluir la calibración de los sensores 10 con ataques simulados por expertos en tácticas paramilitares, que realizan físicamente secuencias de ataque. Esto puede incluir el uso de fuego real e intentos para completar objetivos reales. La precisión del sistema puede mejorarse continuamente usando los sensores 10 (por ejemplo, LIDAR) para medir continua o periódicamente distancias y mapear geoespacialmente el área con el fin de actualizar la múltiple fenomenología y evaluar la disposición de los componentes.

Puede usarse una estructura de implementación de cuatro fases para personalizar el método y el sistema para un activo físico/área dada. (Véase la Fig. 9). Las fases pueden incluir una fase de Evaluación de Riesgos, de Diseño de Sistema de Protección Física (PPS), de Integración y Distribución de Sistema y de Puesta en Marcha e Implementación.

La fase de Evaluación de Riesgos puede incluir la identificación de los activos críticos dentro del área a proteger, así como las vulnerabilidades y consecuencias potencialmente asociadas. Esto puede incluir el enfoque de Metodología de Evaluación de Riesgos (RAM) de Sandia National Laboratories u otras metodologías similares, donde se calculan las amenazas, consecuencias y la efectividad protectora mediante ecuaciones matemáticas para cuantificar o cualificar un riesgo. Esto se logra en general en un esfuerzo colaborativo (incluyendo grupos de trabajo) con los usuarios para abordar las vulnerabilidades de seguridad y las consecuencias potenciales asociadas y amenazas. La fase de Evaluación de Riesgos generalmente incluye identificar los activos críticos dentro del área a proteger, así como las vulnerabilidades de los activos, para diseñar escenarios iniciados por adversarios y consecuencias potenciales asociadas. Los escenarios de adversario pueden construirse usando un software Monte Carlo y otro software de simulación y modelado tal como ARES AVERT™.

Las Amenazas Base de Diseño son parámetros que usan factores de contexto, datos de sensor y datos de accionador para generar un valor cuantificable, usado como una variable dentro de las reglas de decisión. Esto permite que las reglas de decisión operen como parámetros dentro del razonamiento automatizado y del software de control lógico, de modo que la contramedida implementada por el sistema tiene la mayor probabilidad de mitigar los daños provocados por el suceso. El Espectro de Amenaza Base de Diseño mostrado en la Fig. 10 es ilustrativo del espectro de tipo de amenazas que pueden producirse a partir de la inteligencia recopilada desde diversas agencias de inteligencia y fuerzas del orden, y a partir de una base de diseño para el experto en la materia (SME), para diseñar diversos aspectos del sistema de defensa y rechazo (por ejemplo barreras, alarmas, sensores, dispositivos de control de acceso, accionadores no letales, interfaces gráficas de usuario y humano-máquina, etc.). En este sentido, un SME alimenta la información de tipo de amenaza del Espectro de Amenaza Base de Diseño en el software de simulación y modelado. A continuación, el software de simulación y modelado puede determinar y/o predecir los escenarios probables (patrones de comportamiento y tácticas) de cada tipo de Amenaza Base de Diseño. Pueden desarrollarse y programarse reglas de decisión y tareas de adversario basándose en los escenarios que se desarrollan como resultado de ejecutar el software de simulación y modelado.

El sistema no tiene que identificar qué amenaza está atacando para ser efectivo, solo qué tácticas específicas se están empleando y qué contramedidas agregar e implementar para debilitar y retardar

cualquiera que sea la amenaza o las amenazas. Si la amenaza es una amenaza Base de Diseño que es disparar al sitio protegido, a continuación el sistema puede reaccionar para interrumpir la capacidad de la Amenaza Base de Diseño golpeando al objetivo inhibiendo la visión de la Amenaza Base de Diseño y enviando sonidos dolorosos y/o de distracción.

El sistema puede ser programado para responder a un comportamiento del adversario "amenazante" basándose en el comportamiento del adversario ajustado al patrón de una amenaza. El sistema puede computar las vulnerabilidades que podrían ser explotadas por parte del adversario, con lo que la respuesta del sistema puede ser evaluar la situación basándose en un patrón de comportamiento del adversario en relación al riesgo potencial y generar una contramedida para minimizar el riesgo. Las reglas de decisión pueden tener dos partes: un antecedente que está describiendo un patrón; y una consecuencia que describe una respuesta. El uso de los términos impreciso o probabilístico en la consecuencia significa que un comportamiento dado coincidirá con el antecedente en un grado. Por tanto, cada regla actúa como un "arquetipo" para todos los comportamientos que son "similares" a ese patrón y las reglas representan los escenarios aprendidos. El escenario desarrollado puede compararse con cada regla de escenario aprendido mediante la coincidencia en un grado. Un comportamiento dado podría coincidir con múltiples reglas en varios grados. Se emplea la mejor coincidencia o alguna combinación de las mejores coincidencias para determinar la respuesta.

La caracterización de las amenazas dentro de un intervalo de nivel de amenaza (por ejemplo, niveles de amenaza Alto, Medio, Bajo) puede basarse en las tareas y actividades específicas que la persona o personas/vehículo o vehículos están realizando en el momento del posible ataque, y la contramedida puede modificarse de acuerdo con el nivel de amenaza caracterizado. La caracterización es dinámica basándose en datos los que se recopilan y analizan continuamente mediante el bucle de realimentación y en las evaluaciones del conocimiento de la situación.

La fase de Diseño de Sistema de Protección Física (PPS) puede incluir desarrollar un diseño efectivo para frustrar ataques. Pueden desarrollarse conceptos de operaciones (CONOPS) para proporcionar opciones de mitigar las vulnerabilidades y reducir el riesgo asociado, que puede basarse en restricciones presupuestarias y tolerancia al riesgo. También pueden usarse opciones CONOPS para aumentar la efectivad protectora del sistema. Estos conceptos pueden incluir acceso a sitios, diseño de sitio, iluminación de todo el espectro, evacuación de emergencia, tecnologías actuales, capacidades de seguridad física y personal de respuesta, tecnologías de ciberseguridad, etc. Con estos conceptos en mente, puede generarse un diseño del tipo y la disposición de los accionadores, sensores y otros componentes.

La fase de Diseño de PPS puede llevarse a cabo en dos partes. La parte I puede incluir desarrollar un diseño efectivo para frustrar ataques. Todos los escenarios de adversarios construidos anteriormente usando un software de simulación y modelado, tal como ARES AVERT™, Monte Carlo™, etc., pueden re-ejecutarse frente a interacciones u opciones del Diseño de PPS en iteraciones. En cada iteración de Diseño de PPS conceptual posterior, pueden hacerse cambios para alcanzar el nivel deseado de efectividad protectora y la correspondiente reducción del riesgo. Estos cambios pueden incluir, sin limitación, añadir/mejorar equipos, añadir/mejorar sistemas de seguridad software, configurar y programar el software para definir adicionalmente e implementar requisitos cambiantes en la automatización del sistema, razonamientos automatizados y comportamientos de HMI, lo cual puede hacerse de manera conjunta con la planificación para tareas y procedimientos humanos, modificar entornos construidos (por ejemplo mejorar la protección contra explosiones añadiendo barreras adicionales, aumentando distancias de seguridad, etc.) y cambiando características topográficas para aumentar el nivel de dificultad a los adversarios mientras progresan y atraviesan el entorno en diversas trayectorias postuladas hacia la infraestructura crítica que se está protegiendo.

La parte II puede incluir otra fase de diseño para diseñar tareas y actividades con el fin de desarrollar documentos de construcción, gestión de proyectos e implementación. Éstos pueden incluir, sin limitación, planos de ingeniería, especificaciones, procedimientos de operacionales de seguridad, planificación maestra de entrenamiento de respuesta, presupuesto o presupuestos del proyecto, etc.

La fase de Integración y Distribución de Sistema puede incluir comprobar la instalación y la funcionalidad de los componentes prescritos en la fase de Diseño de PPS. Esto puede incluir un proceso de gestión de proyecto altamente especializado que está personalizado para garantizar la distribución en la instalación de una solución integrada inteligente completa. En el caso de instalaciones de infraestructura crítica que se gobiernan por reguladores, imponer justificaciones para la recuperación de gastos a las agencias regulatorias (por ejemplo, comisiones de servicio público o de suministros públicos) con la ayuda de un software de simulación y modelado que demuestra que la solución o las soluciones de seguridad implementadas por la instalación son las más eficaces y rentables. Esto puede incluir demostraciones de que se consigue el nivel máximo de efectividad protectora dada la cantidad de dinero invertido.

La fase de Puesta en Marcha e Implementación puede incluir la comprobación y validación del rendimiento

del sistema, establecer procedimientos operativos, realizar ejercicios de respuesta y de entrenamiento del personal de seguridad físico. Esto puede incluir la comprobación y validación inicial y en uso del rendimiento del sistema, el establecimiento de procedimientos operativos, la realización de ejercicios de respuesta y de entrenamiento del personal de seguridad físico. La consideración y evaluación en uso de nuevas amenazas y tecnologías puede factorizarse y reciclarse mediante el inicio, en la primera fase, de la actualización del sistema. Se proporciona un entrenamiento en parte usando un software de simulador de entrenamiento y de combate realista interactivo. Éste puede ser un software de entrenamiento ARES BlueTrain™ u otro software que permite una visualización de alta fidelidad de los resultados analíticos de la de simulación y el modelado. El software de simulación y entrenamiento puede programarse para soportar sesiones de entrenamiento de un solo participante o de múltiples participantes.

Además, la implementación de cuatro fases puede iterarse periódicamente, o según se necesite, para mantener y/o mejorar un nivel deseado de protección. En este sentido, el software de simulación y modelado puede usarse en la reevaluación y rediseño del sistema.

Ejemplo

En una realización ilustrativa, el método para proteger activamente un activo físico/área mediante la defensa y rechazo puede incluir: recibir, mediante una red informática, datos de sensor asociados a características de un entorno que corresponde a un activo físico/área desde un sensor configurado para identificar un evento; identificar, mediante la red informática, un evento como una amenaza y tener conciencia de la situación; generar, por la red informática, una pluralidad de contramedidas; aplicar, por la red informática, reglas de decisión para seleccionar una contramedida; transmitir, por la red informática, datos de contramedidas a un accionador, donde los datos de contramedidas se configuran para accionar el al menos un accionador; y generar un bucle de realimentación continuo, a través de la red informática, para recibir los datos de accionador y los datos de sensor; caracterizar de nuevo la ocurrencia, desarrollar de nuevo el conocimiento de la situación, generar de nuevo la pluralidad de contramedidas y aplicar de nuevo reglas de decisión para transmitir de nuevo datos de contramedidas adaptadas.

Recibir datos de sensor, caracterizar la ocurrencia, generar la pluralidad de contramedidas, aplicar reglas de decisión, transmitir datos de contramedidas y generar el bucle de realimentación continuo puede ser realizado por al menos uno del software de control lógico y software de motor de razonamiento automatizado. Identificar el evento como una amenaza puede basarse en la probabilidad de que el evento conlleva un riesgo para el activo físico/área, donde el aplicar las reglas de decisión puede incluir al menos una de reducir la probabilidad de que la amenaza provoque el riesgo y retrasar el tiempo requerido para que la amenaza se convierta en un riesgo.

El evento puede ser una persona detectada por el sensor, donde activar el accionador incluye generar emisiones no letales y no destructivas en respuesta a la misma. Aplicar las reglas de decisión en esta situación puede incluir impedir o retrasar el riesgo que conlleva la persona, que puede comprender impedir sus movimientos.

Generar la pluralidad de contramedidas puede comprender modelar matemáticamente escenarios aprendidos y modelar matemáticamente un evento actual, donde el método puede entonces generar una interfaz gráfica de usuario que muestra los escenarios aprendidos, el evento actual y la pluralidad de contramedidas. Pueden emplearse las Amenazas Base de Diseño para determinar y predecir los escenarios probables de cada tipo de amenaza y pueden desarrollarse las reglas de decisión al menos en parte de los escenarios probables. Además, las amenazas pueden caracterizarse dentro de un intervalo de nivel de amenaza base en tareas y actividades específicas que la persona está realizando en el momento del evento.

Arquitectura de sistema informático

En referencia de nuevo a la Fig. 2, se describe una red informática que puede usarse con el sistema. Siempre que se haga referencia a un usuario en esta descripción, se entiende que esta referencia incluye el o los dispositivos informáticos asociados 101, el servidor o servidores informáticos 102, la base o bases de datos 103 y/o el uso de los mismos. Las redes de comunicación distribuidas 104 usadas para facilitar la conexión y comunicación entre cada dispositivo informático 101 son habituales en la técnica. Cada dispositivo informático 101 puede comunicarse por completo o en parte mediante sitios web a través de una red de comunicación 104, que puede incluir un servidor web.

Las interacciones entre el usuario, los accionadores 20, los sensores 10 y la red informática 100 pueden implementarse usando un hardware, un software, un firmware, medios legibles por ordenador no transitorios con instrucciones almacenadas en los mismos o una combinación de éstos, y pueden implementarse en un único o múltiples sistemas informáticos u otros sistemas de procesamiento. El hardware, software o cualquier combinación de éstos puede incorporar módulos y componentes para ejecutar las funciones del sistema.

Si se usa una lógica programable, tal lógica puede ejecutarse en una plataforma de procesamiento comercialmente disponible o en un dispositivo para este fin. El experto en la materia apreciará que, con las ventajas de la presente descripción, las realizaciones del objeto aquí descrito pueden practicarse con diversas configuraciones de sistemas informáticos, incluyendo sistemas multiprocesador, miniordenadores, ordenadores centrales, ordenadores enlazados o agrupados con funciones distribuidas, así como con ordenadores ubicuos o en miniatura que pueden incluirse en prácticamente cualquier dispositivo. Por ejemplo, puede usarse al menos un dispositivo procesador 105 y una memoria 106a, 106b para implementar las realizaciones aquí descritas.

Un dispositivo procesador 105, tal como se discute aquí, puede ser un único procesador, una pluralidad de procesadores o una combinación de ambos. Los dispositivos de procesador 105 pueden tener uno o más núcleos de procesador. Los términos “medios de programa informático”, “medios legibles por ordenador no transitorios” y “medios usables por ordenador”, tal como se citan aquí, se usan para referirse en general a medios tangibles, tal como, por ejemplo, una unidad de almacenamiento extraíble y un disco duro instalado en una unidad de disco duro.

Un dispositivo procesador 105 puede ser un dispositivo procesador especial o general. Un dispositivo procesador 105 puede conectarse a una infraestructura de comunicaciones. Una infraestructura de comunicaciones puede incluir, sin limitación, un bus, una cola de mensajes, una red, un esquema de paso de mensajes multi-núcleo, etc. La red 100 puede incluir una memoria principal 106a. Una memoria principal 106a puede incluir, sin limitación, una memoria de acceso aleatorio, una memoria de sólo lectura, etc. La red 100 puede incluir una memoria secundaria 106b. Una memoria secundaria 106b puede incluir, sin limitación, una unidad de disco duro, una unidad de almacenamiento extraíble, una unidad de disco flexible, una unidad de cinta magnética, una unidad de disco óptico, una memoria flash, etc. La memoria 106a, 106b puede ser una memoria no volátil.

Una unidad de almacenamiento extraíble puede leer de y/o escribir en una unidad de almacenamiento extraíble de manera bien conocida. Una unidad de almacenamiento extraíble puede incluir un medio de almacenamiento extraíble que puede leerse por y escribirse en una unidad de almacenamiento extraíble. Por ejemplo, si una unidad de almacenamiento extraíble es una unidad de disco flexible, una unidad de almacenamiento extraíble puede ser un disco flexible. Una unidad de almacenamiento extraíble puede ser medio de grabación legible por ordenador no transitorio.

En algunas realizaciones, una memoria secundaria 106b puede incluir medios alternativos para permitir que se carguen programas informáticos u otras instrucciones en la red 100. Ésta puede ser, por ejemplo, una unidad de almacenamiento extraíble y/o una interfaz. Ejemplos de tales medios pueden incluir, sin limitación, un cartucho de programa e interfaz de cartucho (por ejemplo, como se encuentran en los sistemas de videojuego), un chip de memoria extraíble (por ejemplo EEPROM, PROM, etc.) y una conexión asociada y/u otras unidades de almacenamiento extraíbles e interfaces, como será evidente, a la vista de la presente descripción, al experto en la materia.

La red 100 puede incluir una interfaz de comunicaciones 107. Una interfaz de comunicaciones 107 puede configurarse para permitir que el software y los datos se transfieran entre la red 100 y los dispositivos externos. Las interfaces de comunicación 107 pueden incluir, sin limitación, un módem, una interfaz de red (por ejemplo una tarjeta de Ethernet), un puerto de comunicaciones, una tarjeta y ranura de PCMCIA, etc. El software y los datos transferidos a través de la interfaz de comunicaciones pueden estar en forma de señales, que pueden ser electrónicas, electromagnéticas, ópticas u otras señales, como será evidente, a la vista de la presente descripción, para el experto en la materia. Las señales pueden viajar a través de una ruta de comunicaciones 108, que puede configurarse para transportar señales y puede implementarse usando cable, fibra óptica, una línea telefónica, un enlace de teléfono móvil, un enlace de frecuencia de radio, etc.

Los medios de programa informático y usables por ordenador pueden referirse a memorias, tal como una memoria principal 106a y una memoria secundaria 106b, que pueden ser semiconductores de memoria (por ejemplo DRAM, etc.). Estos productos de programa informático pueden ser medios para proporcionar un software a la red 100. Los programas informáticos (por ejemplo, la lógica de control informática) pueden almacenarse en una memoria principal 106a y/o en una memoria secundaria 106b. Los programas informáticos también pueden recibirse a través de una interfaz de comunicaciones 107. Tales programas informáticos, cuando se ejecutan por un dispositivo procesador 105, pueden habilitar a la red 100 para que ejecute comandos y actúe sobre los diversos componentes del sistema. Por consiguiente, tales programas informáticos pueden representar controladores de la red 100 descrita. Cuando la presente descripción se implementa usando software, el software puede almacenarse en un producto de programa informático y cargarse en la red 100 usando una unidad de almacenamiento extraíble, una interfaz, una unidad de disco duro y/o una interfaz de comunicaciones 107.

Un dispositivo informático 101 puede ser un procesador, microprocesador, miniordenador, servidor,

ordenador central, portátil, asistente de datos personal, dispositivo de correo electrónico inalámbrico, teléfono móvil, teléfono inteligente, buscapersonas, máquina de fax, escáner o cualquier otro dispositivo programable configurado para habilitar la transmisión y/o recepción de datos, que puede ser a través de una red. Un dispositivo informático 101 puede incluir un dispositivo periférico, tal como un dispositivo de entrada/salida. Un dispositivo periférico puede incluir, sin limitación, un teclado, un ratón, una pantalla de visualización, una pantalla táctil, un lápiz, un monitor, una impresora, una unidad de disco duro, una unidad de disco flexible, una palanca de mandos, un escáner de imágenes, etc.

La red 100 puede usar una o más redes informáticas electrónicas para promover la comunicación entre los diferentes componentes, transferir datos y/o compartir información de recursos. Tales redes informáticas pueden materializarse en, sin limitación, al menos una de Ethernet, LAN inalámbrica, MAN, WAN, VPN, SAN, GAN, HomePNA, etc.

Diversas realizaciones de la presente descripción se describen en términos de esta red informática 100 ilustrativa. Será evidente para el experto en la materia, a la vista de la presente descripción, cómo implementar el sistema usando otras realizaciones de la red informática 100, junto con otras realizaciones de arquitecturas informáticas. Aunque las operaciones pueden describirse como un proceso secuencial, algunas de las operaciones pueden realizarse en paralelo, simultáneamente y/o en un entorno distribuido, y con códigos de programa almacenado en local o en remoto para el acceso por una máquina de un único o múltiples procesadores. En algunas realizaciones, el orden de las operaciones puede distribuirse sin salirse del alcance del objeto descrito. La red informática 100 puede comprender un procesador 105 que puede esta operativamente asociado a al menos un módulo 109, que puede programarse para visualizar paneles 110 y/o pantallas de visualización 113 en un monitor de dispositivo informático 111. El procesador 105 puede programarse para ejecutar instrucciones legibles por ordenador incluidas dentro de un módulo 109. Las instrucciones legibles por ordenador pueden estar en forma de software de aplicación almacenado en un medio legible por ordenador no transitorio operativamente asociado a un procesador 104. Cada módulo 109 puede configurarse para generar la GUI y/u otra interfaz de usuario, permitiendo que al menos un usuario emita comandos, el acceso a los datos almacenados en un medio de almacenamiento de datos operativamente asociado al procesador 105 y/o la transmisión de datos a y desde el medio de almacenamiento de datos. Un módulo 109 puede incluir un software, un firmware, un hardware o cualquier combinación razonable de éstos.

Un módulo 109 puede programarse para visualizar al menos un panel 110. Un panel 110 puede configurarse para visualizar información y conceder acceso a datos relacionados con ciertos aspectos y funcionalidades del sistema. Diferentes paneles 110 de cada módulo 109 pueden programarse para habilitar la visualización e interacción entre los usuarios, los componentes del sistema y el propio sistema de diferentes formas. Las visualizaciones e interacciones diferenciadas de los diversos módulos 109 y paneles 110 pueden configurarse para permitir una interacción acordada, filtrar la visualización de información y proteger la información sensible. Mediante los diversos módulos 109 y paneles 110, la red informática 100 proporciona una red de comunicación 104 para orquestar la interacción entre un usuario, el sistema y los diversos componentes del sistema.

Será evidente para el experto en la materia que numerosas modificaciones y variaciones de los ejemplos y realizaciones descritos son posibles a la vista de los contenidos anteriores de la descripción. Los ejemplos y las realizaciones descritas se indican con propósitos ilustrativos únicamente. Otras realizaciones alternativas pueden incluir algunas o todas las características aquí descritas. Por tanto, es la intención abarcar todas de tales modificaciones y realizaciones alternativas, ya que pueden ocurrir dentro del verdadero alcance de esta invención, la cual tiene una amplitud completa. Adicionalmente, la descripción de un intervalo de valores es de cada valor numérico dentro de ese intervalo, incluyendo los valores extremos.

REIVINDICACIONES

1. Método para proteger activamente un activo físico/área mediante defensa y rechazo, que comprende:

recibir, por una red informática, datos de sensor asociados a características de un entorno que corresponde a un activo físico/área, desde al menos un sensor (10) configurado para identificar un evento;
identificar, por la red informática, un evento como una amenaza basándose en una probabilidad de que el evento genera un riesgo para el activo físico/área y tomar conciencia de la situación;
generar, por la red informática, una pluralidad de contramedidas, incluyendo cada contramedida, cuando se aplica, un resultado probabilístico de al menos uno de reducir la probabilidad de que la amenaza provoca el riesgo y retrasar el tiempo requerido para que la amenaza se convierta en riesgo;
aplicar, por la red informática, reglas de decisión para seleccionar una contramedida;
transmitir, por la red informática, datos de las contramedidas a al menos un accionador (20), donde los datos de las contramedidas se configuran para accionar el al menos un accionador (20) para conseguir el resultado probabilístico; y
generar un bucle de realimentación continuo, a través de la red informática, para recibir datos del accionador y datos del sensor, y caracterizar de nuevo dinámicamente el evento, desarrollar de nuevo conocimiento de la situación, generar de nuevo la pluralidad de contramedidas y aplicar de nuevo reglas de decisión para transmitir de nuevo datos de contramedidas.

2. Método según la reivindicación 1, donde la recepción de datos de sensor, la caracterización del evento, la generación de la pluralidad de contramedidas, la aplicación de reglas de decisión, la transmisión de datos de contramedidas y la generación del bucle de realimentación continuo se llevan a cabo un software de control lógico.

3. Método según la reivindicación 1, donde la recepción de datos de sensor, la caracterización del evento, la generación de la pluralidad de contramedidas, la aplicación de reglas de decisión, la transmisión de datos de contramedidas y la generación del bucle de realimentación continuo se llevan a cabo mediante un software de motor de razonamiento automatizado.

4. Método según la reivindicación 1, donde el evento es al menos una persona detectada por el al menos un sensor (10).

5. Método según la reivindicación 4, donde la activación del al menos un accionador (20) comprende generar emisiones no letales o no destructivas.

6. Método según la reivindicación 5, donde cuando la al menos una persona es identificada como amenaza, la aplicación de las reglas de decisión comprende denegar o retrasar que la al menos una persona conlleve el riesgo.

7. Método según la reivindicación 6, donde denegar o retrasar que la al menos una persona conlleve el riesgo comprende interrumpir los movimientos de la al menos una persona.

8. Método según la reivindicación 1, donde generar la pluralidad de contramedidas comprende modelar matemáticamente escenarios aprendidos y modelar matemáticamente un evento actual.

9. Método según la reivindicación 8, que además comprende generar una interfaz gráfica de usuario que muestra los escenarios aprendidos, el evento actual y la pluralidad de contramedidas.

10. Método según la reivindicación 9, donde se usan Amenazas Base de Diseño para determinar y predecir escenarios probables de cada tipo de amenaza.

11. Método según la reivindicación 10, donde las reglas de decisión se desarrollan, al menos en parte, en escenarios probables.

12. Método según la reivindicación 4, donde la amenaza se caracteriza dentro de un intervalo de nivel de amenaza basándose en tareas y actividades específicas que la al menos una persona está realizando en el momento del evento.

13. Sistema para proteger activamente un activo físico/área, mediante defensa y rechazo, que comprende:

una red informática que tiene al menos un procesador, un medio de almacenamiento no transitorio y un dispositivo informático con un visualizador;
al menos un accionador (20) en comunicación con la red informática;
al menos un sensor (10) en comunicación con la red informática; y,

un software de aplicación (30) almacenado en el medio de almacenamiento no transitorio programado para ejecutar comandos y control del sistema y visualizar una interfaz en el dispositivo informático que permite que un usuario ejecute el comando y el control del sistema a través de al menos un módulo;
donde el software de aplicación (30) incluye al menos uno de un software de motor de razonamiento automatizado y un software de control lógico programado para coordinar automáticamente la activación del al menos un accionador (20) y del sensor de acuerdo con las reglas de decisión para detectar, identificar y localizar amenazas de un evento e implementar al menos una contramedida en respuesta a las mismas;
donde las reglas de decisión son parámetros programados en el software de aplicación (30) para identificar las amenazas basándose en una probabilidad de que éstas generen un riesgo para un activo físico/área y para dirigir la activación del al menos un accionador (20) y un sensor (10) durante la implementación de la al menos una contramedida;
donde la al menos una contramedida incluye, cuando se aplica, un resultado probabilístico de al menos una de reducir la probabilidad de que las amenazas provoquen el riesgo y retrasar el tiempo requerido para que las amenazas se conviertan en el riesgo, siendo la contramedida una activación concertada del al menos un accionador (20) y sensor (10) para evitar un daño al activo físico/área representado por las amenazas;
donde los datos de sensor se transmiten desde el al menos un sensor (10) a al menos uno de otro sensor (10), al al menos un accionador (20) y a la red informática y son procesados por el software de aplicación (30) para desarrollar la al menos una contramedida; y,
donde, durante la implementación de la al menos una contramedida, se transmiten los datos de contramedida desde la red informática a al menos uno del accionador (20) y el sensor (10) a través de un bucle de realimentación continuo para caracterizar dinámicamente de nuevo el evento, re-desarrollar la contramedida y transmitir de nuevo los datos de contramedida.

14. Sistema según la reivindicación 13, donde:

el al menos un sensor (10) se configura para detectar y registrar características de un entorno cerca del activo físico/área para detectar el evento y recopilar datos con respecto a éste; y,
el al menos un accionador (20) se configura para generar emisiones no letales y no destructivas a humanos y equipos.

15. Sistema según la reivindicación 13, donde la al menos una contramedida se basa, al menos en parte, en al menos uno de escenarios aprendidos modelados matemáticamente y en un evento actual modelado matemáticamente.

16. Sistema según la reivindicación 15, donde se usan Amenazas Base de Diseño para determinar y predecir escenarios probables de cada tipo de amenaza.

17. Sistema según la reivindicación 13, donde el software de aplicación (30) se programa para tener conocimiento de la situación mediante al menos uno de:

recopilar, condensar y fusionar datos de sensor e implementar automáticamente la al menos una contramedida dirigida contra adversarios que provocan el evento atacando al activo físico/área, donde la al menos una contramedida se configura para interrumpir el movimiento del adversario; y,
una interfaz gráfica de usuario geoespacial presentada al usuario y uso de algoritmos de toma de decisiones para implementar secuencias de acuerdo con la al menos una contramedida.

18. Método según la reivindicación 1, donde: el al menos un sensor (10) es una pluralidad de sensores (10) dispuestos para detectar un área que rodea el activo físico/área; y la amenaza es un individuo situado dentro del área que rodea el activo físico/área.

19. Método según la reivindicación 1, donde las reglas de decisión comprenden reglas de producción de restricciones que inhiben la activación de una contramedida basándose en un análisis de factores de contexto que incluyen factores políticos, ambientales, tecnológicos y sociales.

20. Sistema según la reivindicación 13, donde las reglas de decisión comprenden reglas de producción de restricciones que inhiben la activación de una contramedida basándose en un análisis de factores de contexto que incluyen factores políticos, ambientales, tecnológicos y sociales.

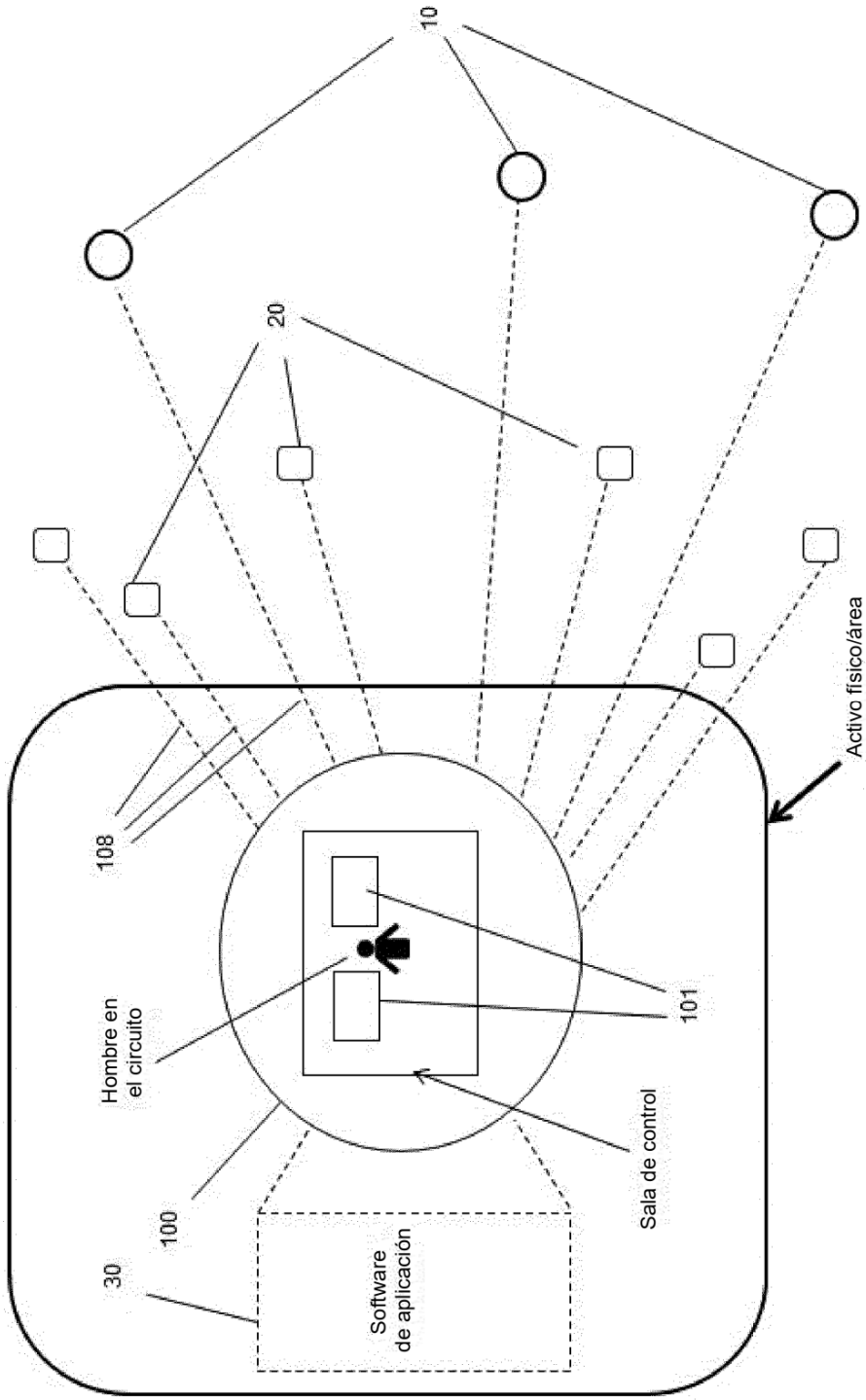

10
20
108
Hombre en el circuito
101
Activo físico/área
Sala de control
100
30
Software de aplicación

FIG. 1

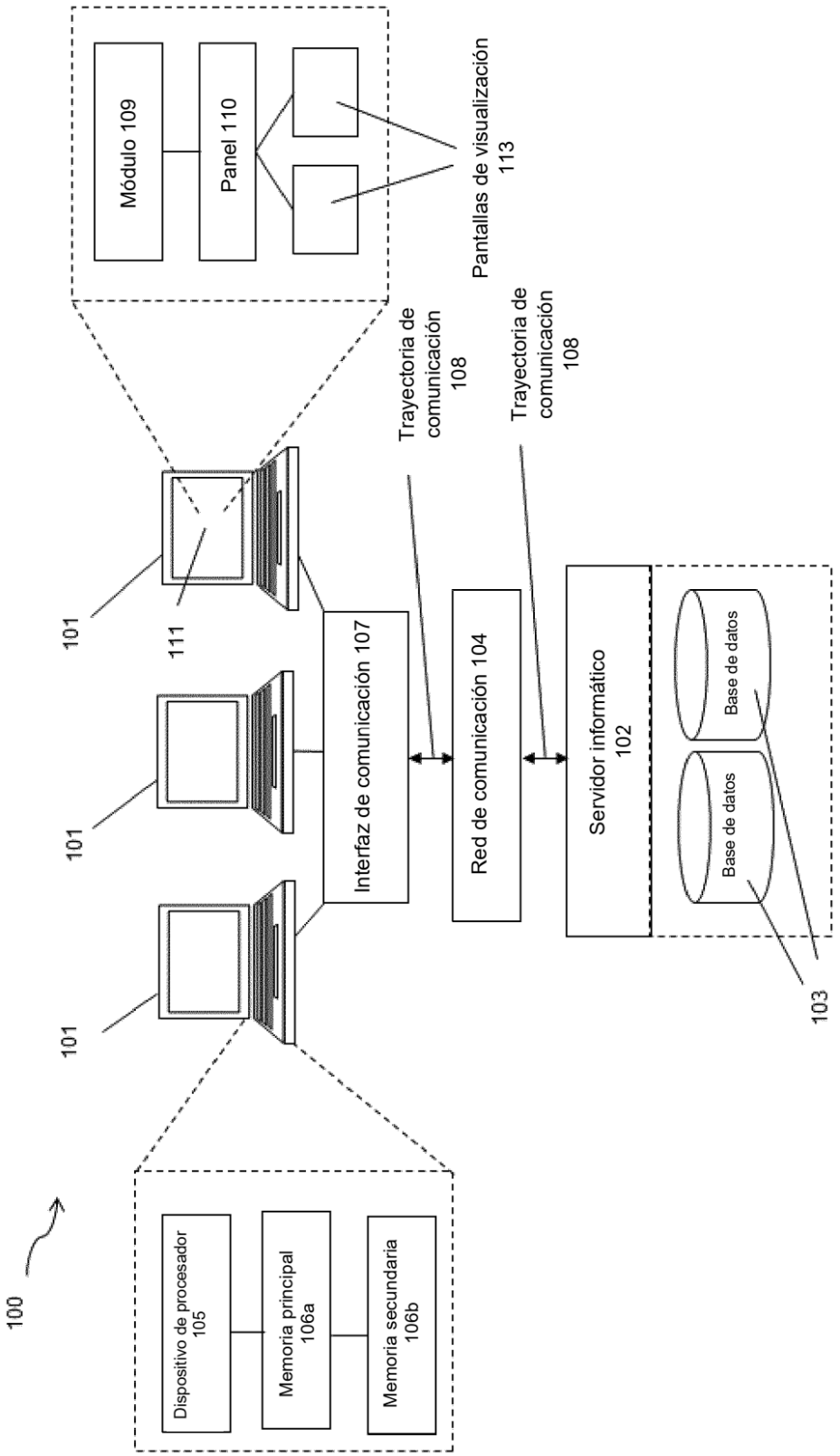

100
Dispositivo de procesador 105
Memoria principal 106a
Memoria secundaria 106b
101
101
101
111
Interfaz de comunicación 107
Trayectoria de comunicación 108
Trayectoria de comunicación 108
Red de comunicación 104
Servidor informático 102
Base de datos
Base de datos
103
Módulo 109
Panel 110
Pantallas de visualización 113

FIG. 2

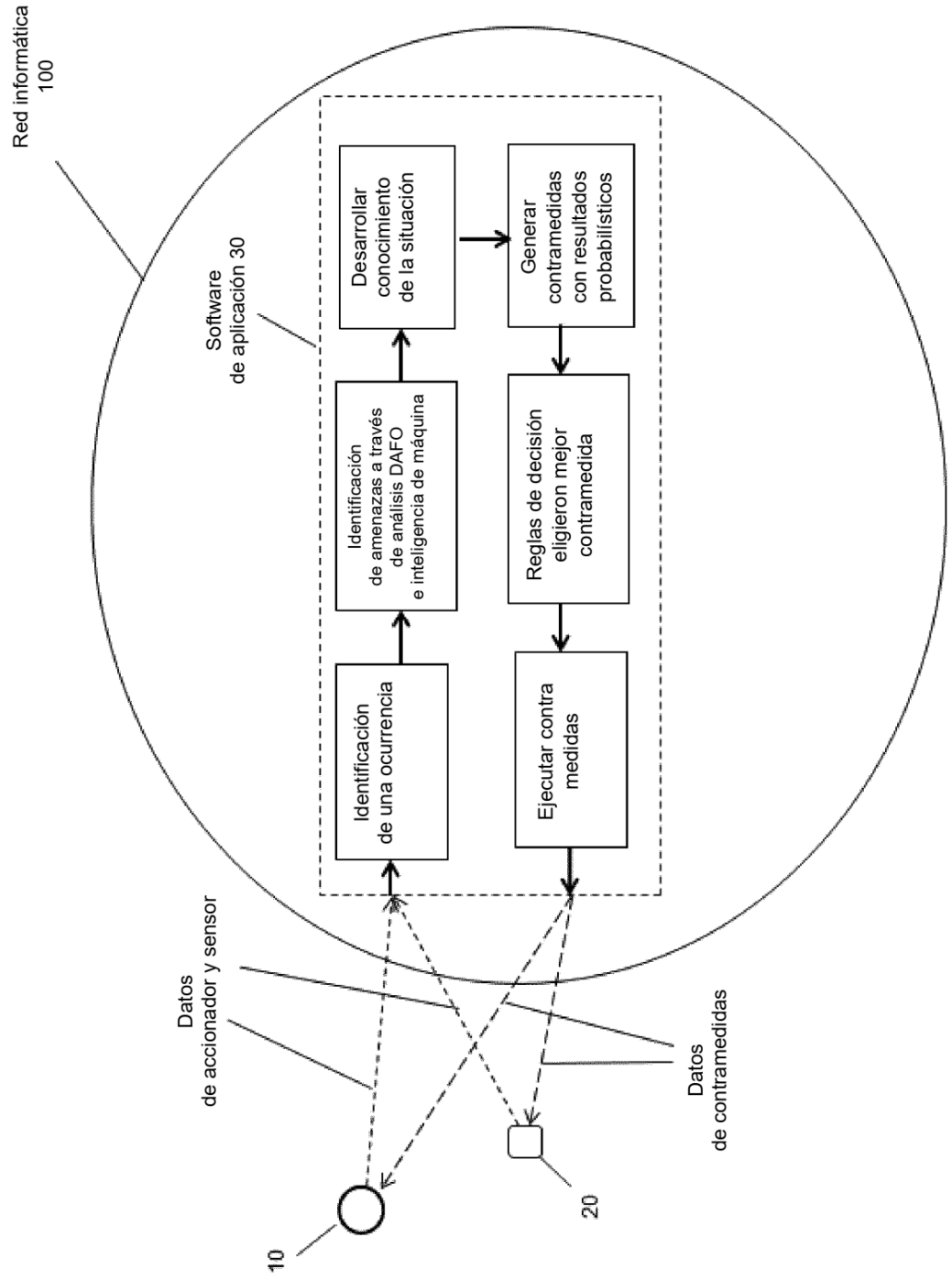

Red informática
100
Software
de aplicación 30
Identificación
de una ocurrencia
Identificación
de amenazas a través
de análisis DAFO
e inteligencia de máquina
Desarrollar
conocimiento
de la situación
Generar
contramedidas
con resultados
probabilísticos
Reglas de decisión
eligieron mejor
contramedida
Ejecutar contra
medidas
Datos
de accionador y sensor
Datos
de contramedidas
10
20

FIG. 3

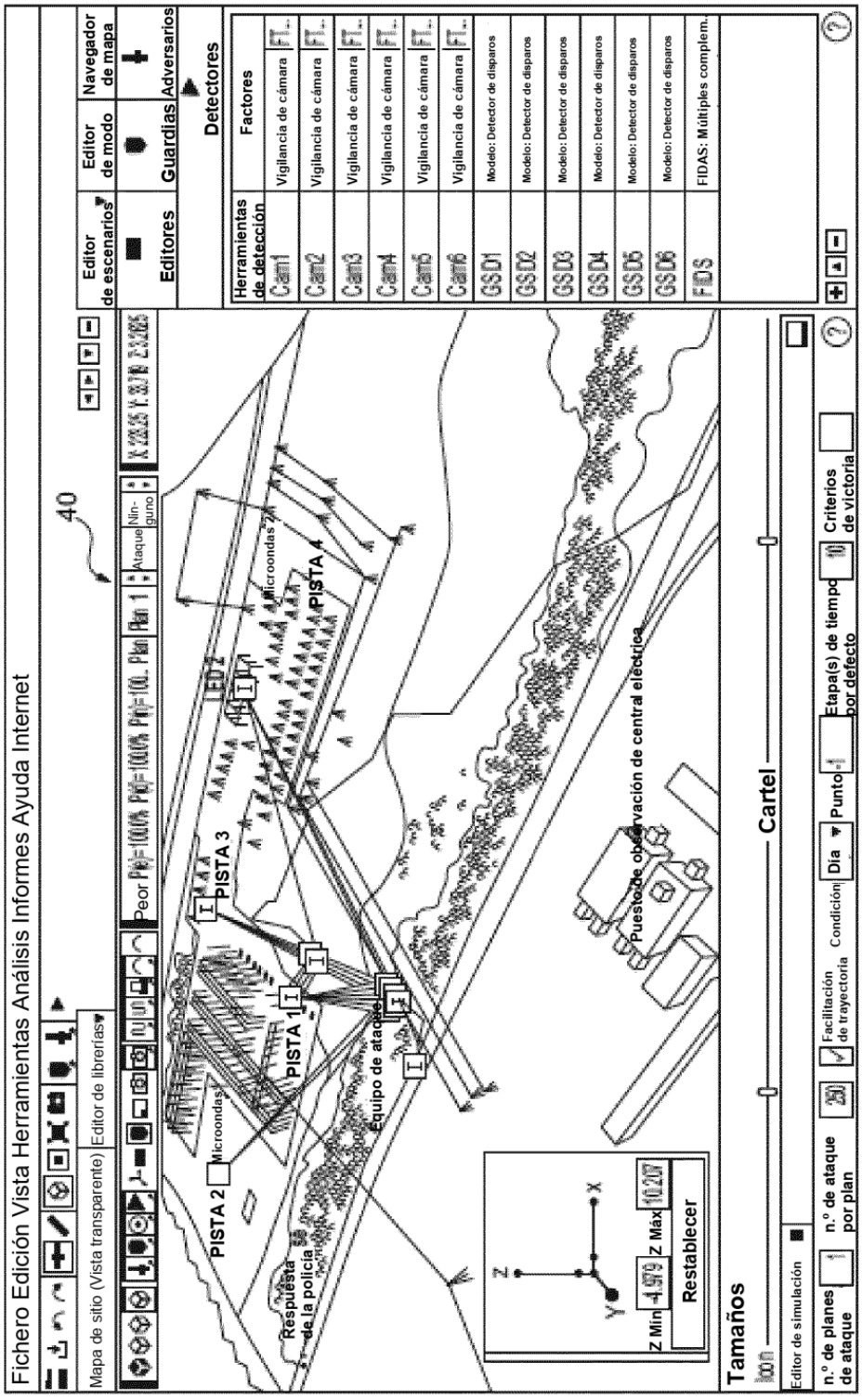

Fichero Edición Vista Herramientas Análisis Informes Ayuda Internet
Mapa de sitio (Vista transparente)
Editor de librerías
40
Editor de escenarios
Editor de modo
Navegador de mapa
Editores
Guardias
Adversarios
Detectores
Herramientas de detección
Factores
Cam1
Cam2
Cam3
Cam4
Cam5
Cam6
GSD1
GSD2
GSD3
GSD4
GSD5
GSD6
FIDS
Vigilancia de cámara
Modelo: Detector de disparos
FIDAS: Múltiples complem.
Peor
Plan 1
Ataque
Ningu
PISTA 1
PISTA 2
PISTA 3
PISTA 4
Microondas
Respuesta de la policía
Equipo de ataque
Puesto de observación de central eléctrica
Cartel
Tamaños
Z Min
Z Máx
Restablecer
Editor de simulación
n.º de planes de ataque
n.º de ataque por plan
Facilitación de trayectoria
Condición
Día
Punto
Etapa(s) de tiempo por defecto
Criterios de victoria

FIG. 4A

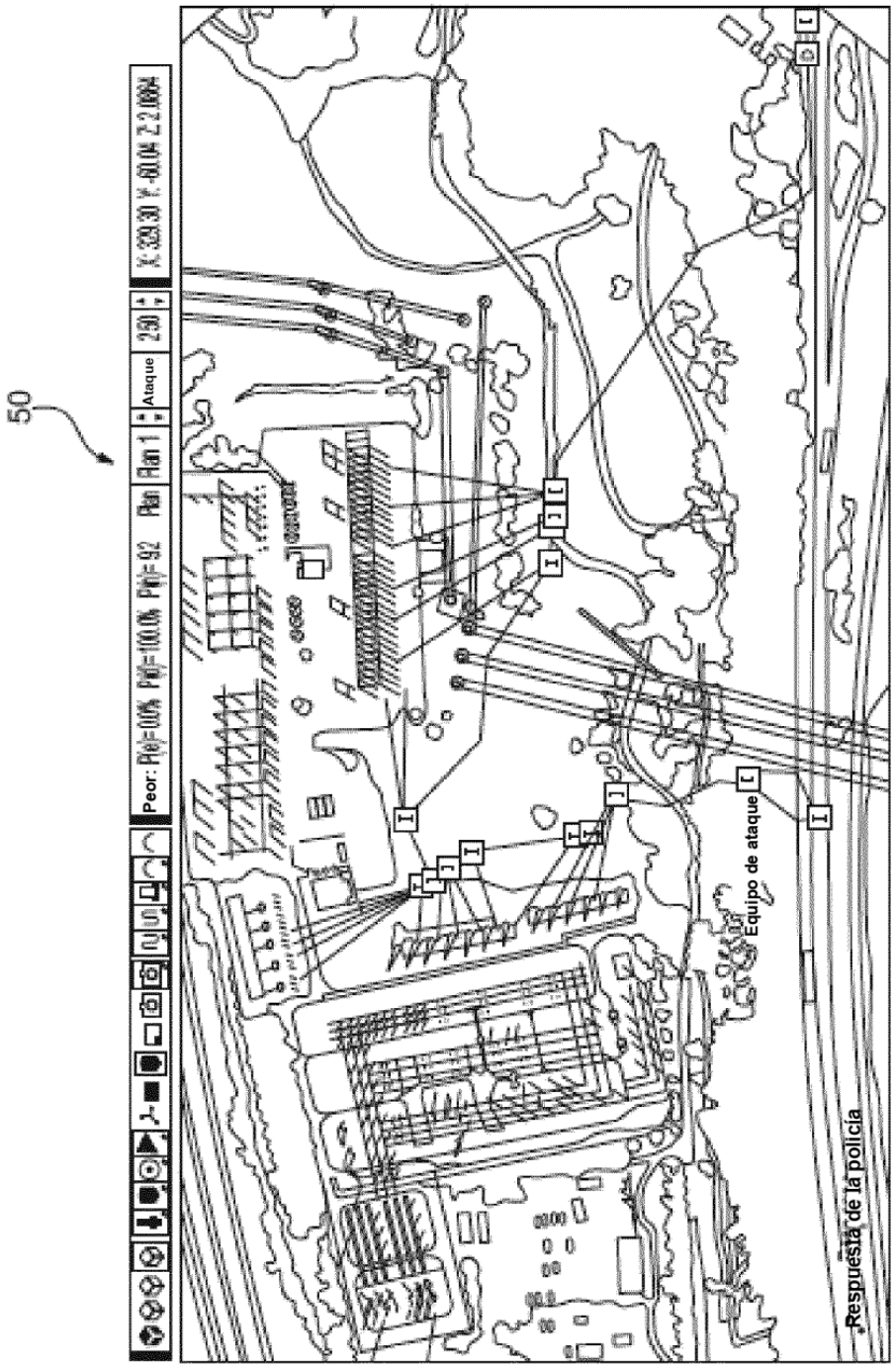

50
Peor:
Plan 1
Ataque
Equipo de ataque
Respuesta de la policía

FIG. 4B

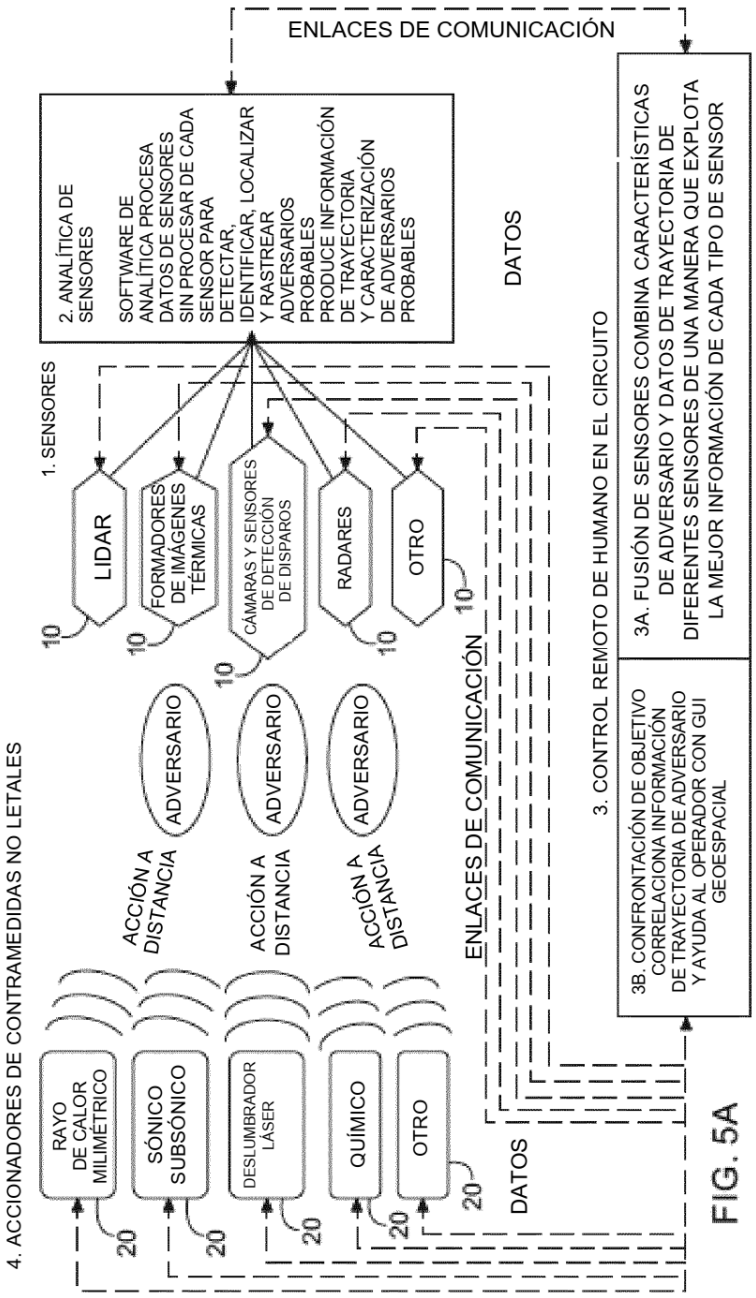

ENLACES DE COMUNICACIÓN
2. ANALÍTICA DE SENSORES
SOFTWARE DE ANALÍTICA PROCESA DATOS DE SENSORES SIN PROCESAR DE CADA SENSOR PARA DETECTAR, IDENTIFICAR, LOCALIZAR Y RASTREAR ADVERSARIOS PROBABLES PRODUCE INFORMACIÓN DE TRAYECTORIA Y CARACTERIZACIÓN DE ADVERSARIOS PROBABLES
DATOS
1. SENSORES
LIDAR
FORMADORES DE IMÁGENES TÉRMICAS
CÁMARAS Y SENSORES DE DETECCIÓN DE DISPAROS
RADARES
OTRO
10
ADVERSARIO
ACCIÓN A DISTANCIA
ENLACES DE COMUNICACIÓN
3. CONTROL REMOTO DE HUMANO EN EL CIRCUITO
3A. FUSIÓN DE SENSORES COMBINA CARACTERÍSTICAS DE ADVERSARIO Y DATOS DE TRAYECTORIA DE DIFERENTES SENSORES DE UNA MANERA QUE EXPLOTA LA MEJOR INFORMACIÓN DE CADA TIPO DE SENSOR
3B. CONFRONTACIÓN DE OBJETIVO CORRELACIONA INFORMACIÓN DE TRAYECTORIA DE ADVERSARIO Y AYUDA AL OPERADOR CON GUI GEOESPACIAL
4. ACCIONADORES DE CONTRAMEDIDAS NO LETALES
RAYO DE CALOR MILIMÉTRICO
SÓNICO SUBSÓNICO
DESLUMBRADOR LÁSER
QUÍMICO
OTRO
20
DATOS

FIG. 5A

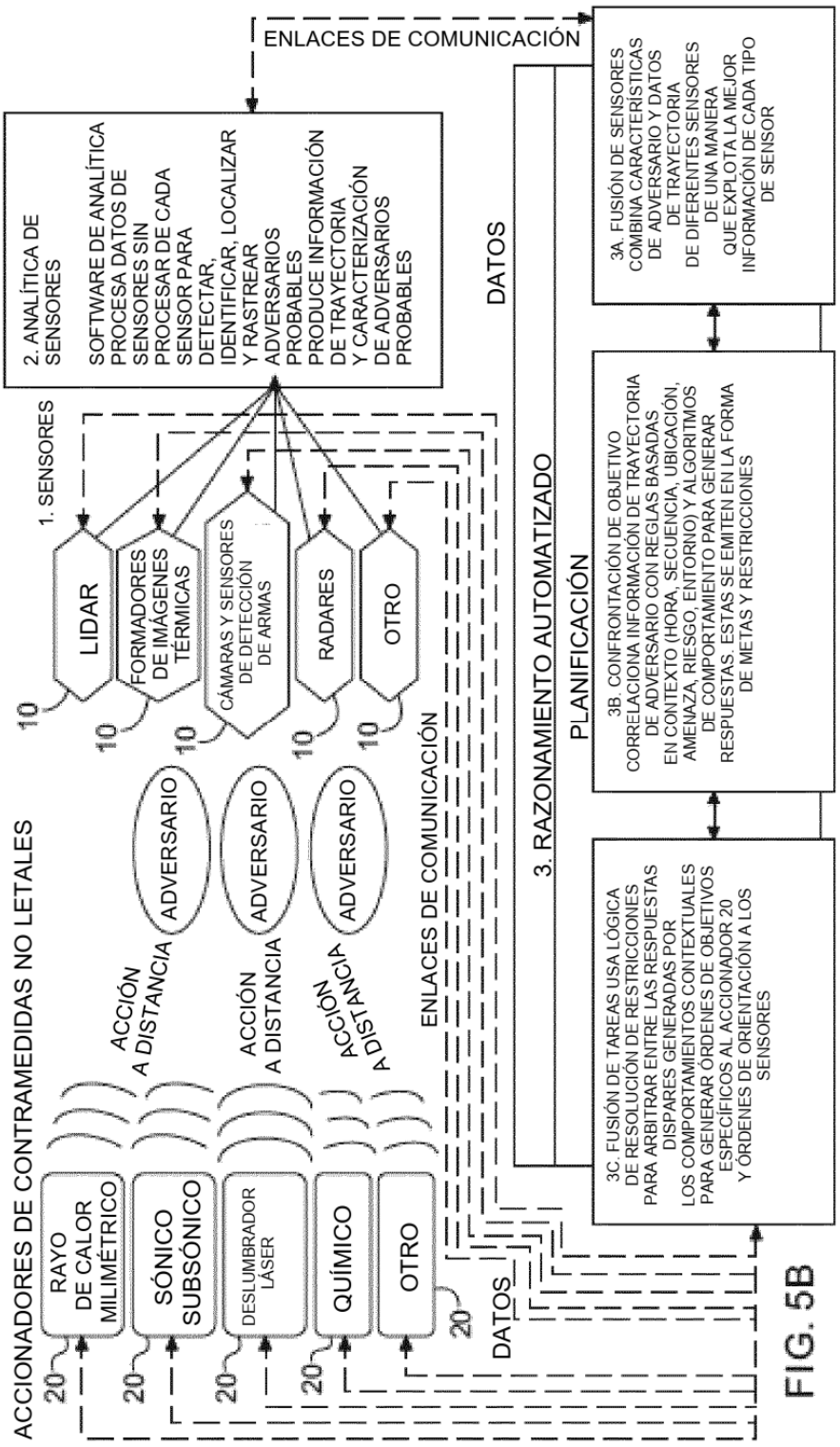

ENLACES DE COMUNICACIÓN
2. ANALÍTICA DE SENSORES
SOFTWARE DE ANALÍTICA PROCESA DATOS DE SENSORES SIN PROCESAR DE CADA SENSOR PARA DETECTAR, IDENTIFICAR, LOCALIZAR Y RASTREAR ADVERSARIOS PROBABLES PRODUCE INFORMACIÓN DE TRAYECTORIA Y CARACTERIZACIÓN DE ADVERSARIOS PROBABLES
DATOS
3A. FUSIÓN DE SENSORES COMBINA CARACTERÍSTICAS DE ADVERSARIO Y DATOS DE TRAYECTORIA DE DIFERENTES SENSORES DE UNA MANERA QUE EXPLOTA LA MEJOR INFORMACIÓN DE CADA TIPO DE SENSOR
1. SENSORES
LIDAR
FORMADORES DE IMÁGENES TÉRMICAS
CÁMARAS Y SENSORES DE DETECCIÓN DE ARMAS
RADARES
OTRO
10
3. RAZONAMIENTO AUTOMATIZADO
PLANIFICACIÓN
3B. CONFRONTACIÓN DE OBJETIVO CORRELACIONA INFORMACIÓN DE TRAYECTORIA DE ADVERSARIO CON REGLAS BASADAS EN CONTEXTO (HORA, SECUENCIA, UBICACIÓN, AMENAZA, RIESGO, ENTORNO) Y ALGORITMOS DE COMPORTAMIENTO PARA GENERAR RESPUESTAS. ESTAS SE EMITEN EN LA FORMA DE METAS Y RESTRICCIONES
ENLACES DE COMUNICACIÓN
ADVERSARIO
ACCIÓN A DISTANCIA
3C. FUSIÓN DE TAREAS USA LÓGICA DE RESOLUCIÓN DE RESTRICCIONES PARA ARBITRAR ENTRE LAS RESPUESTAS DISPARES GENERADAS POR LOS COMPORTAMIENTOS CONTEXTUALES PARA GENERAR ÓRDENES DE OBJETIVOS ESPECÍFICOS AL ACCIONADOR 20 Y ÓRDENES DE ORIENTACIÓN A LOS SENSORES
. ACCIONADORES DE CONTRAMEDIDAS NO LETALES
RAYO DE CALOR MILIMÉTRICO
SÓNICO SUBSÓNICO
DESLUMBRADOR LÁSER
QUÍMICO
OTRO
20
DATOS

FIG. 5B

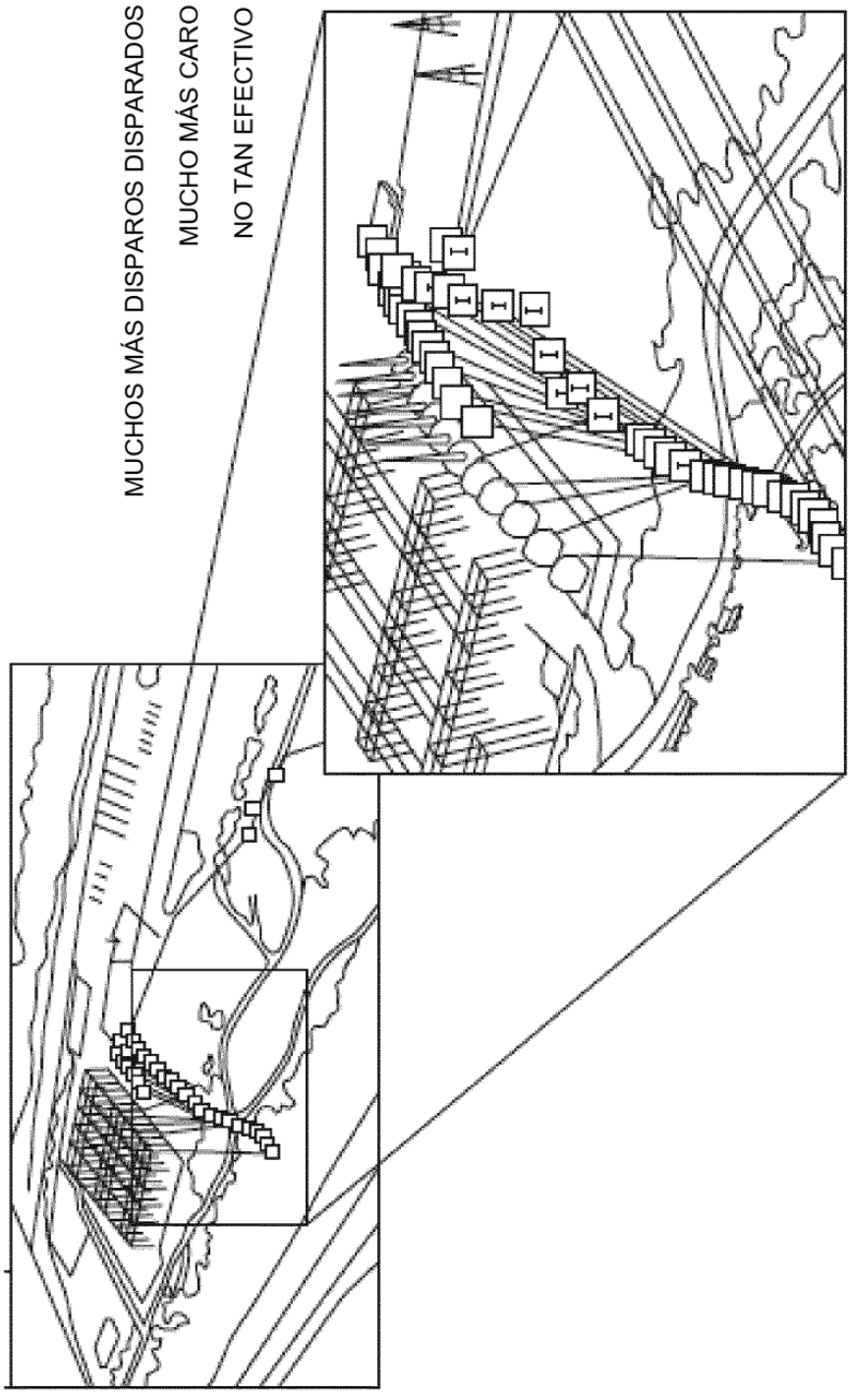

MUCHOS MÁS DISPAROS DISPARADOS
MUCHO MÁS CARO
NO TAN EFECTIVO

FIG. 6A

RCADS = GRANDES AHORROS

FUERZA DE SEGURIDAD PRESENCIAL CON PPS PASIVO
(EJEMPLO DE UN SOLO SITIO)

FUERZA DE PROTECCIÓN DE SUBESTACIÓN					
UNIDAD DE RESPUESTA RÁPIDA DE 4 PERSONAS	FTE (INCLUYENDO TIEMPO DE PREPARACIÓN Y DESPLAZAMIEN-TO)	FTE TOTALES	TASA DE MANO DE OBRA DE FTE CARGADO PROMEDIO POR HORA	HORAS DE FTE ANUALES TOTALES	COSTE ANUAL DE FTE TOTAL
4	6	24	50,00 $	499,20	2.496.000,00 $

ESTIMACIÓN DE COSTE DE SISTEMA DE PROTECCIÓN FÍSICA PASIVO (PPS)	
	3.000.000,00 $
MANTENIMIENTO ANUAL AL 15% DESPUÉS DEL PRIMER AÑO	450.000,00 $
COSTE DEL PRIMER AÑO DE PROPIEDAD (COMBINADO)	5.496.000,00 $
COSTE DE CINCO (5) AÑOS DE PROPIEDAD (COMBINADO)	17.280.000,00 $
COSTE DE DIEZ (10) AÑO DE PROPIEDAD (COMBINADO)	32.010.000,00 $

RCADS NO REQUIERE NINGUNA
FUERZA DE SEGURIDAD PRESENCIAL
(COMPARACIÓN DE UN SOLO SITIO)

ESTIMACIÓN DE COSTE DE SISTEMA DE PROTECCIÓN FÍSICA PASIVO (PPS) DE RCADS PASIVO		
(INCL PPS PASIVOS)	4.200.000,00 $	
MANTENIMIENTO ANUAL AL 15% DESPUÉS DEL PRIMER AÑO	630.000,00 $	
COSTE DEL PRIMER AÑO DE PROPIEDAD (COMBINADO)	4.200.000,00 $	
COSTE DE CINCO (5) AÑOS DE PROPIEDAD (COMBINADO)	6.720.000,00 $	
COSTE DE DIEZ (10) AÑO DE PROPIEDAD (COMBINADO)	9.870.000,00 $	

ESTIMACIÓN DE COSTE DE SISTEMA DE PROTECCIÓN FÍSICA PASIVO (PPS) DE RCADS PASIVO	
AHORROS DE COSTES EN CINCO **(5)** AÑOS	**10.560.000,00 $**
AHORROS DE COSTES EN DIEZ **(10)** AÑOS	**22.140.000,00 $**

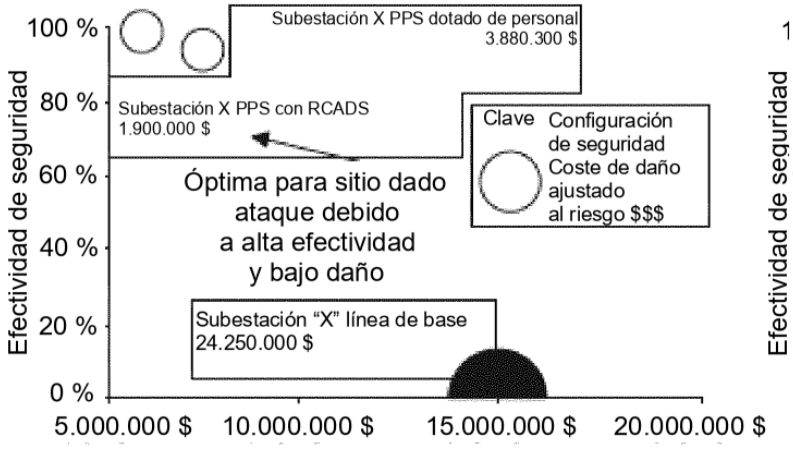
FIG. 6B

RESUMEN DE RESULTADOS

VISTA GENERAL

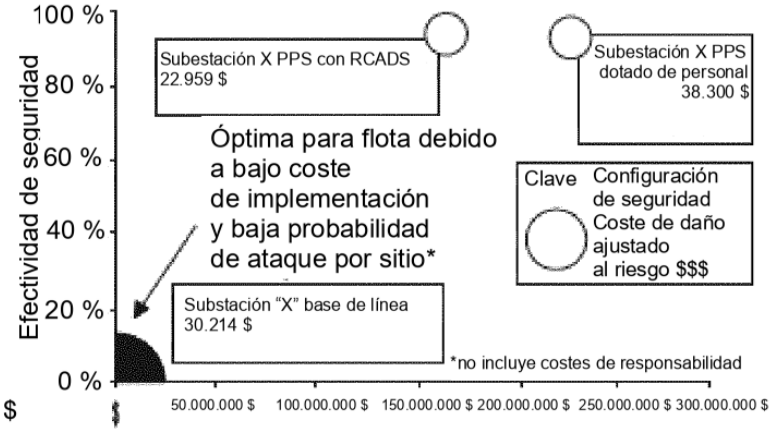
A CONTINUACIÓN ESTÁN LOS RESULTADOS ANALÍTICOS DE AVERT COMPILADOS, DESDE LA PERSPECTIVA DE SITIO GENÉRICO (IZQUIERDA) Y GESTIÓN DE UNA FLOTA DE 40 SUBESTACIONES TEÓRICAS (DERECHA). LA ELECCIÓN ÓPTIMA DEPENDE DE LA PERSPECTIVA. DADO UN ATAQUE DE TIPO FRANCOTIRADOR SIMILAR EN SUBESTACIÓN GENÉRICA, EL SISTEMA RCADS DEMUESTRA SER LA ELECCIÓN ÓPTIMA, CON UN COSTE BAJO DE IMPLEMENTACIÓN MIENTRAS QUE MANTIENE UNA ALTA EFECTIVIDAD Y TASAS BAJAS DE DAÑO. SIN EMBARGO, PARA UNA FLOTA DE SITIOS, CUALQUIER IMPLEMENTACIÓN DE SEGURIDAD A GRAN ESCALA DOMINA EL COSTE PARA UNA FLOTA. EN NINGUNO DE LOS CASOS LA SOLUCIÓN ÓPTIMA ES LA SOLUCIÓN DOTADA DE PERSONAL YA QUE LAS TASAS DE DAÑO Y COSTES SON MAYORES QUE LOS RCADS

EFECTIVIDAD DE SITIO GENÉRICO FRENTE A COSTES



Coste total = Coste de implementación de Metcalf + Daño de Metcalf

EFECTIVIDAD DE FLOTA GENÉRICA FRENTE A COSTES



Coste total = Coste de implementación de flota + Daño de flota

FIG. 6C

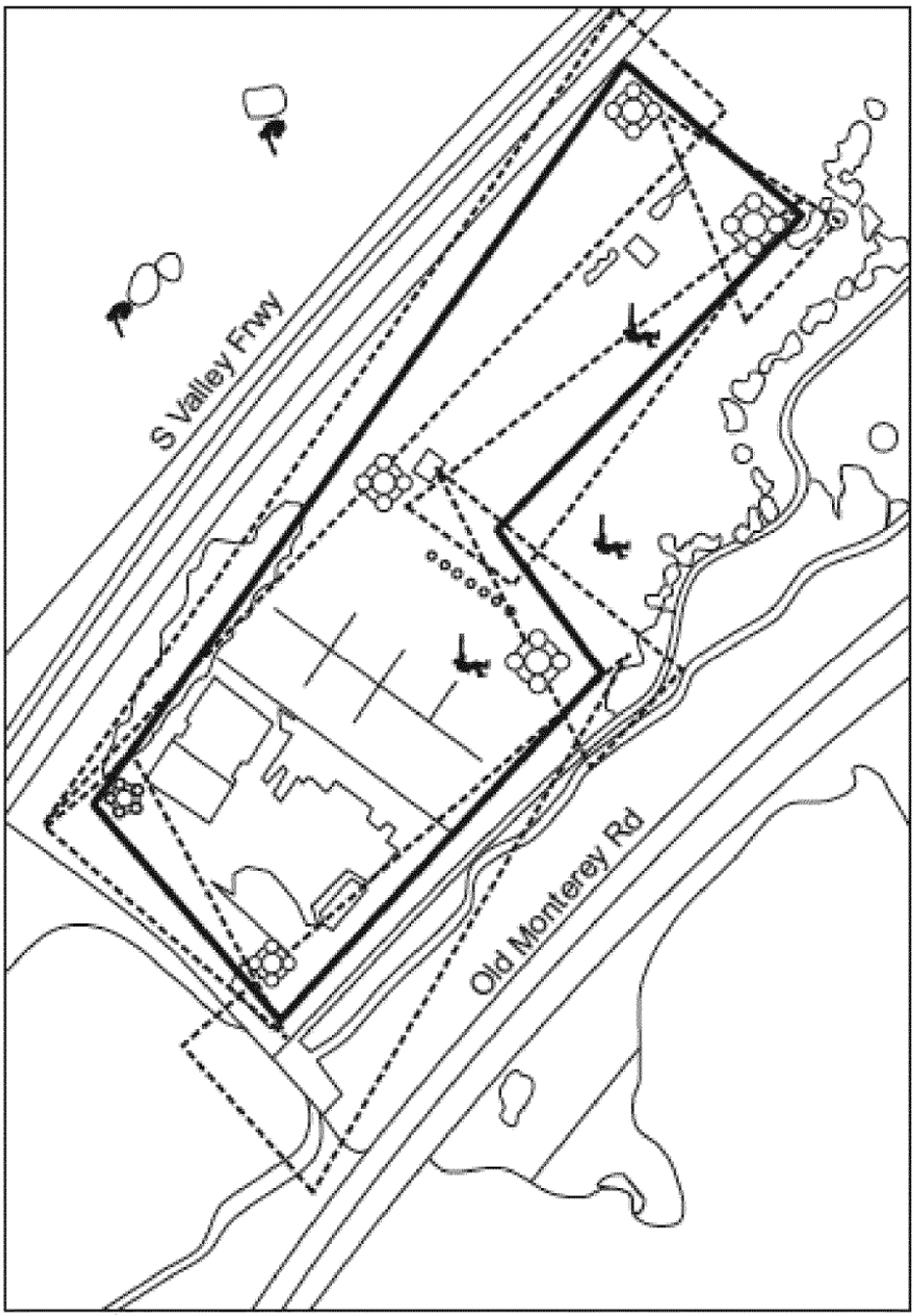


FIG. 7A

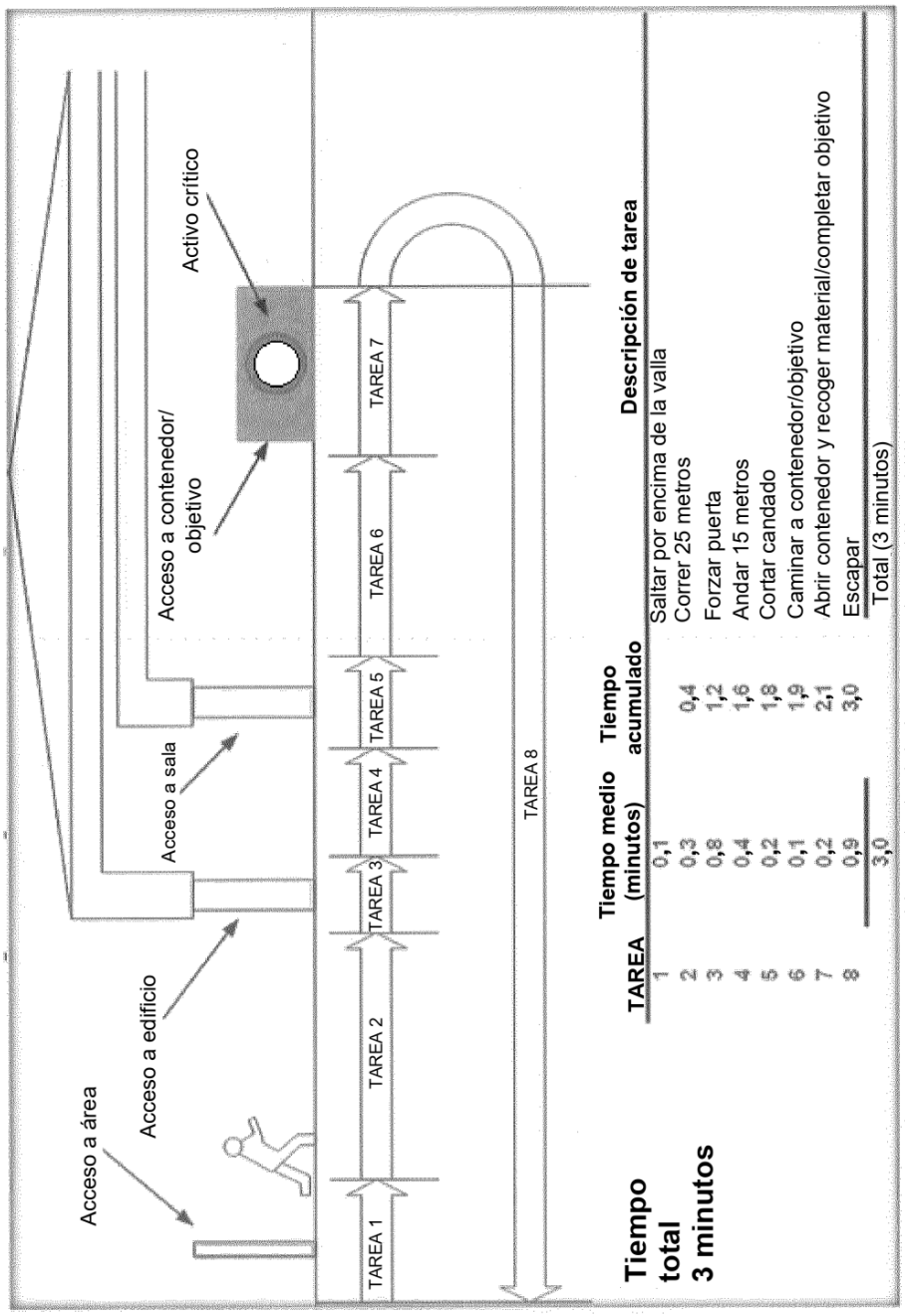

Acceso a área
Acceso a edificio
Acceso a sala
Acceso a contenedor/ objetivo
Activo crítico
TAREA 1
TAREA 2
TAREA 3
TAREA 4
TAREA 5
TAREA 6
TAREA 7
TAREA 8
Tiempo total 3 minutos
TAREA | Tiempo medio (minutos) | Tiempo acumulado | Descripción de tarea
1 | 0,1 | | Saltar por encima de la valla
2 | 0,3 | 0,4 | Correr 25 metros
3 | 0,8 | 1,2 | Forzar puerta
4 | 0,4 | 1,6 | Andar 15 metros
5 | 0,2 | 1,8 | Cortar candado
6 | 0,1 | 1,9 | Caminar a contenedor/objetivo
7 | 0,2 | 2,1 | Abrir contenedor y recoger material/completar objetivo
8 | 0,9 | 3,0 | Escapar
3,0 | | | Total (3 minutos)

FIG.7B

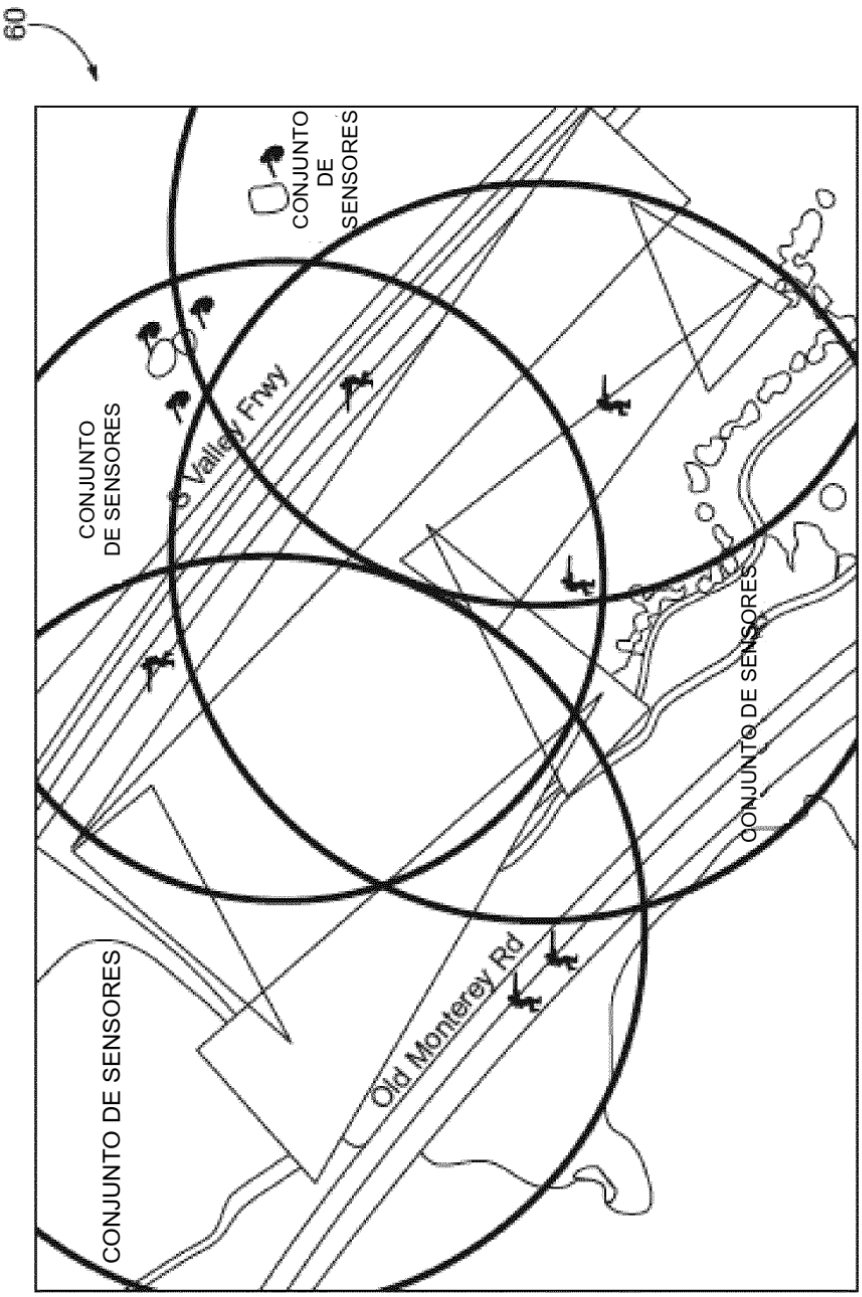

60
CONJUNTO DE SENSORES
CONJUNTO DE SENSORES
Valley Frwy
CONJUNTO DE SENSORES
CONJUNTO DE SENSORES
Old Monterey Rd

FIG. 8A

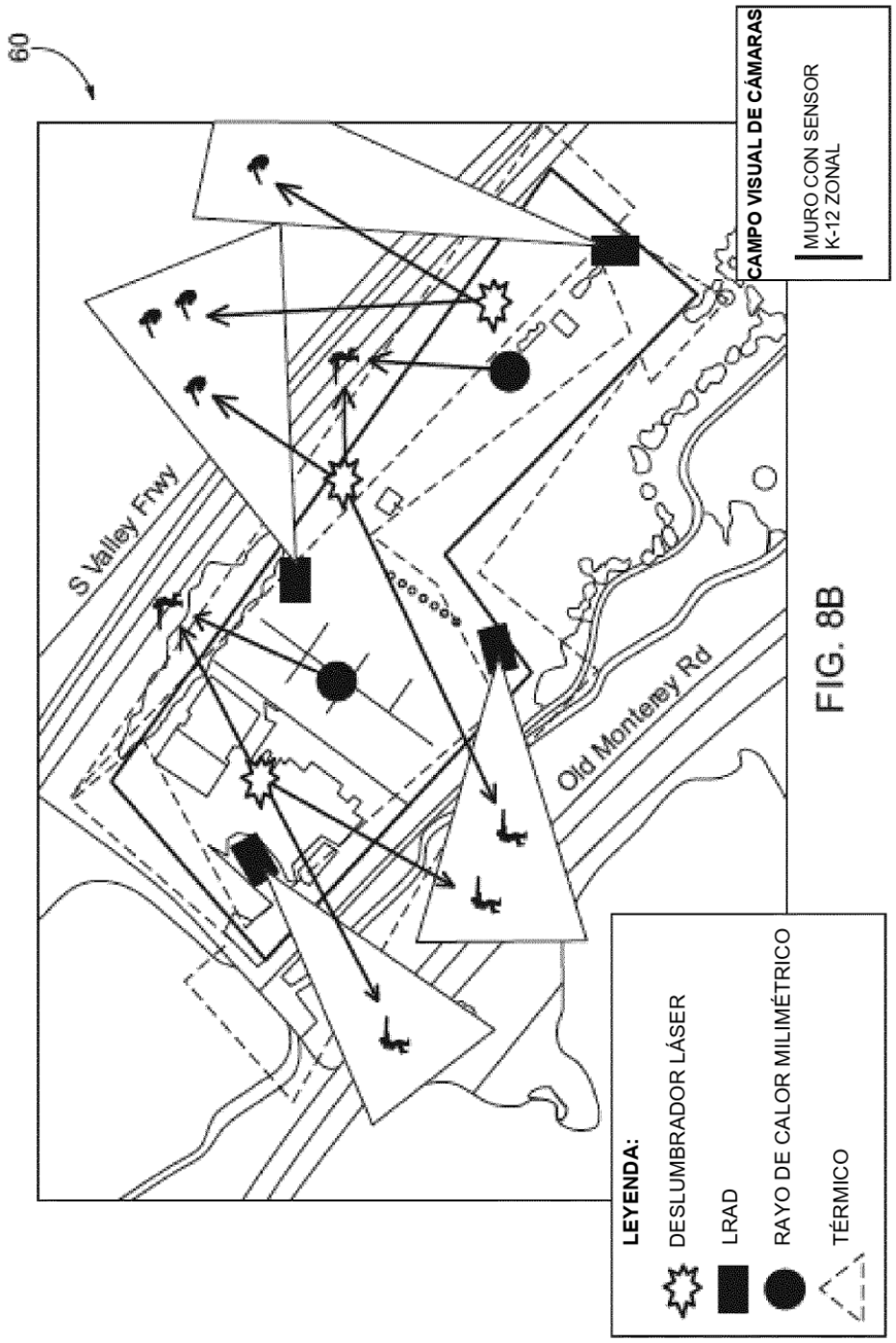

60
S Valley Frwy
Old Monterey Rd
CAMPO VISUAL DE CÁMARAS
MURO CON SENSOR
K-12 ZONAL
LEYENDA:
DESLUMBRADOR LÁSER
LRAD
RAYO DE CALOR MILIMÉTRICO
TÉRMICO

FIG. 8B

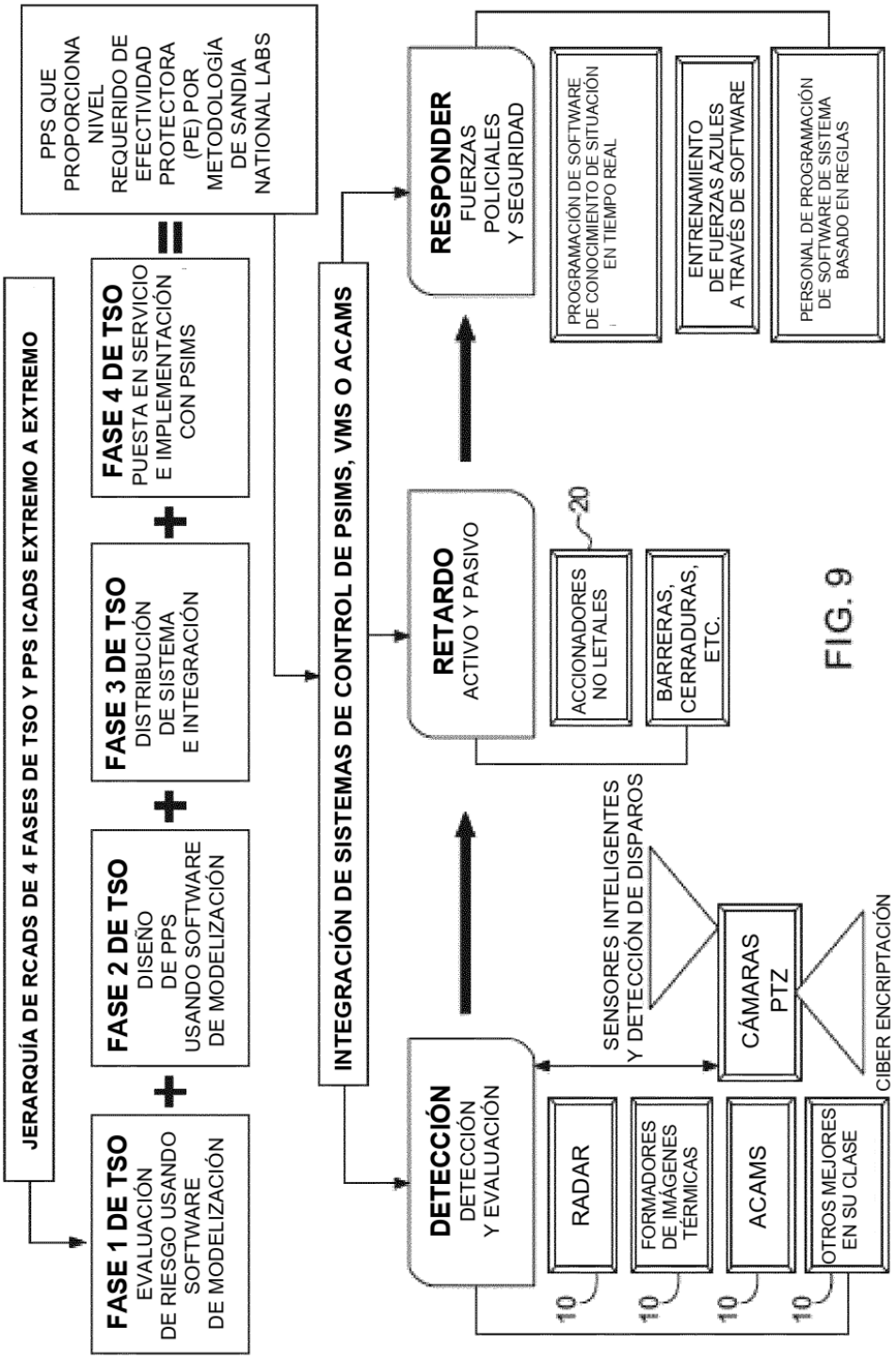

JERARQUÍA DE RCADS DE 4 FASES DE TSO Y PPS ICADS EXTREMO A EXTREMO
FASE 1 DE TSO
EVALUACIÓN
DE RIESGO USANDO
SOFTWARE
DE MODELIZACIÓN
FASE 2 DE TSO
DISEÑO
DE PPS
USANDO SOFTWARE
DE MODELIZACIÓN
FASE 3 DE TSO
DISTRIBUCIÓN
DE SISTEMA
E INTEGRACIÓN
FASE 4 DE TSO
PUESTA EN SERVICIO
E IMPLEMENTACIÓN
CON PSIMS
PPS QUE
PROPORCIONA
NIVEL
REQUERIDO DE
EFECTIVIDAD
PROTECTORA
(PE) POR
METODOLOGÍA
DE SANDIA
NATIONAL LABS
INTEGRACIÓN DE SISTEMAS DE CONTROL DE PSIMS, VMS O ACAMS
DETECCIÓN
DETECCIÓN
Y EVALUACIÓN
RADAR
FORMADORES
DE IMÁGENES
TÉRMICAS
ACAMS
OTROS MEJORES
EN SU CLASE
10
SENSORES INTELIGENTES
Y DETECCIÓN DE DISPAROS
CÁMARAS
PTZ
CIBER ENCRIPTACIÓN
RETARDO
ACTIVO Y PASIVO
20
ACCIONADORES
NO LETALES
BARRERAS,
CERRADURAS,
ETC.
RESPONDER
FUERZAS
POLICIALES
Y SEGURIDAD
PROGRAMACIÓN DE SOFTWARE
DE CONOCIMIENTO DE SITUACIÓN
EN TIEMPO REAL
ENTRENAMIENTO
DE FUERZAS AZULES
A TRAVÉS DE SOFTWARE
PERSONAL DE PROGRAMACIÓN
DE SOFTWARE DE SISTEMA
BASADO EN REGLAS

FIG. 9

ESPECTRO DE AMENAZA BASE DE DISEÑO (DBT) DE EJEMPLO PARA INFRAESTRUCTURA DE ENERGÍA ELÉCTRICA

(Desarrollar escenarios de ataque basándose en espectro de amenaza postulada para cada ubicación)

AMENAZA n.º 1

Adversario	N.º de adversarios	Conocimientos	Equipo/vehículos	Armas	Objetivo
Intruso de alto nivel (terrorista o activista)	3 a 5	Conocimiento amplio de operaciones de energía eléctrica, sistemas de seguridad y sistemas DCS/SCADA.	Herramientas de mano, herramientas eléctricas, explosivos, vehículos personales.	Armas de fuego, explosivos.	1) Destrucción de infraestructuras e interrupción del servicio. 2) Pérdida de confianza pública.

AMENAZA n.º 2

Adversario	N.º de adversarios	Conocimientos	Equipo/vehículos	Armas	Objetivo
Infiltrado de nivel medio-alto (antiguo empleado o actual, disgustado)	1 a 2	Conocimiento (medio a amplio) de operaciones de energía eléctrica, sistemas de seguridad y sistemas DCS/SCADA.	Herramientas de mano, herramientas eléctricas y vehículos personales.	Armas de fuego, explosivos, cuchillos.	Destrucción de infraestructuras, equipo y provocar daño financiero o sufrimiento a personal/dirección actual.

AMENAZA n.º 3

Adversario	N.º de adversarios	Conocimientos	Equipo/vehículos	Armas	Objetivo
Intruso de nivel medio-alto con conocimiento interno (extremista)	2 a 3	Conocimiento moderado de sistemas de energía eléctrica	Herramientas de mano, herramientas eléctricas y vehículos personales.	Ninguna	Interrupción del servicio, provocar sufrimiento financiero, notoriedad, humillación de la empresa.

AMENAZA n.º 4

Adversario	N.º de adversarios	Conocimientos	Equipo/vehículos	Armas	Objetivo
Intruso de nivel medio-bajo (vándalo)	1 a 5	Poco o ningún conocimiento de sistemas de energía eléctrica.	Herramientas de mano y vehículos personales.	Armas de fuego, cuchillos.	Daño de equipo o notoriedad.

FIG.10