(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 784 258**

(51) Int. CI.:

G06F 21/56 (2013.01)
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)
G05B 17/00 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.10.2014 PCT/IB2014/065710**

(87) Fecha y número de publicación internacional: **07.05.2015 WO15063715**

(96) Fecha de presentación y número de la solicitud europea: **30.10.2014 E 14859246 (2)**

(97) Fecha y número de publicación de la concesión europea: **15.01.2020 EP 3063694**

(54) Título: **Defensa cibernética**

(30) Prioridad:

01.11.2013 US 201361898487 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.09.2020

(73) Titular/es:

CYBERGYM CONTROL LTD. (100.0%)
5 Hatzoref Street
58856 Holon, IL

(72) Inventor/es:

HASON, OFIR

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Defensa cibernética

Campo técnico

Las realizaciones de la invención se refieren a procedimientos de protección de instalaciones de infraestructura contra ciberataques.

Antecedentes

Las instalaciones de infraestructura modernas, tales como centrales eléctricas, plantas de tratamiento de agua, sistemas de distribución de oleoductos y gasoductos, en lo sucesivo, genéricamente denominada instalaciones de infraestructura, son instalaciones complejas que producen, controlan y/o distribuyen grandes cantidades de recursos esenciales para el buen funcionamiento de la sociedad moderna. Cada instalación de infraestructura incorpora un entorno complicado que por lo general comprende una red de operarios humanos y un sistema integrado de equipos automatizados, sistemas de vigilancia y una red de ordenadores que cooperan para controlar los equipos que responden a los datos proporcionados por los sistemas de vigilancia y los operarios humanos. Los ordenadores, sistemas de vigilancia, los equipos y los operarios se comunican a través de una red de comunicación que puede comprender dispositivos de comunicación tanto inalámbricos como por cable. Los ordenadores y los conjuntos de instrucciones que ejecutan y los sistemas de información a los que acceden, los sistemas de vigilancia y la red de comunicación se conocen convencionalmente como un sistema de control de supervisión y adquisición de datos (SCADA). Los operarios humanos acceden a SCADA a través del equipo de interfaz hombre-máquina (HMI), como consolas, teclados y equipos de control de reconocimiento de voz.

Una sola instalación de infraestructura dada puede proporcionar servicios y recursos a una población en un área de servicio de la instalación que puede tener una extensión geográfica relativamente limitada, como la de un pequeño pueblo o parte de un pueblo, o para una población en una región geográfica relativamente extendida, como la de una gran ciudad, grupo de ciudades, o un estado. Por lo general, las instalaciones de infraestructura están integradas para cooperar y proporcionar servicios y recursos a las poblaciones en regiones geográficas muy grandes que se extienden más allá del área de servicio de una sola de las instalaciones de infraestructura cooperantes.

Por ejemplo, considerando que una sola central eléctrica puede proporcionar energía a una población de todo el vecindario o de la ciudad, se puede integrar una pluralidad de centrales eléctricas para formar una red eléctrica que proporciona energía a una población en una región de un país que comprende un estado, o más de un estado en el país. Y se puede integrar una pluralidad de centrales eléctricas para proporcionar una red eléctrica de centrales eléctricas interdependientes que proporciona energía a un país o a una región geográfica que se extiende más allá de las fronteras de un solo país. Por ejemplo, una red eléctrica conocida como la interconexión de Quebec proporciona energía a la provincia canadiense de Quebec y al noreste de los Estados Unidos. Las redes eléctricas Western Interconnection y Eastern Interconnection proporcionan energía respectivamente a los estados occidentales de los Estados Unidos y a los estados del sudeste de los Estados Unidos. El sistema Indian Power se divide en cinco grandes redes regionales. una gran red eléctrica proporciona energía a la mayor parte de Europa continental.

Las diversas centrales eléctricas y redes eléctricas concentran, usan y controlan activos físicos y económicos de enorme valor, y las interrupciones y/o daños a su funcionamiento o a los activos pueden causar daños económicos sustanciales a las economías nacionales y globales, causar daños físicos e incluso provocar la pérdida de vidas. Por ejemplo, una pérdida de energía conocida como el apagón de 2003 dejó a unos cincuenta y cinco millones de personas en el noreste de Canadá y los Estados Unidos sin electricidad durante unas cuatro horas. Se estima que el "corto" apagón de cuatro horas ha costado unos seis mil millones de dólares.

El apagón fue causado por un error de software en un sistema de alarma en FirstEnergy Corporation de Ohio. El error evitó que se activara una alarma para alertar a los operarios de que redistribuyan la energía de la línea de transmisión después de que las líneas de transmisión sobrecargadas en un área rural se hundieran y golpearan los árboles, causando una descarga repentina que dejó fuera de servicio las líneas caídas. Las líneas fuera de servicio provocaron una falla en cascada en la que otras líneas de transmisión se sobrecargaron sucesivamente, dejándolas rápidamente fuera de servicio y generando el apagón.

Si bien el apagón de 2003 no fue intencional, las instalaciones de energía, como centrales eléctricas y redes eléctricas, están expuestos a daños intencionales por ciberataques de diversos grados de sofisticación y gravedad. Los ciberataques intentan infligir daños en las instalaciones de energía explotando las vulnerabilidades de los sistemas SCADA que controlan las instalaciones ante diversos tipos de ataques que pueden dañar su funcionamiento. Los ciberataques pueden estar dirigidos a conjuntos de instrucciones informáticas comprometedoras, ejecución de los conjuntos de instrucciones, datos procesados mediante la ejecución de los conjuntos de instrucciones y/o a cómo se comunican los ordenadores entre sí, con equipos que controlan, y/o el mundo exterior. Los ejemplos de ciberataques incluyen: denegación de servicio; presentación de solicitud falsa o información falsa al personal operativo; entrada de datos espurios a bases de datos y/o equipos; operación no autorizada de los equipos de la instalación; interrupción de las comunicaciones; y corrupción del conjunto de instrucciones por malware como el gusano informático stuxnet.

Para proteger las instalaciones, los operarios implementan diversos procedimientos de seguridad e instalan diversas tecnologías diseñadas para evitar y/o mitigar las consecuencias de un ciberataque. Sin embargo, la complejidad de las instalaciones y los recursos tecnológicos y financieros a menudo fácilmente disponibles para las personas, las organizaciones y los estados nacionales para elaborar un ciberataque permiten miles de escenarios posibles para ciberataques de diferentes formas y perniciosidad. Como resultado, configurar la protección adecuada para una central de energía es una tarea difícil que generalmente requiere abordar un gran perfil de problemas de seguridad y generalmente requiere una revisión repetida. Mientras que los procedimientos y tecnologías de seguridad implementados parecen ser relativamente efectivos para abordar un tatuaje de fondo constante, de nivel relativamente bajo, ciberataques a pequeña escala a los que las instalaciones están regularmente expuestas, es difícil, si no imposible, por ejemplo, predecir su eficacia contra eventos cibernéticos de baja frecuencia y alto impacto (HILF), "cisne negro".

El documento US2013/198847 desvela un procedimiento implementado por ordenador para su uso en la evaluación de al menos una amenaza a un sistema complejo que incluye identificar uno o más componentes físicos del sistema complejo y modelar uno o más componentes físicos con múltiples agentes de software interactivo. Los múltiples agentes están programados para vigilar y controlar al menos una función de los componentes físicos modelados. Se identifican una o más amenazas a un objetivo del sistema complejo. Cada amenaza se define como una amenaza cibernética o física y el objetivo se define como un componente cibernético o componente físico. El procedimiento incluye simular un ataque al sistema complejo por la amenaza identificada y evaluar el impacto del ataque en el sistema complejo.

Sumario

Un aspecto de una realización de la invención se refiere a proporcionar un procedimiento para desarrollar tecnologías de software y hardware, protocolos y sistemas, en lo sucesivo denominadas genéricamente tecnologías de "protección cibernética", para evitar y/o mitigar las consecuencias de los ciberataques en una instalación de infraestructura. En una realización de la invención, la instalación de infraestructura comprende una central de energía. Opcionalmente, el procedimiento facilita la mejora de la anticipación de los ciberataques.

Un aspecto de una realización de la invención se refiere a proporcionar una instalación de simulación que comprende un modelo operativo de la central de energía que imita las operaciones de la central de energía "real", en la que y con la que las personas de la instalación de simulación interactúan para generar tecnologías de protección cibernética. El modelo operativo, que se puede denominar instalación modelo, comprende equipos reales y/o virtuales que corresponden y operan de forma similar a los equipos en la central de energía real.

Un aspecto de una realización de la invención se relaciona con la configuración de un "formato de interacción" de acuerdo con el que las personas interactúan y con la instalación de simulación.

En un formato de interacción en una realización de la invención, el primer y segundo equipo de personas tienen acceso a la instalación de simulación para generar tecnologías de protección cibernética. El primer equipo de personas, en lo sucesivo, también denominados "agentes de ataque de simulación", tiene instrucciones de intentar montar ciberataques en la instalación modelo para interrumpir las operaciones de la instalación modelo. El segundo grupo de personas, en lo sucesivo, también denominados "agentes de defensa de simulación", tiene instrucciones de defender la instalación modelo contra ciberataques y mantener el funcionamiento normal de la instalación modelo.

Un aspecto de una realización de la invención se relaciona con las actividades de vigilancia de los agentes de defensa y ataque de simulación para competir entre sí e implementar y/o crear estrategias cibernéticas para interrumpir y frustrar la interrupción del funcionamiento de la instalación modelo para adquirir un registro forense de las actividades. El registro forense puede procesarse como se describe a continuación para proporcionar tecnologías de protección cibernética para la instalación modelo y la instalación real.

El registro forense puede incluir una historia cronológica de las acciones realizadas por los agentes de ataque de simulación en ataques crecientes en la instalación modelo y las medidas defensivas tomadas por los agentes de defensa para defender la instalación modelo contra los ataques y los resultados de los ataques y medidas defensivas. La actividad de vigilancia de los agentes de defensa y ataque de simulación pueden incluir la vigilancia de la actividad HMI de los agentes. La vigilancia de la actividad HMI incluye opcionalmente el registro de pulsaciones de teclas para seguir el uso de teclados por parte de los agentes de simulación para montar un ciberataque y/o participar y usar un conjunto de instrucciones informáticas defensivas para protegerse contra el ciberataque. La vigilancia de la actividad HMI puede comprender la vigilancia de la interacción de un agente de simulación con una pantalla de video del ordenador, opcionalmente mediante el uso de tecnología de seguimiento ocular para rastrear la dirección de la mirada del agente y determinar los puntos de vista del agente de simulación (POR) y el movimiento del POR entre las características de la pantalla. Opcionalmente, la actividad de vigilancia de los agentes de simulación comprende la vigilancia de las características fisiológicas de los agentes para proporcionar indicaciones, por ejemplo, de niveles de preocupación, estrés y/o estado de alerta.

Un aspecto de una realización de la invención se refiere al procesamiento de datos en el registro forense para proporcionar reconocimiento de ciberataque, sistemas y/o protocolos de alerta y respuesta para su uso en la protección

de la instalación modelo contra ciberataques montados por los agentes de ataque de simulación y, opcionalmente, para proteger la central de energía real contra ciberataques montados por agentes de ataque reales. Proporcionar los sistemas y/o protocolos opcionalmente comprende procesar los datos forenses para generar una base de datos, en lo sucesivo, también denominada base de datos de ciberataques y defensa (base de datos CYBAD) que comprende datos que identifican y caracterizan ciberataques y ciberdefensas.

En una realización de la invención, los ciberataques se identifican y caracterizan en CYBAD por vectores característicos. Los componentes de un vector característico de ciberataque codifican opcionalmente valores para parámetros que miden el rendimiento del equipo real y virtual en la central de energía modelo que corresponde al equipo en la central de energía real. Opcionalmente, los componentes del vector característico incluyen a modo de ejemplo, valores para retrasar la transmisión y/o mediciones de pérdida de paquetes para datos transmitidos entre una lista particular de nodos en el sistema SCADA de la planta de energía, temperaturas de un conjunto de turbinas, y/o tiempos de la última configuración de las clasificaciones de sobrecorriente del interruptor automático. Opcionalmente, un vector característico de ciberataque codifica un árbol de ataque que caracteriza el ciberataque.

En una realización de la invención, se define al menos un vector característico de estado para la instalación modelo y, opcionalmente, la central de energía real. El al menos un vector característico de estado comprende componentes que pueden usarse para reconocer e indicar una probabilidad de que el modelo o la instalación real estén sujetos a un ciberataque y se reevalúen repetidamente. Opcionalmente, el reconocimiento de una probabilidad de ataque en un momento dado se determina en respuesta a un producto escalar del vector de estado en el momento dado y un vector característico comprendido en la base de datos CYBAD.

En una realización de la invención, las estrategias de defensa para evitar y/o minimizar los efectos de los ciberataques se identifican y caracterizan en la base de datos CYBAD por "vectores característicos de defensa". Una contramedida a un ciberataque dado puede determinarse en respuesta a un valor de un producto escalar del vector característico de ciberataque y un vector característico de defensa.

En una realización de la invención, los sistemas y/o protocolos están configurados y ejecutados por redes neuronales que están entrenadas en datos comprendidos en la base de datos CYBAD.

Por lo tanto, se proporciona, de acuerdo con una realización de la invención, una instalación de simulación cibernética que comprende: una instalación de modelo físico operativo de una instalación de infraestructura real que imita al menos en parte las operaciones de la instalación de infraestructura real y comprende equipo que corresponde e imita las operaciones de equipo en la instalación de infraestructura real; software de herramientas de ataque para su uso por personas en el montaje de ciberataques en la instalación modelo; software de herramientas de gestión y operaciones para su uso por personas en el funcionamiento y defensa de la instalación modelo contra ciberataques montados usando el software de herramientas de ataque; y un controlador con memoria y operable para adquirir y almacenar en la memoria un registro forense de ciberataques montados en la instalación modelo y estrategias de defensa emprendidas para defender la instalación modelo contra los ciberataques.

Opcionalmente, el equipo en la instalación modelo comprende equipos físicos. Como alternativa o adicionalmente, el equipo en la instalación modelo puede comprender equipos virtuales.

En una realización de la invención, la instalación de simulación cibernética comprende agentes recopiladores que adquieren datos de estado de operaciones relevantes o indicativos del funcionamiento del equipo en la instalación modelo. Opcionalmente, el controlador recibe los datos de estado de operaciones y almacena los datos de estado de operaciones en la memoria como parte del registro forense. La instalación de simulación cibernética opcionalmente comprende un módulo creador de modelos que procesa datos en el registro forense para generar vectores de estado de operaciones que comprenden componentes que tienen valores que responden a los datos de estado de operaciones proporcionados por cada uno de una pluralidad de agentes recopiladores.

En una realización de la invención, la instalación de simulación cibernética comprende sensores de actividad humana que adquieren datos indicativos de la actividad de personas que usan el software de herramientas de ataque para montar ciberataques en la instalación modelo o usan el software de herramientas de operaciones y gestión para operar y defender la instalación modelo contra los ciberataques. Opcionalmente, el controlador recibe los datos adquiridos por los sensores de actividad humana y almacena los datos recibidos en la memoria como parte del registro forense. En una realización de la invención, la instalación de simulación cibernética comprende un módulo creador de modelos que procesa datos en el registro forense para generar vectores de estado de operaciones que tienen componentes que tienen valores que responden a los datos proporcionados por cada uno de una pluralidad de sensores de actividad humana.

En una realización de la invención, el módulo creador de modelos define al menos un clasificador que responde a los vectores de estado de operaciones para determinar si un vector de estado de operaciones en un momento dado indica que la instalación modelo se encuentra bajo un ciberataque. Opcionalmente, el al menos un clasificador comprende un clasificador de vectores de soporte. Como alternativa o adicionalmente, el al menos un clasificador comprende una red neuronal.

Además, se proporciona de acuerdo con una realización de la invención, una instalación de infraestructura real

configurada para usar el registro forense proporcionado por una instalación de simulación cibernética de acuerdo con una realización de la invención para defender la infraestructura real contra el ciberataque.

Se proporciona además, de acuerdo con una realización de la invención, una instalación de infraestructura real configurada para usar un clasificador de acuerdo con una realización de la invención para determinar si la instalación real se encuentra bajo un ciberataque.

En una realización de la invención, la instalación de infraestructura real comprende una central eléctrica.

Además, de acuerdo con una realización de la invención, se proporciona un procedimiento para desarrollar una estrategia para defender una instalación de infraestructura contra ciberataques, el procedimiento comprende: adquirir un registro forense proporcionado por una instalación de simulación cibernética de acuerdo con una realización de la invención que responda a personas que usan el software de herramientas en la instalación de simulación cibernética para montar y defenderse contra ciberataques en una instalación de infraestructura modelo de la instalación de simulación cibernética; y el procesamiento de datos en el registro forense para generar una estrategia de defensa para defender la instalación de infraestructura contra ciberataques.

En la descripción, a menos que se indique lo contrario, adjetivos tales como "sustancialmente" y "aproximadamente" que modifican una condición o relación característica de una característica o características de una realización de la invención, se entiende que significan que la condición o característica se define dentro de tolerancias que son aceptables para el funcionamiento de la realización para una aplicación para la que está destinada. A menos que se señale lo contrario, la palabra "o" en la descripción y en las reivindicaciones se considera como "o" inclusiva en lugar de o exclusiva, e indica al menos uno de, o cualquier combinación de artículos a los que se une.

Este Sumario se proporciona para introducir una selección de conceptos de una forma simplificada, que se describirán de manera más pormenorizada, más adelante, en la descripción detallada. Este sumario no tiene la intención de identificar características clave o características esenciales del objeto reclamado, ni está destinado a usarse en la limitación del ámbito del objeto reivindicado.

Breve descripción de las Figuras

A continuación se describen ejemplos no limitativos de realizaciones de la invención con referencia a las figuras adjuntas al presente documento que se enumeran a continuación de este párrafo. Las características idénticas que aparecen en más de una figura están por lo general etiquetadas con una misma etiqueta en todas las figuras en las que aparecen. Una etiqueta que etiqueta un icono que representa una característica dada de una realización de la invención en una figura puede usarse para hacer referencia a la característica dada. Las dimensiones de las características que se muestran en las figuras se eligen por conveniencia y claridad de presentación y no necesariamente se muestran a escala.

la Figura 1A muestra esquemáticamente una instalación de infraestructura que comprende una central eléctrica y una red de distribución de energía y una instalación de simulación correspondiente a la central eléctrica y a la red, de acuerdo con una realización de la invención; y

la Figura 1B muestra esquemáticamente una imagen ampliada de la central eléctrica y la red de distribución mostrada en la Figura 1A.

Descripción detallada

La Figura 1A muestra esquemáticamente una central 200 de energía real y una instalación 20 de simulación que comprende una instalación 22 modelo que modela la instalación real, de acuerdo con una realización de la invención. A modo de ejemplo, la central 200 de energía comprende una central 200 eléctrica conectada a una porción de una red 300 de energía que comprende cables 302 de transmisión eléctrica para suministrar energía eléctrica a clientes 304 industriales y domésticos. A modo de ejemplo, se supone que la central 200 eléctrica es una central eléctrica de combustión de carbón que comprende una configuración compleja de producción de energía y equipos de control mostrados esquemáticamente, o representados por iconos, en la Figura 1A. Los componentes de una central eléctrica de vapor son bien conocidos y solo algunos de los equipos que puede comprender una central eléctrica de combustión de carbón se muestran en la Figura y solo algunos de los equipos mostrados se describen explícitamente. La Figura 1B muestra esquemáticamente una imagen ampliada de la central 200 eléctrica en la que se ven más claramente los detalles estructurales de la central eléctrica.

La central 200 eléctrica comprende un complejo generador 202 de vapor que quema carbón suministrado por un sistema 240 de alimentación de carbón en un horno 204 para generar vapor para impulsar un sistema 260 de turbina. El sistema 260 de turbina hace girar un generador 270 electromecánico para producir energía eléctrica. La energía eléctrica a una tensión de salida del generador 270 electromecánico se transmite a un transformador 272 elevador que eleva la tensión de la energía a una alta tensión adecuada para su transmisión a los clientes 304 a través de la red 300 de distribución. Los transformadores reductores (no mostrados) convierten la energía eléctrica de alta tensión transmitida a través de los cables 302 de transmisión en energía a una tensión adecuada para su uso por clientes 304 domésticos e industriales.

El sistema 240 de alimentación de carbón puede comprender un transportador 242 de carbón que transporta carbón 244 a un pulverizador 246 que produce y entrega una mezcla de carbón pulverizado y aire al horno 204 en el que la mezcla se quema para producir calor para convertir el agua contenida en un tambor 206 de la caldera en vapor. La combustión de la mezcla de carbón y aire en el horno 204 está representada esquemáticamente por "llamas" 208. El vapor generado en el tambor 206 de la caldera circula al sistema 260 de turbina desde el complejo generador 202 de vapor a través de bobinas de intercambio de calor denominadas convencionalmente como "supercalentador" y "recalentador", etiquetadas con los números 210 y 211 en la Figura 1A.

El sistema 260 de turbina comprende por lo general una turbina 261 de alta presión, una turbina 262 de presión intermedia y una turbina 263 de baja presión. El vapor para impulsar la turbina 261 de alta presión circula desde el complejo generador 202 de vapor a través del supercalentador 210. El vapor que sale de la turbina 261 de alta presión se devuelve al complejo generador 202 de vapor en el que se recalienta en el horno 204 en el recalentador 211 y se suministra a la turbina 262 de presión intermedia después de pasar a través del recalentador. La turbina de presión intermedia que sale del vapor 262 se alimenta desde la turbina de presión intermedia para impulsar la turbina 263 de baja presión. El vapor que sale de la turbina 263 de baja presión se devuelve al tambor 206 de la caldera a través de un condensador 212 y una bobina de intercambio de calor 214 denominada "economizador". La refrigeración para el condensador 212 es proporcionada por una torre 216 de enfriamiento y los efluentes de la combustión del carbón en el horno 204 se liberan al aire como humo 218 a través de una chimenea 220 después de pasar a través de un precipitador 221 que elimina las partículas de los efluentes.

La operación de la planta 200 de energía y el control de los equipos en la planta de energía están mediados por un sistema SCADA representado esquemáticamente por un icono 250 de ordenador. Los datos, en lo sucesivo, también denominados datos de estado de operaciones, relevantes y/o indicativos del funcionamiento de los equipos en la planta 200 de energía y/o una red de comunicaciones que soporta la comunicación hacia y desde los equipos son adquiridos por sensores, que pueden denominarse "agentes recopiladores" acoplados directa o indirectamente a los equipos. Los agentes recopiladores transmiten los datos de estado de operaciones que adquieren a SCADA 250 para procesarlos para vigilar y controlar los equipos y las operaciones de la planta 200 de energía. En la Figura 1A, los agentes recopiladores están representados esquemáticamente por cajas 252 de llamada que tienen punteros que indican el equipo al que están acoplados respectivamente.

Cabe señalar que, mientras que los agentes recopiladores, tales como los agentes 252 recopiladores, no se muestran para la red 300 de distribución, los agentes recopiladores para controlar el funcionamiento de la red de distribución se distribuyen generalmente a través de una red de distribución para adquirir datos de estado de las operaciones que indican el estado de funcionamiento de los componentes de la red. Por ejemplo, se pueden usar agentes recopiladores para controlar las cargas de corriente y las temperaturas de los cables 302 de transmisión y las tensiones de entrada y salida de los transformadores reductores. Una red de distribución comprende o tiene también por lo general acceso a un sistema SCADA, que recibe los datos de estado de operaciones adquiridos por los agentes recopiladores para los parámetros relevantes para el funcionamiento de los componentes de la red y controla los componentes que responden a los datos recibidos. En la siguiente descripción se supone que la red 300 de distribución tiene acceso y está controlada por SCADA 250.

La instalación 20 de simulación comprende opcionalmente un modelo 30 físico de la central 200 eléctrica y un modelo 40 físico de la red 300 de distribución de acuerdo con una realización de la invención. El modelo 30 de la central eléctrica imita el funcionamiento de la central 200 eléctrica y está representado esquemáticamente por una imagen reducida de la central 200 eléctrica. De manera similar, el modelo 40 de la red de distribución imita el funcionamiento de la red 300 de distribución y, opcionalmente, los clientes 304, en lo sucesivo, también denominados colectivamente red 300 de distribución, y está representado esquemáticamente por una imagen reducida de la red 300 de distribución y los clientes 304.

El modelo 30 de la central eléctrica comprende equipos físicos y, opcionalmente, virtuales, indicados colectivamente en la Figura 1A con el número 31, que corresponden a los equipos físicos comprendidos en la central 200. El modelo 30 de la central eléctrica comprende también un sistema 32 SCADA que vigila y controla los equipos 31 de forma similar a la manera en que SCADA 250 controla y vigila los equipos en la central 200. Opcionalmente, el equipo 31 comprende agentes 33 recopiladores que corresponden a los agentes 252 recopiladores en la central 200 eléctrica y adquieren y proporcionan a SCADA 32 datos de estado de operaciones relevantes para vigilar y controlar el funcionamiento de los dispositivos en el equipo 31. Se observa que, si bien el modelo 30 de la central eléctrica está representada por una miniatura de la central 200 eléctrica, no necesariamente comprende entidades de equipos físicos y/o virtuales para cada parte del equipo comprendida en la central 200 eléctrica y puede modelar solo una parte de la central 200 eléctrica o una parte de las funciones realizadas por la planta 200 de energía.

El equipo 31 físico puede comprender un equipo idéntico al equipo correspondiente comprendido en la central 200 eléctrica, así como un equipo físico configurado para imitar el equipo correspondiente comprendido en la central 200 eléctrica que no es idéntico al equipo correspondiente. El equipo virtual comprende entidades construidas por software, que puede comprender equipos físicos configurados por el software, que imitan el equipo correspondiente comprendido en la central 200. Una entidad de equipo virtual dada que corresponde a una parte del equipo físico dada en la central 200 eléctrica opera sustancialmente como si fuera la entidad física correspondiente. La entidad de equipo virtual dada se comunica y coopera con otros equipos reales y/o virtuales en el modelo 30 de manera similar a la forma

en que el equipo correspondiente en la central 200 eléctrica se comunica y coopera con otros equipos en la central 200 eléctrica. Se puede acceder a la entidad de equipo virtual dada a través de SCADA 32 de forma similar a la manera en que SCADA 250 puede acceder a los equipos en la planta 200 de energía.

De forma similar al modelo 30 de la central eléctrica, que comprende equipos físicos y opcionalmente virtuales correspondientes a equipos comprendidos en la central 200, el modelo 40 de la red de distribución comprende equipos físicos y, opcionalmente, virtuales, que corresponden al equipo físico comprendido en la red 300 de distribución. Y, si bien el modelo 40 de la red de distribución está representado por una miniatura de la red 300 de distribución, no necesariamente comprende entidades de equipos físicos y/o virtuales para cada parte del equipo comprendida en la red 300 de distribución. El modelo de la red de distribución puede modelar solo una parte de la red 300 de distribución o una parte de las funciones realizadas por la red 300 de distribución. Opcionalmente, el modelo 40 de la red de distribución comprende agentes de recopilación (no mostrados) que corresponden a los agentes de recopilación (no mostrados) en la red 300 de distribución y proporcionan datos de estado de operaciones relevantes para el funcionamiento de los componentes del modelo 40 de la red de distribución para SCADA 32.

La instalación 20 de simulación comprende un ordenador o sistema informático centralizado o distribuido, en lo sucesivo, un controlador representado por un icono 50 de ordenador opcionalmente para configurar SCADA 32 y actualizar el funcionamiento de los modelos 30 y 40 en respuesta a los datos recibidos del funcionamiento real de la central 200 eléctrica y la red 300 de distribución. De acuerdo con una realización de la invención, los datos de la central 200 eléctrica se reciben a través de un canal 53 de comunicación unidireccional seguro que transmite datos desde la central 200 eléctrica y la red 300 de distribución, pero no transmite datos a la central eléctrica ni/o a la red de distribución. Los datos se transmiten entre el controlador 50 y los modelos 30 y/o 40 a través de un canal de comunicación o red representada por una flecha 55 de bloque con doble cabeza de flecha. En una realización de la invención, los datos generados o adquiridos por el controlador 50 pueden proporcionarse para su uso por la central 200 eléctrica y/o la red 300 de distribución mediante documentación escrita u otro canal de comunicación considerado suficientemente seguro contra el ciberataque. El suministro de datos mediante documentación escrita o un canal "suficientemente seguro" se representa esquemáticamente mediante una flecha 54 de bloque discontinua.

La instalación 20 de simulación está configurada para proporcionar agentes 61 de ataque de simulación y agentes 62 de defensa de simulación con acceso al modelo 30 de la central eléctrica y/o al modelo 40 de la red de distribución para participar en una "sesión de batalla cibernética". En la sesión de batalla cibernética, los agentes 61 de ataque de simulación intentan llevar a cabo ciberataques que dañan o deterioran el funcionamiento del modelo 30 de la central eléctrica y/o el modelo 40 de la red de distribución y luchan con agentes de defensa de simulación que operan para defender el modelo 30 y/o 40 atacado y frustran los ataques.

El controlador 50 comprende opcionalmente una memoria en la que almacena y gestiona datos en una base de datos CYBAD. El controlador 50 opera para adquirir y almacenar en CYBAD un registro forense de la sesión de batalla cibernética que puede procesarse como se describe a continuación para promulgar tecnologías de protección cibernética para proteger la central 200 eléctrica y/o la red 300 de distribución en respuesta a la sesión de batalla cibernética. Opcionalmente, el controlador 50 comprende un módulo creador de modelos que procesa datos en el registro forense para proporcionar tecnologías de protección cibernética. En una realización, las tecnologías de protección cibernética comprenden un clasificador para reconocer e identificar los ciberataques en el modelo 30 y/o modelo 40.

Proporcionar acceso para los agentes 61 de ataque de simulación al modelo 30 y/o modelo 40 puede comprender proporcionar a los agentes de ataque de simulación ordenadores, software y recursos financieros virtuales, en lo sucesivo, genéricamente denominados "software de herramientas de ataque", de varios niveles de sofisticación para montar ciberataques en la instalación modelo. El software de herramientas de ataque es opcionalmente similar al software de herramientas que podría estar disponible para los agentes de ataque de la vida real para emprender un ciberataque en la central 200.

Opcionalmente, la sofisticación del software herramientas de ataque se clasifica como baja, media o alta. La sofisticación de bajo nivel se refiere a software de herramientas de ataque generalmente disponibles para delincuentes de la "vida real" menos experimentados, hackers y hacktivistas, normalmente motivados por intereses personales. El software de herramientas de ataque de sofisticación de nivel medio se refiere a las herramientas generalmente disponible para hackers relativamente experimentados y expertos, que podría, por ejemplo, pertenecer a un grupo criminal o pequeño grupo terrorista, que tienen acceso a recursos financieros generalmente más allá de los recursos financieros disponibles para un solo individuo. La sofisticación de alto nivel se refiere al software herramientas disponible para los estados nacionales y grupos terroristas nacionales o internacionales.

Proporcionar a los agentes 62 de defensa de simulación acceso a los modelos 30 y 40 puede comprender proporcionar a los agentes de defensa de simulación ordenadores y software, en adelante, software de herramientas de gestión y operaciones (O&M), para acceder a SCADA 32, operar y mantener la instalación modelo, y defender la instalación modelo contra ciberataques montados por los agentes 61 de ataque de simulación. El software de herramientas de O&M refleja ventajosamente, al menos en parte, el software de herramientas de O&M empleadas para operar, vigilar y defender la central 200 eléctrica y la red 300 de distribución contra ciberataques.

En una realización de la invención, la instalación 20 de simulación comprende sensores de actividad humana representados por iconos 51. Los sensores 51 de actividad humana pueden usarse para vigilar la actividad de los agentes 61 de ataque y los agentes 62 de defensa en la batalla entre ellos e interactuar con la instalación 20 de simulación durante la sesión de batalla cibernética y adquirir datos para el registro forense de la sesión de batalla cibernética. El controlador 50 puede almacenar datos de actividad humana proporcionados por los sensores 51 en CYBAD como parte del registro forense de la sesión de batalla cibernética.

A modo de ejemplo, los sensores 51 pueden comprender opcionalmente cámaras de video que graban videos de actividad de agentes de defensa y ataque de simulación durante la sesión de batalla cibernética. Los sensores 51 pueden comprender cualquiera de varios sensores HMI tales como sensores y dispositivos de registro de pulsaciones de teclas para el siguiente uso de teclados por los agentes 61 y 62 de simulación de ataque y defensa para activar e implementar conjuntos de instrucciones de software para montar o defenderse contra ciberataques. Los dispositivos de registro de pulsaciones de teclas conocidos en la técnica para el registro de pulsaciones de teclas del uso del teclado del agente de simulación de acuerdo con una realización de la invención pueden comprender sensores de pulsación de teclas acústicos y/o electromagnéticos o programas de seguimiento de pulsaciones de teclas instalados en ordenadores usadas por los agentes 61 y 62. Opcionalmente, los sensores 51 comprenden tecnología de seguimiento ocular para seguir las direcciones de observación de los agentes 61 y 62 de simulación y determinar sus puntos de vista (POR) y el movimiento del POR entre las características de las pantallas de computadora con las que interactúan los agentes de simulación.

En una realización de la invención, los sensores 51 comprenden, cualquiera de los diversos sensores de función corporal ponibles y/o sin contacto para controlar las características fisiológicas de los agentes de simulación para proporcionar indicaciones, por ejemplo, de niveles de preocupación, estrés y/o estado de alerta durante una batalla cibernética. A modo de ejemplo, un sensor de función corporal ponible puede ser un brazalete sensor para detectar la frecuencia cardíaca y/o la presión arterial. Un sensor sin contacto puede comprender un sensor óptico para detectar el color de la piel para inferir el estrés o la frecuencia cardíaca o un sensor IR para detectar la temperatura corporal.

En una realización de la invención, el controlador 50 supervisa los agentes 33 recopiladores comprendidos en el equipo 31, ya sea directamente o mediante SCADA 32, para vigilar el funcionamiento de equipos individuales reales o virtuales en el modelo 30 de la central eléctrica durante la batalla cibernética y adquirir datos de estado de las operaciones del equipo durante la batalla cibernética. Los datos de estado de operaciones pueden almacenarse como parte del registro forense de la batalla cibernética en CYBAD.

En una realización de la invención, el módulo creador de modelos comprendido en el controlador 50 procesa datos de estado de operaciones en CYBAD para definir y determinar un vector de estado de operaciones dependiente del tiempo para el modelo 30 que representa un estado operativo del módulo 30 de la central eléctrica en momentos determinados durante la sesión de batalla cibernética. Un vector de estado de operaciones para el modelo 30 puede tener componentes que asuman en cualquier momento dado valores proporcionados por cada uno de una pluralidad de agentes 33 recopiladores comprendidos en el modelo 30 en el momento dado. Opcionalmente, un vector de estado de operaciones comprende datos proporcionados por sensores 51 de actividad humana que pueden proporcionar, por ejemplo, datos que indican el uso y/o el estado de equipos HMI tales como teclados de ordenador.

Opcionalmente, el módulo creador de modelos define al menos un clasificador que responde a los vectores de estado para la sesión de batalla cibernética para determinar si un vector de estado en un momento dado durante la batalla cibernética indica que el modelo 30 se encuentra bajo un ciberataque montado por agentes de ataque simulador 61. Opcionalmente, el al menos un clasificador comprende un clasificador de vectores de soporte. En una realización de la invención, el al menos un clasificador comprende una red neuronal que está entrenada en vectores de estado de operaciones almacenados en CYBAD. Opcionalmente, el controlador 50 mantiene una biblioteca de vectores de estado de operaciones representativos, en lo sucesivo denominados vectores característicos de ID de ataque, que el al menos un clasificador ha determinado indica ciberataques y puede usarse para identificar formas particulares de ciberataques. En una realización de la invención, los al menos un clasificador y/o vectores característicos de ID de ataque se utilizan para determinar si un vector de estado de operaciones definido por SCADA 250 para la central 200 eléctrica y/o la red 300 de distribución indica que la central 200 eléctrica y/o la red de distribución están bajo ciberataque y opcionalmente para determinar una forma del ataque.

En una realización de la invención, el módulo creador de modelos procesa datos en CYBAD para determinar qué estrategias de defensa emprendidas por los agentes 62 de defensa de simulación contra los ciberataques montados por los agentes 61 de ataque de simulación tienen éxito en evitar los ciberataques o mitigar el daño que incurren. Opcionalmente, el módulo creador de modelos proporciona un mapa y una secuencia de procedimientos realizados en una estrategia de defensa exitosa. En una realización de la invención, el módulo creador de modelos define vectores característicos, en adelante, vectores característicos de ID de defensa, para estrategias de defensa exitosas que etiqueten y caractericen las estrategias de defensa. Opcionalmente, el modelo del creador de modelos configura los vectores característicos de la estrategia de defensa para que los productos escalares (punto) de los vectores característicos de ID de defensa con los vectores característicos de ID de ataque puedan usarse para indicar qué estrategias de defensa se realizan ventajosamente para frustrar un ciberataque dado.

En una realización de la invención, los vectores característicos de ID de defensa se utilizan para determinar estrategias

de defensa ventajosas que se llevarán a cabo para defender la central 200 eléctrica y/o la red 300 de distribución contra ciberataques. Cuando un vector de estado de operaciones para la central 200 eléctrica y/o la red 300 de distribución indica que la central eléctrica y/o la red eléctrica pueden estar bajo un ciberataque, se calculan los productos escalares del vector de estado de operaciones y los vectores característicos de ID de defensa. Un vector de función de ID de defensa que tiene un producto escalar más grande con el vector de estado de operaciones se usa opcionalmente para evitar o minimizar el daño del posible ciberataque.

Los datos de actividad humana adquiridos por los sensores 51 y almacenados en CBAD como parte del registro forense de la sesión de batalla cibernética pueden usarse para configurar entornos en los que los agentes 62 de defensa operan para mejorar su capacidad de defensa contra ciberataques. Por ejemplo, los datos se pueden usar para configurar pantallas en la pantalla de video de la computadora para mejorar la efectividad de las alertas visuales presentadas en la pantalla de video para alarmar a los agentes de defensa ante la probabilidad de un ciberataque. Los datos de actividad humana pueden usarse para mejorar las indicaciones a los agentes de defensa para que realicen actividades apropiadas para frustrar un ciberataque. Los datos de la actividad humana también se pueden usar para configurar ventajosamente la configuración espacial de los agentes de defensa para mejorar la cooperación entre los agentes de defensa que pueden ser necesarios para unirse a una tarea de defensa común.

Se observa que, mientras que en la descripción anterior de las realizaciones de la invención, se describe una instalación de simulación cibernética configurada para una central eléctrica y una red de energía, La práctica de la invención no se limita a centrales eléctricas y redes eléctricas. Una instalación de simulación cibernética puede configurarse para su uso en el desarrollo y análisis de estrategias de defensa y/o ciberataque para cualquiera de las diversas instalaciones de infraestructura, como a modo de ejemplo, plantas de tratamiento de agua, sistemas de distribución de petróleo y sistemas de distribución de gasoductos.

En la descripción y reivindicaciones de la presente solicitud, cada uno de los verbos, "comprende", "incluye" y "tiene", y sus conjugados, se usan para indicar que el objeto u objetos del verbo no son necesariamente una lista completa de componentes, elementos o partes del sujeto o sujetos del verbo,

Las descripciones de realizaciones de la invención en la presente solicitud se proporcionan a modo de ejemplo y no pretenden limitar el ámbito de la invención. Las realizaciones descritas comprenden diferentes características, no todas se requieren en todas las realizaciones de la invención. Algunas realizaciones utilizan solo algunas de las características o posibles combinaciones de las características. Las variaciones de las realizaciones de la invención que se describen, y las realizaciones de la invención que comprenden diferentes combinaciones de características observadas en las realizaciones descritas, ocurrirá a personas de la técnica. El ámbito de la invención está limitado solo por las reivindicaciones.

REIVINDICACIONES

1. Una instalación (20) de simulación que comprende:

una instalación (30, 40) modelo operativa de una instalación (200, 300) de infraestructura real que imita al menos en parte las operaciones de la instalación de infraestructura real y comprende equipos que corresponden e imitan las operaciones de equipo en la instalación de infraestructura real;

software de herramientas de ataque para su uso por un primer equipo de personas (61) en el montaje de ciberataques en la instalación (30) modelo;
software de herramientas de gestión y operaciones para su uso por un segundo equipo de personas (62) en el funcionamiento de la instalación modelo y en la defensa de la instalación modelo contra los ciberataques montados por el primer equipo de personas que utilizan el software de herramientas de ataque; y

un controlador (50) que tiene memoria y es operable para adquirir y almacenar en la memoria un registro forense de ciberataques montado por el primer equipo de personas en la instalación modelo y estrategias de defensa emprendidas por el segundo equipo de personas para defender la instalación modelo contra los ciberataques, en la que el registro forense comprende datos indicativos de al menos uno de la actividad humana del segundo equipo y características fisiológicas del segundo equipo.

2. La instalación de simulación de acuerdo con la reivindicación 1, en la que el equipo en la instalación modelo comprende equipo físico que no está conectado a la instalación de infraestructura real.

3. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 1 o 2 en la que los equipos en la instalación modelo comprende equipo (31) virtual.

4. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 1 a 3 y que comprende agentes recopiladores (33) que no están acoplados a la instalación de infraestructura real que adquiere datos de estado de operaciones relevantes o indicativos del funcionamiento del equipo en la instalación modelo.

5. La instalación de simulación de acuerdo con la reivindicación 4, en la que el controlador recibe los datos de estado de operaciones y almacena los datos de estado de operaciones en la memoria como parte del registro forense.

6. La instalación de simulación de acuerdo con la reivindicación 5 y que comprende un módulo creador de modelos que procesa datos en el registro forense para generar vectores de estado de operaciones que comprenden componentes que tienen valores que responden a los datos de estado de operaciones proporcionados por cada uno de una pluralidad de agentes recopiladores.

7. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en la que los datos del registro forense indicativos de al menos uno de la actividad humana del segundo equipo y las características fisiológicas del segundo equipo comprenden datos adquiridos por al menos un sensor (51) de actividad humana que adquiere datos indicativos de actividad de personas en el segundo equipo seleccionado de: una cámara de vídeo configurada para grabar vídeos de actividad de personas en la instalación; un sensor de interfaz hombre máquina (HMI); un rastreador de miradas; un sensor portátil para vigilar las características fisiológicas; o un sensor sin contacto para vigilar las características fisiológicas.

8. La instalación de simulación de acuerdo con la reivindicación 7, en la que el controlador recibe los datos adquiridos por los sensores de actividad humana y almacena los datos recibidos en la memoria como parte del registro forense.

9. La instalación de simulación de acuerdo con la reivindicación 8 y que comprende un módulo creador de modelos que procesa datos en el registro forense para generar vectores de estado de operaciones que comprenden componentes que tienen valores que responden a los datos proporcionados por cada uno de una pluralidad de sensores de actividad humana.

10. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 6 y 9, en la que el módulo creador de modelos define al menos un clasificador que responde a los vectores de estado de operaciones para determinar si un vector de estado de operaciones en un momento dado indica que la instalación modelo se encuentra bajo un ciberataque.

11. La instalación de simulación de acuerdo con la reivindicación 10, en la que el al menos un clasificador comprende un clasificador de vectores de soporte.

12. La instalación de simulación de acuerdo con la reivindicación 10, en la que el al menos un clasificador comprende una red neuronal.

13. La instalación de simulación de acuerdo con cualquiera de las reivindicaciones 1-12, en la que la instalación de infraestructura real está configurada para usar el registro forense para defender la instalación de infraestructura real contra ciberataques.

14. La instalación de simulación de acuerdo con la reivindicación 10, en la que la instalación de infraestructura real está configurada para usar al menos un clasificador para determinar si la instalación de infraestructura real se encuentra bajo un ciberataque.

15. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones anteriores, en la que la instalación de infraestructura real comprende al menos una de una central (200) eléctrica, plantas de tratamiento de agua, sistemas de distribución de oleoductos y gasoductos.

16. Un procedimiento para desarrollar una estrategia para defender una de una instalación modelo y una instalación (30, 40, 200, 300) real contra un ciberataque, comprendiendo el procedimiento:

adquirir en un controlador (50) un registro forense proporcionado por una instalación (20) de simulación de acuerdo con cualquiera de las reivindicaciones 1-15 en respuesta a personas del primer equipo que utilizan el software de herramientas en la instalación de simulación para montar ciberataques en la instalación modelo y personas del segundo equipo que utilizan el software de herramientas en la instalación de simulación para defenderse de los ciberataques en la instalación (30, 40) modelo y para mantener el funcionamiento de la instalación de simulación; en el que el registro forense comprende datos indicativos de al menos uno de la actividad humana del segundo equipo y características fisiológicas del segundo equipo; y
procesar por el controlador (50) los datos en el registro forense para generar una estrategia de defensa para su uso por personas del segundo equipo para defender la de una instalación modelo y una instalación real contra ciberataques.

17. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 1-15, en la que el software de herramientas de ataque y el software de herramientas de operaciones y administración son para su uso por el primer equipo de personas y el segundo equipo de personas para competir entre sí, y el registro forense comprende datos indicativos de una competencia entre el primer equipo de personas y el segundo equipo de personas.

18. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 1-15, en la que el software herramientas de ataque incluye recursos financieros virtuales.

19. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 1-15, en la que el software herramientas de ataque tiene al menos dos niveles de sofisticación, correspondiente a diferentes tipos de agentes de ataque de la vida real.

20. La instalación de simulación de acuerdo con una cualquiera de las reivindicaciones 1-15, en la que los datos indicativos de al menos uno de la actividad humana del segundo equipo y las características fisiológicas del segundo equipo se utilizan para configurar entornos que mejoran la capacidad de las personas para defenderse de los ciberataques.

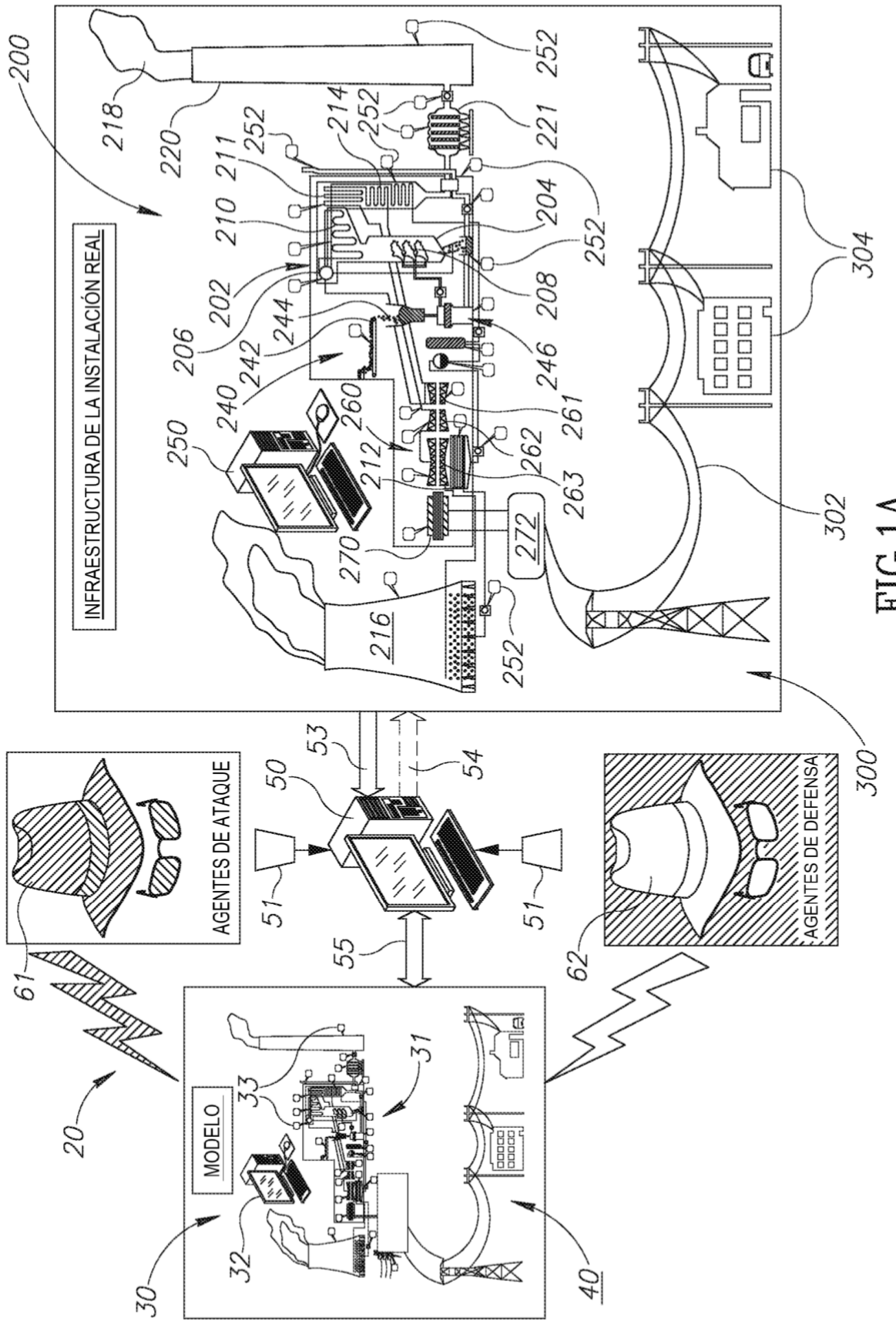
INFRAESTRUCTURA DE LA INSTALACIÓN REAL
AGENTES DE ATAQUE
AGENTES DE DEFENSA
MODELO
200
300
20
30
40
50
51
53
54
55
61
62
202
204
206
208
210
211
212
214
216
218
220
221
240
242
244
246
250
252
260
261
262
263
270
272
302
304
31
32
33

FIG.1A

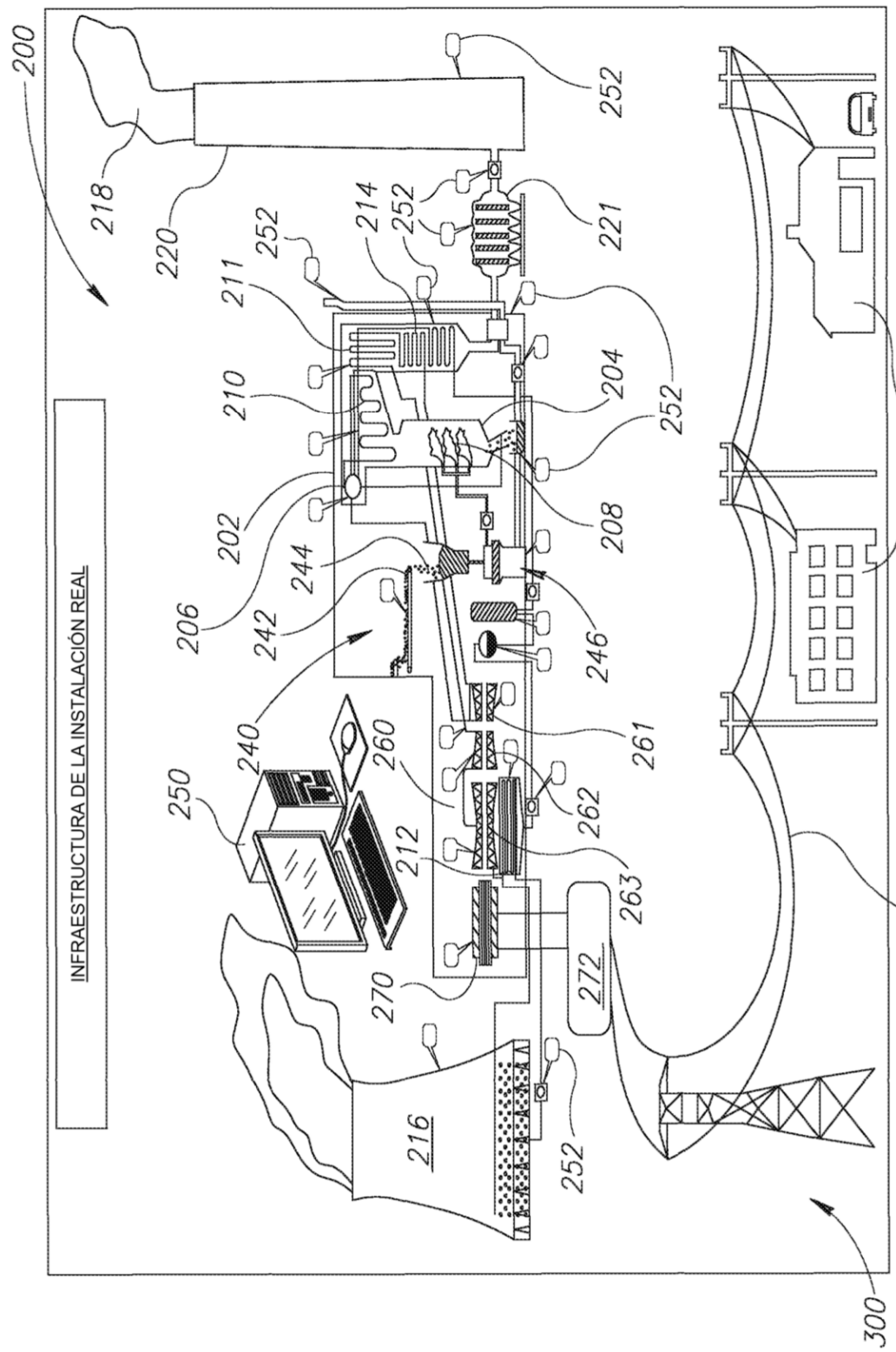
INFRAESTRUCTURA DE LA INSTALACIÓN REAL
200
218
220
252
214
211
210
204
202
206
244
242
240
208
246
261
260
262
250
212
263
270
272
216
304
302
300

FIG.1B