

CREACIÓN DE DATOS SEGUROS EN UNA CADENA DE SUMINISTRO DE
PETRÓLEO Y GAS

CAMPO DE LA INVENCION

5 La presente invención se relaciona de manera general con un sistema y un método para crear datos seguros y confiables en una cadena de suministro de gas y petróleo.

ANTECEDENTES DE LA INVENCION

La administración de la cadena de suministro es
10 un problema difícil para organizaciones que regularmente realizan negocios en el transporte de un gran número de productos sobre un área geográfica grande. La capacidad para seguir y rastrear productos, artículos o activos sobre una cadena de suministro es suficientemente difícil, mucho
15 menos que las presiones agregadas para determinar o validar si un producto, artículos o activos específicos son falsificados, limpiados o adulterados. Actualmente, existen sistemas en los cuales los productos, artículos o activos pueden ser recolectados y distribuidos en los cuales la
20 información de localización y estado con respecto al movimiento de los productos, artículos o activos es verificada a través de la cadena de suministro.

La industria del petróleo y gas se divide típicamente en tres sectores: upstream, midstream y
25 downstream como se ilustra en la Figura 2. La industria del

petróleo y gas se divide típicamente en tres sectores, upstream, midstream y downstream. El sector upstream se conoce como el sector de exploración y producción. El sector upstream incluye la búsqueda y exploración de campos de petróleo crudo y gas natural subterráneos y subacuáticos potenciales (por ejemplo identificación de reservas de hidrocarburos potenciales), la perforación de pozos exploratorios, y la perforación y terminación posterior de los pozos que recuperan y llevan (producen) el petróleo crudo y/o gas natural a la superficie. El sector midstream implica el transporte (por tubería, ferrocarril, camión, etc.), almacenamiento y comercialización al mayoreo de productos de petróleo crudo o refinado. Las tuberías y otros numerosos sistemas de transporte pueden ser usados para mover petróleo crudo de los sitios de producción a las refinerías y entregar los diferentes productos refinados a los distribuidores del sector downstream. El sector downstream se refiere a la refinación del petróleo crudo y el procesamiento y purificación de gas natural crudo, así como la comercialización y distribución de productos derivados de petróleo crudo y gas natural. El sector downstream proporciona a los consumidores productos como gasolina o petróleo, queroseno, combustible para propulsión a chorro, gasóleo, calefacción, petróleo, lubricantes, ceras, asfalto, gas natural y gas de petróleo licuado así como cientos de petroquímicos.

En años recientes, ha habido un incremento mayor de actividades ilegales relacionadas con los activos de petróleo y gas. Por ejemplo, el número de robos de petróleo y gas en áreas como Texas y México se ha incrementado casi diez veces en los pasados diez años. La corrupción, robo, falsificación, hurto y otras actividades ilegales ocurren a lo largo de todas las fases y sectores de la cadena de suministro, incluyendo los sectores upstream, midstream y downstream. Las derivaciones de tuberías, desviación de petróleo crudo, secuestro de camiones, túneles subterráneos y hurto de petróleo en refinerías son sólo unos cuantos ejemplos de los tipos de actividades ilegales que se han vuelto muy prevalecientes dentro de la industria. Con este aumento en la actividad, existen varios desafíos enfrentados por la industria de petróleo y gas. Por ejemplo, los eventos que ocurren no siempre están relacionados entre sí geográficamente o de otro modo, proporcionan una cadena de eventos o incidentes fragmentados. Actualmente, existen muchas soluciones y tecnologías diferentes para ayudar a la administración, pero no son sistemas homogéneos o compatibles. Una falta de comunicación y transparencia coordinada entre regiones, funciones y equipos proporciona varios desafíos, y una falta de capacidad de registro y seguimiento de los eventos vislumbra la capacidad de contabilidad. De este modo, se

vuelve difícil de responder a tales eventos e incidentes de manera oportuna, sino es que del todo.

Por lo tanto, existe la necesidad de proporcionar un sistema de administración inteligente que pueda resolver

5 la necesidad de verificar y reportar o alertar actividades ilegales sobre activos de petróleo y gas que al mismo tiempo incremente la confiabilidad, seguridad, cumplimiento regulatorio y responsabilidad ambiental. Adicionalmente, existe la necesidad de un sistema que verifique de manera

10 remota y analice de manera prescriptiva y predictiva eventos de los activos que ocurran en los sectores upstream, midstream y downstream verificando, prediciendo y proporcionando datos como una alerta para permitir la toma de decisiones desde cualquier lugar. Adicionalmente, existe

15 la necesidad de asegurar datos derivados de productos o artículos o detectores, que sean confiables y seguros y sean usados de manera eficiente para proteger los artículos o productos en la cadena de suministro de petróleo y gas. Adicionalmente, existe la necesidad de un sistema que

20 permita la edición de datos seguros, exactos y confiables de los sectores upstream, midstream y downstream que permita una recolección eficiente de los impuestos a lo largo de la cadena de suministro, y que permita a nivel de estado recuperar correctamente la cantidad de impuestos que

25 deberán ser pagados por los actores implicados en la cadena

de suministro de petróleo y gas. El término activo, como se define aquí, incluye todos los productos e infraestructura de petróleo y gas.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

5 La presente descripción, a través de uno o más de sus diferentes aspectos, modalidades y/o características o subcomponentes específicos, proporcionan varios sistemas, servidores, métodos, medios y programas para interconectar códigos recopilados, como,
10 por ejemplo, algoritmos de java o extracción de datos o mezcla de elementos de hardware y software para generar datos con atributos adicionales útiles en el sistema de administración global (GMS) o en un sistema de administración de integridad (IMS) relacionados con la
15 administración de activos de petróleo y gas.

 En una modalidad, existe un sistema para crear datos seguros relacionados con activos de petróleo y gas mientras atraviesan una cadena de suministro, incluyendo al menos un sistema de depósito el cual recolecta datos
20 seguros generados mediante la captura de información usando un dispositivo observador seguro, y envía los datos seguros a una puerta de enlace y/o módulo de integración de datos el cual es parte de un sistema de administración global o un sistema de administración de
25 integridad para crear eventos agrupados.

En otra modalidad, existe un método para crear datos seguros relacionados con activos de petróleo y gas mientras atraviesan una cadena de suministro, que incluye recolectar datos seguros, en al menos un sistema de depósito, generados mediante la captura de información usando un dispositivo observador seguro, y enviando los datos seguros a una puerta de enlace, y/o módulo de integración de datos que es parte de un sistema de administración global o un sistema de administración de integridad.

En otra modalidad más existe un medio legible por computadora no transitorio que almacena un programa para crear datos seguros relacionados con activos de petróleo y gas mientras atraviesan una cadena de suministro de gas, el programa cuando es ejecutado por un procesador, incluye la recolección de dato seguros, en al menos un sistema de depósito, generados mediante una captura de información usando un dispositivo observador seguro, y enviando los datos seguros a una puerta de enlace y/o módulo de integración de datos el cual es parte de un sistema de administración global o un sistema de administración de integridad para crear eventos agrupados o un reporte de impuesto seguro y confiable o KPI útil para la recuperación de impuestos, reconciliación de impuestos, corregir asimetrías proporcionados desde diferentes entidades a lo

largo de la cadena de suministro de petróleo y gas.

En un aspecto, existe una plataforma de administración de eventos para obtener visibilidad de la cadena de suministro usando los datos seguros recolectados para identificar al menos una de la manipulación indebida, desviación, adulteración, falsificación, fraude y fraude tributario de un producto en la cadena de suministro.

En otro aspecto, el sistema de depósito se comunica con la plataforma de administración de evento vía una red e incluye una pluralidad de dispositivos de almacenamiento accesibles que fueron distribuidos a través del sistema.

En otro aspecto más, un dispositivo observador estándar es configurado para capturar información estándar de un producto de un primer identificador de producto, formando por lo tanto una información capturada de datos estándar, y el dispositivo observador seguro es configurado para capturar la información estándar del producto del primer identificador de producto e información segura de un marcado, tomando por lo tanto la información capturada y los datos seguros.

En otro aspecto más, el marcado incluye una composición que tiene compuestos con propiedades luminiscentes en el intervalo de al menos una de UV, IR e IR cercano y mezclas de las mismas que pueden estar presentes como una clave química.

En otro aspecto, el primer identificador de producto está vinculado al autenticador.

En otro aspecto, cuando el dispositivo observador seguro captura la información estándar y la información
5 segura, los datos seguros son enviados al sistema de depósito, y cuando el dispositivo observador estándar captura la información estándar, los datos estándar son enviados al sistema de depósito.

En otro aspecto, el producto es uno de gasolina o
10 petróleo, queroseno, combustible para propulsión a chorro, gasóleo, calefacción, petróleo, lubricantes, ceras, asfalto, gas natural, gas de petróleo licuado y petroquímicos.

En otro aspecto más, el sistema de depósito
15 almacena los datos estándar vinculados con el producto durante un ciclo de vida del producto en la cadena de suministro, los datos estándar en forma de datos representativos del primer identificador de producto.

En un aspecto, el dispositivo observador estándar
20 y seguro es al menos un detector proporcionado a lo largo de la cadena de suministro para capturar información segura.

En otro aspecto más, el detector detecta datos
incluyendo o relacionados con al menos una de la
25 temperatura, densidad, humedad, medidor de volumen,

gravedad, composición química, presión, peso, variación de presión de una tubería, diferencia de peso de un vehículo o volumen de combustible, localización GPS, sincronización de la ubicación de un vehículo, región geográfica, velocidad de flujo, conductividad, reología, turbidez, formación de imágenes, formación de imágenes térmicas, estado del detector, medidores de tensión, datos relacionados en el estado del tiempo, tráfico, condiciones del vehículo o carretera, velocidad del viento, condiciones barométricas, lluvia, datos de mantenimiento o fecha de mantenimiento, información de posición personal, datos de FR, datos acústicos, viscosidad y posición GPS.

En otro aspecto más, el sistema de depósito almacena los datos estándar y los datos seguros que son vinculados al producto durante el ciclo de vida del artículo en la cadena de suministro, los datos estándar en forma de datos representativos del primer identificador de producto y los datos seguros en forma de datos representativos del marcado.

En otro aspecto más, los datos estándar y los datos seguros son capturados simultáneamente por el dispositivo observador seguro.

En otro aspecto, el producto es marcado con el primer identificador de producto y el marcado.

En otro aspecto más, la información capturada por

el dispositivo observador seguro es de detectores en al menos una de las tuberías a lo largo de la cadena de suministro de petróleo y gas, un producto químico que marca el producto, y unido a una bomba en una estación de gas que
5 distribuye el producto.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La presente invención es descrita además en la descripción detallada siguiente, con referencia a la pluralidad de Figuras denotadas, por medio de ejemplos no
10 limitantes de las modalidades preferidas de la presente invención, en las cuales caracteres similares representan elementos similares a través de las diferentes vistas de las Figuras.

La Figura 1 es un sistema ejemplar para usarse de
15 acuerdo con las modalidades descritas aquí.

La Figura 2 es una cadena de suministro ejemplar para usarse en la industria de petróleo y gas.

La Figura 3 es otro diagrama ejemplar de un sistema de administración de integridad de acuerdo con una
20 modalidad de la descripción.

La Figura 4 un ejemplo de red de cadena de suministro de acuerdo con una modalidad de la descripción.

La Figura 5 es un diagrama ejemplar de un sistema de administración de integridad que se interconecta con una
25 plataforma de recuperación de impuestos especiales a través

de una interfaz de plataforma de impuestos especiales de acuerdo con una modalidad de la descripción.

Las Figuras 6A y 6B ilustran diagramas de flujo ejemplares de codificación y marcación de un objeto y de
5 seguimiento y autenticación de eventos de acuerdo con el sistema.

La Figura 7 ilustra un diagrama de bloques ejemplar de la generación de un evento seguro de acuerdo con el sistema.

10 La Figura 8 ilustra un depósito global ejemplar de acuerdo con el sistema.

La Figura 9 es un diagrama ejemplar de un sistema de administración global de acuerdo con una modalidad de la descripción.

15 La Figura 10 ilustra un diagrama ejemplar de una interfaz de acuerdo con una modalidad de la descripción.

Las Figuras 11A a 11D muestran una secuencia ejemplar de eventos en los cuales los datos capturados
20 ocurren con el tiempo para determinar una probabilidad.

La Figura 12 es un diagrama ejemplar de una interfaz de acuerdo con una modalidad de la descripción.

La Figura 13 es una modalidad ejemplar de un flujo de proceso de la interfaz de acuerdo con una
25 modalidad de la descripción.

DESCRIPCIÓN DETALLADA DE LA INVENCION

La presente descripción, a través de uno o más de sus diferentes aspectos, modalidades y/o características o subcomponentes específicas, de este modo pretende llevar a
5 cabo una o más de las ventajas como se hace notar específicamente más adelante.

La Figura 1 es un sistema ejemplar para usarse de acuerdo con las modalidades descritas aquí. El sistema 100 es mostrado de manera general y puede incluir un sistema de
10 computadora 102, el cual es indicado de manera general. El sistema de computadora 102 puede operar como un dispositivo independiente o puede ser conectado a otros sistemas o dispositivos periféricos. Por ejemplo, el sistema de computadora 102 puede incluir, o ser incluido dentro de,
15 cualquiera de una o más computadoras, servidores, sistemas, redes de comunicación o ambiente de nube.

El sistema de computadora 102 puede operar con la capacidad de un servidor en un ambiente de red, o en la capacidad de una computadora de usuario cliente en el
20 ambiente de red. El sistema de computadora 102, o porciones del mismo, puede ser implementado como, o incorporado en, varios dispositivos, como una computadora personal, una computadora tipo tableta, un decodificador o receptor de señales, un asistente digital personal, un dispositivo
25 móvil, una computadora de mano, una computadora portátil,

una computadora de escritorio, un dispositivo de comunicaciones, un teléfono inalámbrico, un dispositivo de confianza personal, un aparato de red, o cualquier otra máquina capaz de ejecutar un conjunto de instrucciones (secuenciales o de otro modo) que especifique acciones que deban ser realizadas por ese dispositivo. Además, aunque es ilustrado un solo sistema de computadora 102, las modalidades adicionales pueden incluir cualquier colección de sistemas o subsistemas que individual o conjuntamente ejecuten instrucciones o realicen funciones.

Como se ilustra en la Figura 1, el sistema de computadora 102 puede incluir al menos un procesador 104, como, por ejemplo, una unidad de procesamiento central, una unidad de procesamiento de gráficos, o ambas. El sistema de computadora 102 también puede incluir una memoria de computadora 106. La memoria de computadora 106 puede incluir una memoria estática, una memoria dinámica, o ambas. La memoria de computadora 106 puede de manera adicional o alternativa incluir un disco duro, memoria de acceso aleatorio, o memoria caché, o cualquier combinación de las mismas. Por supuesto, aquellos expertos en la técnica apreciarán que la memoria de computadora 106 puede comprender cualquier combinación de memorias conocidas o un solo almacén.

Como se muestra en la Figura 1, el sistema de computadora 102 puede incluir un dispositivo de visualización de computadora 108, como una pantalla de cristal líquido, un diodo emisor de luz orgánico, un
5 dispositivo de visualización de panel plano, un dispositivo de visualización en estado sólido, un tubo de rayos catódicos, un dispositivo de visualización de plasma, o cualquier otro dispositivo de visualización conocido.

El sistema de computadora 102 puede incluir al
10 menos un dispositivo de entrada de computadora 110, como un teclado, un dispositivo de control remoto que tenga un teclado numérico inalámbrico, un micrófono acoplado a un motor de reconocimiento de voz, una cámara como una cámara de video o cámara estática, un dispositivo de control de
15 cursor, o cualquier combinación de los mismos. Aquellos expertos en la técnica apreciarán que las diferentes modalidades del sistema de computadora 102 pueden incluir dispositivos de entrada múltiples 110. Además, aquellos expertos en la técnica apreciarán además que los
20 dispositivos de entrada ejemplares 110 ilustrados anteriormente no significa que sean exhaustivos y que el sistema de computadora 102 pueda incluir cualquier dispositivo de entrada adicional, o alternativo, 110.

El sistema de computadora 102 también puede
25 incluir un lector de medio 112 y una interfaz o

interconexión de red 114. Además, el sistema de computadora 102 puede incluir cualquier dispositivo, componentes, partes, dispositivos periféricos, hardware, software o cualquier combinación adicional de los mismos que sean comúnmente conocidos y comprendidos incluidos con o dentro de un sistema de computadora, como, pero sin limitarse a, un dispositivo de salida 116. El dispositivo de salida 116 puede ser, pero no se limita a, un altavoz, una salida de audio, una salida de video, una salida de control remoto, o cualquier combinación de los mismos.

Cada uno de los componentes del sistema de computadora 102 puede ser interconectado y comunicarse vía un bus o canal 118. Como se muestra en la Figura 1, los componentes pueden ser cada uno interconectados y comunicarse vía un bus o canal interno. Sin embargo, aquellos expertos en la técnica apreciarán que cualquiera de los componentes también puede ser conectado vía un bus o canal de expansión. Además, el bus o canal 118 puede permitir la comunicación vía cualquier estándar u otra especificación comúnmente conocida y comprendida como, pero sin limitarse a, una interconexión de un componente periférico, una interconexión expreso de un componente periférico, conexión de tecnología avanzada en paralelo, conexión de tecnología avanzada en serie, etc.

El sistema de computadora 102 puede estar en

comunicación con uno o más dispositivos de computadora adicionales 120 vía una red 122. La red 122 puede ser, pero no se limita a, una red de área local, una red de área ancha, Internet, una red de telefonía, o cualquier otra red
5 comúnmente conocida y comprendida en la técnica. La red 122 es mostrada en la Figura 2 como una red inalámbrica. Sin embargo, aquellos expertos en la técnica apreciarán que la red 122 también puede ser una red alámbrica.

El dispositivo de computadora adicional 120 es
10 mostrado en la Figura 1 como una computadora personal. Sin embargo, los expertos en la técnica apreciarán que, en modalidades alternativas de la presente solicitud, el dispositivo 120 puede ser una computadora portátil, una computadora personal tipo tableta, un asistente digital
15 personal, un dispositivo móvil, una computadora de mano, una computadora de escritorio, un dispositivo de comunicaciones, un teléfono inalámbrico, un dispositivo confiable personal, un aparato de red, o cualquier dispositivo que sea capaz de ejecutar un conjunto de
20 instrucciones, secuenciales o de otro tipo, que especifique acciones que deban ser realizadas por ese dispositivo. Por supuesto, aquellos expertos en la técnica apreciarán que los dispositivos listados anteriormente son meramente dispositivos ejemplares y que el dispositivo 120 puede ser
25 cualquier dispositivo o aparato adicional comúnmente

conocido y comprendido en la técnica sin apartarse del alcance de la presente solicitud. Además, aquellos expertos en la técnica igualmente comprenden que el dispositivo puede ser cualquier combinación de dispositivos y aparatos.

5 Por supuesto, aquellos expertos en la técnica apreciarán que los componentes listados anteriormente del sistema de computadora 102 simplemente son ejemplares y no pretenden ser exhaustivos y/o incluyentes. Además, los ejemplos de los componentes listados anteriormente son
10 ejemplares e igualmente no pretenden ser exhaustivos y/o incluyentes.

La Figura 4 ilustra una red de cadena de suministro ejemplar. El sistema 500 incluye, por ejemplo, upstream 508, midstream 510, downstream 514, un depósito,
15 una interfaz 516 y servicios de descubrimiento 502, 504 y 506 sobre los cuales diferentes componentes de un sistema 500 se comunican a través de una red 520, como Internet. Los servicios de descubrimiento 502, 504 y 506 incluyen una
20 base de datos (e interfaces) para promover el intercambio de datos ofreciendo un servicio que vincule información acerca de productos y activos (por ejemplo petróleo y combustible) a medida que se mueven por ejemplo, a través de una cadena de suministro de upstream 508, a midstream 510, a downstream 514. Cuando un producto pasa a través de
25 los canales de suministro y es registrado por los

dispositivos de captura de datos en cada uno de los sectores 508, 510, y 514 (como se describió anteriormente), los datos capturados en forma de eventos estándar o seguros son enviados al servicio de descubrimiento apropiado. Esto
5 permite verificar los productos a medida que atraviesan la cadena de suministro y generan eventos (estándar o seguros) cuando ocurren en tiempo real.

De manera más específica, cada producto o activo o dato que sea seguido a lo largo de la cadena de
10 suministro de petróleo y gas incluye al menos un identificador o autenticador de producto. Debe apreciarse que el término producto, como se usa aquí, puede incluir o ser reemplazado con cualquier combinación de los términos activo y datos. Es decir, que los productos, activos y
15 datos pueden cada uno atravesar la cadena de suministro. Cualquier referencia a un término puede incluir igualmente la referencia a otro, aún donde no se establezca de manera explícita. Como se explicó, un dispositivo de captura de datos (por ejemplo, detector, cámara, etc.) puede ser usado
20 para identificar un identificador y un autenticador de producto cuando ocurra uno de varios eventos. Esos eventos pueden incluir, pero no se limitan a, búsqueda y exploración, refinación, flujo en una tubería, transporte por camión, etc. Por ejemplo, cuando un producto sea
25 enviado de un distribuidor a un minorista, un detector o un

recolector de datos (por ejemplo reporte manual) en el distribuidor indica que el producto está siendo entregado y esta información es enviada a un servicio de recepción correspondiente (por ejemplo, minorista, estación de gasolina si el producto es combustible, y cuando el producto alcance al minorista, otro detector o recolector de datos indica que el producto ha arribado y esta información es almacenada en un servicio de descubrimiento correspondiente). Debe apreciarse que los datos también pueden ser “capturados” usando una variedad de técnicas. Por ejemplo, podría existir un reporte manual de datos y embarques o algún agrupamiento de datos. En un ejemplo, un evento indicaría que el producto ha sido cargado en el Camión #N. Otro dato indicaría la posición GPS del Camión #N mostrando que éste salió. Entonces se inferiría que el producto está saliendo. Una capa adicional de protección y seguridad es proporcionada usando el depósito e interfaz 516, la cual, como se describió, almacena un identificador y un autenticador de producto que es vinculado o asociado con un producto correspondiente. El identificador y el autenticador de producto proporciona un nivel más de seguridad debido a que únicamente un detector (dispositivo de captura de datos) está diseñado específicamente para leer el identificador y autenticador de producto y puede verificar un producto correspondiente sobre el cual se

colocó. Este nivel agregado de seguridad reduce en gran medida la probabilidad de que entren productos falsificados y manipulados de manera indebida a la cadena de suministro y permite que el interior del sistema tenga datos tan
5 seguros y exactos como sea posible, usados posteriormente en parte del sistema de integración de datos o administración de datos del GMS o IMS.

Se describe una breve explicación del proceso que implica las diferentes cantidades de la Figura 4. El
10 proceso comienza, por ejemplo, con un artículo que pasa a través de una cadena de suministro, del sector upstream 508 a través del sector midstream 510 hasta el sector downstream 514. La custodia del producto es registrada a lo largo de la cadena de suministro con el servicio de
15 descubrimiento respectivo (el cual puede ser el mismo o un servicio diferente). En algunas modalidades, el registro ocurre cuando es capturado un evento acerca del producto. Es decir, cuando ocurre un evento especificado, el evento asociado con el producto es enviado al servicio de
20 descubrimiento. Esta información también es reportada y almacenada en el depósito y la interfaz 514. El depósito y la interfaz 514 pueden validar la autenticidad del producto sobre la base de la información del identificador y autenticador de producto (por ejemplo el marcado) que ha
25 sido previamente capturada y almacenada allí.

La Figura 5 es un diagrama ejemplar de un sistema de administración de integridad de acuerdo con una modalidad de la descripción. El sistema de administración de integridad IMS incluye, pero no se limita a, interfaces con las cuales una plataforma de recuperación de impuestos especiales se interconecta vía una plataforma de impuestos especiales (la plataforma es una plataforma principalmente basada en software), un sistema de administración de datos DMS, un módulo de integración de datos (o plataforma de conectividad empresarial), una interfaz de puerta de enlace y detectores o recolectores de datos usados para capturar datos de los sectores upstream, midstream y downstream, junto con varios sistemas que almacenan y proporcionan datos de socios, franquicias y subsidiarias futuras de una entidad corporativa (no mostrada). El sistema de administración de integridad IMS también puede incluir o extenderse a recursos externos, administración de campo y recursos, aplicaciones predictivas y prescriptivas, administración de eventos basada en evidencias y sistemas legados existentes. Debe apreciarse que el sistema de administración de integridad IMS no se limita a los componentes descritos, ni debe incluir en cada uno de los componentes ilustrados en la modalidad no limitante y ejemplar. Por ejemplo, un sistema de control de supervisión y adquisición de datos (ICS como SCADA) puede reemplazar la

recolección de datos en lugar de la interfaz de puerta de enlace. Como se hizo notar anteriormente, los datos pueden ser almacenados en un solo depósito o depósitos múltiples. La puerta de enlace podría también ser de drones que tengan
5 las mismas capacidades que una puerta de enlace fija que se interconecten con el control de supervisión y adquisición de datos y que recolectarán la información directamente de los detectores o recolectores de datos a nivel upstream, midstream y downstream.

10 El sistema de administración de la integridad IMS administra y controla o se interconecta con al menos una entidad en una cadena de suministro de activos de petróleo y gas. La entidad puede incluir, pero no se limita a, una entidad corporativa, socios, franquicias, subsidiarias y/o
15 una entidad administradora de impuestos futura. Un sistema y método de administración de impuestos especiales para identificar y conciliar asimetrías entre las presentaciones de impuestos, volúmenes de producción y reportes de operación de las diferentes entidades. El sistema de
20 administración de integridad IMS recolecta los datos heterogéneos, no estructurados y fragmentados de detectores, recolectores de datos y subsistemas de verificación en la infraestructura (tubería) de petróleo y gas upstream, midstream y downstream para almacenar y
25 procesar los datos recolectados usando el conocimiento de

los sistemas de la infraestructura de petróleo y gas. Los datos también son recolectados vía las subsidiarias, franquicias y socios futuros, planeación de recursos empresariales u otros sistemas de administración financiera como aplicaciones desarrolladas por clientes legados. Los datos recolectados de las subsidiarias, franquicias y socios futuros pueden incluir, por ejemplo, una factura, pago y datos de administración de efectivo. Los datos son estructurados para el procesamiento y análisis adicionales, y la integridad de los datos estructurados es verificada y asegurada para evitar la manipulación indebida. Eventualmente, los datos son enviados al sistema de administración de datos de DMS, en otra modalidad, para la filtración/transformación, extracción/anotación, correlación, reconciliación, clasificación y almacenamiento.

De manera más específica, los datos recolectados serán adquiridos y procesados en tiempo real y enrutados al sistema de administración de datos DMS. El sistema de administración de datos DMS, en esta modalidad, incluye un módulo de filtración y transformación, un módulo de extracción/anotación, un módulo de correlación y un módulo de clasificación. También se proporciona en el sistema de administración de datos DMS un almacén de datos y un almacén de datos de operación. El sistema de administración

de datos DMS es responsable de filtrar y transformar los datos recolectados y capturados por los detectores, recolectores, subsidiaria, franquicia y/o futuros socios (los cuales pueden ser asegurados y agrupados); extraer y
5 anotar los datos filtrados y transformados; correlacionar los datos extraídos y anotados; y clasificar los datos correlacionados. Los datos clasificados son entonces enviados a un almacén de datos y un almacén de datos de operación para su almacenamiento.

10 El sistema administrador de datos DMS también es responsable de administrar (y almacenar) datos almacenados en este almacén de datos y en este almacén de datos de operación para la interfaz de la plataforma de impuestos especiales. La interfaz de la plataforma de impuestos
15 especiales incluye, por ejemplo, un módulo de identificación de activador de impuestos, un módulo de reporte de operación, un módulo KPI de cumplimiento de impuestos tributario y un módulo constructor de datos consolidados. La interfaz de la plataforma de impuestos
20 especiales se interconecta entre el sistema de administración de datos DMS y la plataforma de recuperación de impuestos especiales. La interfaz de la plataforma de impuestos especiales calcula y da formato a estimados de impuestos especiales sobre la base de una amplia variedad
25 de datos, incluyendo datos de operación volumétricos y

financieros. Los datos calculados y con formato son identificados como una transacción gravable para su reconciliación posterior, y la retroalimentación de KPIs relacionados con impuestos son enviados a un tablero de

5 instrumento de KPI (descrito más adelante) en la plataforma de recuperación de impuestos especiales. En particular, la interfaz de la plataforma de impuestos especiales identifica transacciones gravables para la reconciliación en el módulo de identificación de impuestos, calcula y da

10 formato a datos en el módulo de reporte de operación, proporciona la retroalimentación de los datos con formato en el módulo de cumplimiento de impuestos y consolida los datos enviados desde el módulo de identificación de impuestos, el módulo de reporte de operación y el módulo de

15 cumplimiento de impuestos en el módulo constructor de datos. Adicionalmente, la interfaz de la plataforma de impuestos especiales recibe los datos (los cuales pueden ser asegurados y agrupados) generados por el sistema de administración de datos DMS, permitiendo por lo tanto que

20 una entidad compare y reconcilie al menos uno de los impuestos especiales, la recolección de impuestos y el KPI generado por otras entidades. Esta interfaz permite que el sistema de administración de integridad IMS proporcione una verificación cruzada integrada y una reconciliación de

25 datos relacionados con impuestos entre fuentes de reporte

independientes. Finalmente, esto da transparencia al pago de impuestos, de modo que las actividades fraudulentas puedan ser minimizadas. Como ejemplo, los KPIs tributarios y los datos de impuestos relacionados son datos complejos y
5 deberán ser adaptados en tiempo casi real de acuerdo a reglas específicas proporcionadas por las reglas tributarias estatales. Por ejemplo, si el volumen de petróleo vendido es de 5000 barriles, el valor del impuesto podría ser del 5 por ciento. Cuando el volumen de petróleo
10 vendido es de 500,000 barriles, el valor del impuesto es de solamente el 3 por ciento. La plataforma de recuperación de impuestos mantiene todas las reglas para tratar los datos proporcionados con el DMS y lo relacionado con los impuestos que van a ser generados sobre la base de las
15 reglas proporcionadas de los impuestos correspondientes que deberán ser pagados. Otro ejemplo ocurre en el sector downstream cuando una estación de gasolina declara una cantidad de ventas en dólares que no corresponda al volumen de producto distribuido al lugar.

20 La plataforma de recuperación de impuestos especiales que está interconectada con el IMS incluye, pero no se limita a, un motor de correlación de transacciones financieras, analíticas de datos (por ejemplo, descriptivas, de diagnóstico, predictivas y prescriptivas),
25 un KPI o tablero de instrumentos de reporte, descubrimiento

de datos ad-hoc, un módulo de reporte y publicación, otro módulo de interfaz del sistema, un portal de red, aplicaciones móviles, un motor de flujo de trabajo, un archivo de transacciones, procesamiento de transacciones y un depósito de transacciones. La plataforma de recuperación de impuestos especiales recibe los datos consolidados de la interfaz de la plataforma de impuestos especiales (la cual ha recibido impuestos seguros y exactos relacionados con datos del DMS y parte del IMS) para identificar y reconciliar asimetrías entre los datos consolidados generados automáticamente por la interfaz de la plataforma de impuestos especiales y una declaración de impuestos correspondiente independientemente o generada manualmente (por ejemplo, a nivel de subsidiarias o a nivel corporativo o cualquier entidad implicada en la cadena de suministro de petróleo y gas). La plataforma de recuperación de impuestos especiales también tiene un depósito de transacciones que almacena los datos identificados y reconciliados del motor de correlación, un procesador de transacción para vincular los datos identificados y reconciliados, un archivo de transacciones que almacena datos identificados y reconciliados archivados del motor de correlación; y un módulo analítico de datos que recibe datos procesados y archivados para el análisis descriptivo, de diagnóstico, predictivo y prescriptivo. Los datos enviados al módulo

analítico de datos pueden ser introducidos en un módulo de análisis de predicción y predictivo (aplicación predictiva y prescriptiva) que use una máquina que aprende a identificar secuencias de mediciones (Figura 8A) o datos
5 calculados que sean clasificados como “eventos” que requieran algún forma de acción y/o reporte. La clasificación de un evento, previamente suministrado por el sistema de administración de datos, puede ser confirmada (por un operador humano o máquina) y los resultados
10 enviados al módulo de predicción y prescripción para mejorar el sistema de capacitación para el algoritmo de aprendizaje, permitiendo que éste “aprenda” durante el curso del tiempo. Usando el aprendizaje de la máquina, el sistema de administración de integridad IMS aprenderá
15 cuáles series de mediciones de eventos tomadas juntas indicarán que un cierto evento o grupo de eventos ha ocurrido. Usando los eventos “aprendidos”, el sistema es capaz de utilizar datos históricos y mejorar la exactitud con el tiempo. Los reportes de impuestos de la plataforma
20 de recuperación de impuestos especiales proporcionarán a las subsidiarias, socios y franquicias de petróleo y gas cuáles podrían incluir información acerca de declaraciones pasadas, consolidaciones y proyecciones futuras. En consecuencia, la plataforma de recuperación de impuestos
25 especiales permite la administración de impuestos con una

entrada frontal para el acceso del contribuyente, una presentación de impuestos unificada y un depósito de volumen de producción y reconciliación, integradas en analíticas de datos y un tablero de instrumentos de reporte para la administración de impuestos, un sistema integrado y centralizado para la administración y recuperación de impuestos especiales de petróleo y gas, y la identificación y reconciliación de asimetrías entre presentaciones de impuestos, volúmenes de producción y reportes de operación, proporcionando por lo tanto la recuperación eficiente de impuestos especiales. De manera más específica, en una modalidad, en la etapa de la reconciliación de impuestos, el sistema verifica automáticamente dos veces una declaración manual con los datos capturados automáticamente (y transformados de manera segura y usados para crear datos relacionados con impuestos agrupados útiles capaces de crear una declaración de impuestos segura y válida para propósitos de verificación). Es importante notar, que una ventaja particular del IMS de acuerdo a la presente invención cuando se interconecta con la plataforma de recuperación de impuestos vía la plataforma de impuestos especiales, es la calidad de los datos proporcionados a la plataforma de impuestos especiales. El IMS no únicamente recopilará datos de varias fuentes, sino que creará datos seguros y exactos, lo cual será útil para crear datos

agrupados y reportes seguros y confiables, útiles para una recolección de impuestos eficiente y corregir asimetrías en la cadena de suministro de petróleo y gas.

La Figura 6A ilustra un diagrama de flujo
5 ejemplar para marcar un producto de acuerdo con el sistema. En 700, es creado un identificador de producto usando las técnicas descritas anteriormente. El identificador de producto es capturado en un depósito de información en 702, y el producto es marcado con el identificador de producto
10 en 704. En 706, la información del activo (producto) y el identificador de producto correspondiente son almacenados juntos en el depósito y asociados para su uso posterior, por ejemplo para autenticar posteriormente el producto cuando éste atraviese una cadena de suministro. La Figura
15 6B ilustra un diagrama de flujo ejemplar de seguimiento y autenticación de un evento de acuerdo con el sistema. En 710, el producto se desplaza a lo largo de una cadena de suministro, haciendo varias paradas en varios sectores (por ejemplo los sectores upstream, midstream y downstream). En
20 cada uno de los sectores, cuando ocurre un evento especificado (712), el producto es identificado con un dispositivo de captura de datos (por ejemplo un detector). El dispositivo de captura de datos, como se explicó, identifica el identificador de producto (marca) en 714 y la
25 información capturada es reportada para su autenticación

posterior en 716. Los dispositivos de captura de datos no seguros o comercialmente disponibles (es decir un dispositivo que no es capaz de leer un evento seguro (como se define más adelante)) leen el marcado del producto de modo que la verificación del evento no incluye la autenticación usando el identificador o autenticador de objeto seguro. Un dispositivo de captura de datos seguro, por otro lado, es un dispositivo autenticado y dedicado que lee el marcado del producto de modo que el identificador o autenticador de objeto seguro del producto pueda ser utilizado para validar y autenticar el producto a lo largo de la cadena de suministro. La identificación y autenticación de un producto cuando ocurre un evento en este respecto es llamado un evento seguro. Es decir, el evento que ha hecho que la información sea enviada al sistema es "seguro" en virtud del hecho de que el dispositivo de captura de datos es capaz de identificar y verificar que el identificador o autenticador de producto seguro está asociado apropiadamente con el producto. Por ejemplo, el identificador o autenticador de objeto seguro puede ser una marca en el activo que sea identificada y vinculada con el evento.

Ahora se describe un ejemplo del proceso descrito en las Figuras 6A y 6B. La cadena de suministro incluye

“socios” en los tres diferentes sectores, un socio en el sector upstream, un socio en el sector midstream y un socio en el sector downstream. El socio del sector upstream envía un evento al servidor de descubrimiento que indica que un

5 producto será buscado y explorado en la cadena de suministro. Cuando el socio del sector upstream ha completado la fabricación del producto en un producto sostenible (por ejemplo, petróleo o combustible), el producto es marcado con un identificador y autenticador

10 de producto. El identificador y autenticador de producto que corresponde al producto es almacenado en un depósito, y es creado y enviado otro evento al servidor de descubrimiento indicando que el producto ha sido terminado y está siendo transferido al socio del sector midstream.

15 Una vez recibido en el socio del sector midstream, el producto es explorado por un dispositivo observador seguro (por ejemplo, un detector) para verificar y autenticar el producto usando el identificador y autenticador de producto, y el socio en el sector midstream pasa el

20 producto al socio del sector downstream. Es enviado otro evento al servidor de descubrimiento indicando que el socio del sector midstream ha enviado embarcado el producto a un socio del sector downstream. Una vez recibido en el socio del sector downstream, es enviado un evento adicional al

25 servidor de descubrimiento indicando que el producto ha

sido recibido, y una vez más el producto puede ser verificado y autenticado a lo largo de la cadena de suministro identificando el identificador y autenticador del producto usando un dispositivo observador seguro (por ejemplo, un detector).

Los eventos enviados y almacenados en el servidor de descubrimiento, el cual puede ser el mismo o un servidor de descubrimiento diferente, son observables por los socios en la cadena de suministro usando técnicas conocidas como una base de datos de eventos, filas de espera o colas y tablas de registro. Los eventos pueden ser formados en una variedad de clases dependiendo del producto que atraviese la cadena de suministro. También puede proporcionarse la notificación de mensajes a socios usando un reporte de red seguro, enviando notificaciones de alarma y enviando mensajes vía correo electrónico, SMS, o usando cualesquier otros medios conocidos por el experto en la técnica. Cuando un socio desee autenticar y verificar un producto, puede hacerse una consulta al sistema vía la plataforma de serialización y la interfaz 605, discutida aquí anteriormente. Además de información típica como el tipo de evento, fecha del evento, nombre del socio, etc., el socio también puede solicitar o hacer que se entregue automáticamente información con respecto a la autenticidad del producto (asumiendo que es usado un dispositivo

observador seguro para leer el identificador y el autenticador de producto). A este respecto, el producto puede ser comparado contra la información almacenada en la plataforma de serialización e interfaz 605. Si se determina
5 que se ha encontrado una coincidencia, entonces el producto puede ser verificado, como se describió anteriormente.

La Figura 7 ilustra un diagrama de bloques ejemplar para generar un evento seguro de acuerdo con el sistema. El sistema de eventos seguro ejemplar 800 incluye
10 varios componentes, por ejemplo, un dispositivo observador seguro 802 (por ejemplo, un detector), un producto 810 con una marca 804 (por ejemplo, petróleo o combustible con una marca), un evento seguro 806 y un depósito 808. Los diferentes componentes pueden ser vinculados juntos vía
15 comunicación alámbrica o inalámbrica y pueden ser parte de la misma o redes diferentes (no ilustradas). Como un producto atraviese una cadena de suministro, el dispositivo observador seguro captura datos acerca del producto. Los datos capturados incluyen información del evento estándar e
20 información del evento seguro. Los datos capturados forman un evento seguro 806 el cual es transmitido al depósito 808 para su almacenamiento. Aunque la modalidad descrita describe el almacenamiento del evento seguro 806 en el depósito 808, la descripción no se limita a esa modalidad.
25 Más bien, el evento seguro 806 podría ser almacenado en el

dispositivo observador seguro 802, o en cualquier otro lugar accesible sobre la red.

El marcado 804 sobre el producto 810 incluye información del evento estándar e información del evento
5 seguro. En una modalidad, el marcado 804 incluye ambas de la información del evento estándar y seguro. Es decir, que el marcado puede incluir varias composiciones químicas o incluir identificadores suplementarios que identifiquen la información del evento estándar y/o seguro. En otra
10 modalidad, la información del evento estándar está separada de la información del evento seguro. Un evento seguro 806 es cualquier combinación de datos (marcado) en la que esté presente la información del evento seguro. Por ejemplo, un primer identificador de producto identifica la información
15 del evento estándar (un primer marcado o ausencia de marcado), y un autenticador o segundo identificador de producto (en la forma del marcado) identifica la información del evento seguro (un segundo marcado). Debe apreciarse, sin embargo, que la descripción no se limita a
20 la modalidad descrita, la cual es de naturaleza ejemplar. El dispositivo observador seguro 802 autentifica el marcado 804 y puede agregar una firma o encriptación a los datos capturados y almacena ésta como un evento seguro 806 en el depósito 808.

25 La Figura 8 ilustra un depósito mundial ejemplar

de acuerdo con el sistema. El depósito global 900 incluye, por ejemplo, el depósito R1, el depósito R2 y el depósito Rn. Los depósitos R1, R2 y Rn pueden localizarse en la misma o redes diferentes y pueden estar asociados con el mismo o custodios diferentes (por ejemplo, custodios en los sectores upstream, midstream y downstream) a lo largo de una cadena de suministro S. En el ejemplo ilustrado, ocurren varios eventos cuando un artículo se desplaza en una cadena de suministro S. Un evento en la modalidad ejemplar es representado por el carácter alfanumérico En, donde n es un entero que representa el número de evento. En este caso, se ilustra n total de siete eventos (E1 - E7). Los En eventos con un asterisco ("*") representan un evento seguro y los eventos sin un asterisco representan un evento estándar o no seguro. Como se describió anteriormente, un evento estándar se genera cuando un dispositivo de captura de datos estándar (dispositivo observador normal NOD) lee información del evento estándar identificada en un producto en la cadena de suministro S. Un evento seguro, por otro lado, se genera cuando un dispositivo de captura de datos seguro (dispositivo observador seguro SOD) lee información del evento estándar e información del evento seguro en un producto en la cadena de suministro S, información la cual es autenticada por el dispositivo observador seguro SOD. Como se describió, el NOD y SOD pueden ser detectores o

cualquier dispositivo capaz de identificar el marcado en el producto (o cualquier otro parámetro capturado por el dispositivo observador seguro). En la modalidad ilustrada, el depósito R1 recibe los eventos seguros E1* y E3* capturados desde un dispositivo de observador seguro SOD, y un evento estándar E2 capturado desde un dispositivo observador normal NOD. El depósito R2 recibe un evento estándar E4 capturado por un dispositivo observador normal NOD, y el depósito Rn recibe el evento seguro E6*, capturado por un dispositivo observador seguro SOD y los eventos estándar E5 y E7, capturados por un dispositivo observador normal NOD.

De manera significativa, la capacidad para autenticar un producto usando un dispositivo de captura de datos seguro mejora la capacidad para detectar productos falsificados y/o adulterados o manipulados de manera indebida en un lugar específico en la cadena de suministro S. Es decir que, en el sistema de administración de la presente descripción, la detección de autenticación puede ocurrir en un lugar específico puesto que los eventos seguros se basan en una lectura de un identificador o autenticador de producto (por ejemplo, un marcado) y puesto que los diferentes dispositivos de captura de datos seguros pueden crear diferentes eventos seguros sobre la base del identificador o autenticador de producto. En los

sistemas de administración tradicionales, usan por ejemplo, la tecnología del detector EPCIS y convencional (normal), los productos, activos o artículos falsificados y/o adulterados y/o desviados y manipulados de manera indebida podrían no ser detectados en un lugar específico en la cadena de suministro S, ni aún identificados como lo que ocurrió en algún lugar entre dos puntos (es decir, dos puntos de dispositivo de captura de datos) en la cadena de suministro S. Esto se debe a que el evento capturado en el sistema tradicional, como se explicó anteriormente, es un evento estándar o no seguro en el cual no ocurre un nivel agregado de autenticación. Usando el sistema de administración de suministro global de la presente descripción, es posible recuperar la ubicación de la adulteración y/o falsificación en una forma más rápida que en los sistemas de administración tradicionales como resultado del nivel agregado de autenticación del sistema de administración de suministro global de la presente descripción. En realidad, la búsqueda de la ubicación de la adulteración y/o falsificación puede ser tremendamente acelerada, puesto que ésta puede limitarse a la porción de la cadena de suministro localizada entre el dispositivo de captura de datos seguro, donde la autenticación del producto seguido (o datos capturados del SOD) falló en la cadena de suministro de S (es decir, entre dos puntos de

SOD de captura de datos).

La Figura 9 es un diagrama ejemplar de un sistema de administración global de acuerdo con una modalidad de la descripción. El sistema de administración global GMS incluye, pero no se limita a, un centro de control CCC, un sistema de administración de datos, y un módulo de integración de datos, una interfaz de usuario, una interfaz de puerta de enlace, detectores, recolectores de datos y el sistema de administración de suministro global (como se describe aquí) usado para capturar datos upstream, midstream y downstream. El sistema de administración global GMS también puede incluir o extenderse a recursos externos como ERPs, administración de campo y recursos, aplicaciones predictivas y prescriptivas, administración de eventos basados en evidencias y sistemas legados existentes. Se apreciará que el sistema de administración global GMS no se limita a los componentes descritos, ni debe incluir cada uno de los componentes ilustrados en la modalidad no limitante y ejemplar. Por ejemplo, el sistema de administración de suministro, o un sistema de control de supervisión y adquisición de datos (ICS como el SCADA) puede reemplazar la recolección de datos en lugar de la interfaz de la puerta de enlace. Como se hizo notar anteriormente, los datos pueden ser almacenados en un solo depósito o depósitos múltiples.

El sistema de administración global administra los activos de petróleo y gas en una forma segura (o en una forma no segura, si es deseable) verificando actividades ilegales sobre la cadena de suministro, alertando a las autoridades y/o personal autorizado y respondiendo a las actividades ilegales en una forma apropiada. El sistema de administración global GMS recolecta los datos heterogéneos, no estructurados y fragmentados de sensores, recolectores de datos y subsistemas de verificación y también proporcionadas por el SOD, incluyendo el sistema de administración de suministro global, en la infraestructura (tuberías) de petróleo y gas de los sectores upstream, midstream y downstream, para almacenar y procesar los datos recolectados usando el conocimiento de los sistemas de infraestructura de petróleo y gas. Los datos son estructurados para el procesamiento y análisis adicional, y la integridad de los datos estructurados es verificada y asegurada para evitar la manipulación indebida. Eventualmente, como se describió anteriormente, los datos son enviados al centro de control de CCC para que el personal responda a robo o incidentes de operación similares. Este proceso permite una respuesta más rápida en comparación con los sistemas actuales, al igual que proporciona una base evidencial que constituye una prueba material admisible en un juzgado para apoyar el

procesamiento de delincuentes. Por ejemplo, pueden ser usados drones para proporcionar evidencia en el sitio en que ha ocurrido un evento.

El sistema de administración de integridad IMS recolecta los datos heterogéneos, no estructurados y fragmentados de los detectores, recolectores de datos y subsistemas de verificación, incluyendo aquellos del sistema de administración de suministro global y también proporcionados por el SOD, en la infraestructura (tuberías) de petróleo y gas de los sectores upstream, midstream y downstream para almacenar y procesar los datos recolectados usando el conocimiento de los sistemas de infraestructura de petróleo y gas. Al contrario del GMS, los datos recolectados son estructurados para su análisis y procesamiento adicional, y la integridad de los datos estructurados es verificada y asegurada para evitar la manipulación indebida, y agrupados de tal manera que todos los datos relacionados con aspectos fiscales o aspectos de KPI o administración de subsidiarias o franquicias a nivel corporativo, sean generados y usados para crear reportes de impuesto seguros, y reportes seguros a nivel corporativo para administrar de manera eficiente las diferentes entidades en la cadena de suministro de petróleo y gas, permitiendo la reconciliación de datos relacionados con impuestos y KPI y corregir asimetrías potencialmente

existentes en la cadena de suministro de petróleo y gas.

Ambos sistemas a pesar de sus diferentes propósitos dependen de características comunes, como la puerta de enlace por ejemplo, o módulos de BRE o eventos
5 seguros agrupados para generar alertas o un reporte seguro o datos relacionados con impuestos seguros. Pero esos sistemas GMS e IMS, dependerán fuertemente de los datos proporcionados por el SOD los cuales son seguros y exactos, para usarlos de manera eficiente para sus propios
10 propósitos y funciones. Alertas e intervención por el GMS por ejemplo, recolección de impuestos o reconciliación de datos relacionados con impuestos o corrección de asimetrías con el IMS. Mientras más seguros sean los datos y más confiables sean los datos que tenemos en el sistema,
15 mejores serán los eventos agrupados y el reporte seguro correspondiente (KPI, estimación de impuestos y reconciliación de valor o impuestos) que tendremos en la cadena de suministro de petróleo y gas.

De manera más específica, los datos
20 recolectado serán adquiridos y procesados en tiempo real y enrutados al centro de control CCC (el cual puede estar en forma de un centro de control de órdenes físicas y/o una aplicación operativamente independiente del personal, o cualquier combinación de las mismas) para la presentación
25 apropiada para el personal del centro de órdenes. Los datos

estructurados serán analizados de acuerdo a modelos y/o algoritmos computacionales para identificar eventos, donde los eventos pueden ser incidentes de operación como aquellas actividades ilegales descritas anteriormente y

5 también problemas de operación, los cuales pueden ser identificados y presentados a los operadores en tiempo real. En paralelo (o en otro momento), los datos estructurados y los eventos pueden ser introducidos en un módulo de análisis de predicción y prescripción (aplicación

10 predictiva y prescriptiva) que use aprendizaje de máquina, como se describió anteriormente, para identificar las secuencias de mediciones o datos calculados que sean clasificados como "eventos" que requieran alguna forma de acción y/o reporte. La clasificación de un evento,

15 previamente suministrado por el sistema de administración de datos, puede ser confirmado (por un operador humano o máquina) y los resultados enviados al módulo de predicción y prescripción para mejorar el sistema de capacitación para el algoritmo de aprendizaje, permitiendo que éste "aprenda"

20 durante el transcurrir del tiempo. Usando el aprendizaje de máquina, el sistema de administración global o el sistema de administración de integridad aprenderá cuáles series de mediciones de eventos, tomadas juntas indicarán que un cierto evento o grupo de eventos ha ocurrido. Usando los

25 eventos "aprendidos", el sistema puede utilizar datos

históricos y mejorar la exactitud con el tiempo. La exactitud también puede ser suplementada con verificación humana o de un dron en el lugar donde ocurran los eventos, y usando las alertas generadas por el sistema.

5 El sistema de administración de datos, de manera similar al centro de control CCC, también puede estar en comunicación con el módulo de predicción y prescripción, el cual usará el aprendizaje de máquina de datos estructurados y eventos como el sistema de aprendizaje para clasificar
10 eventos, los cuales pueden ser comprendidos como secuencias de mediciones. El módulo de predicción y prescripción proporciona información para identificar probables eventos (en diferentes grados) en el futuro, o eventos en progreso que puedan ser enviados como eventos al centro de control
15 CCC. El módulo de predicción y prescripción también puede prescribir la respuesta del evento muy probablemente para obtener un resultado positivo sobre la base de la historia de los eventos. De manera similar, tendencias reconocidas (o conocidas) que ocurran durante el transcurrir del tiempo
20 pueden ser usadas para mejorar los eventos agrupados para generar de manera más exacta las alertas en el centro de control CCC.

La Figura 10 ilustra un diagrama ejemplar de una interfaz de acuerdo con una modalidad de la descripción.
25 Como se ilustra, la interfaz (puerta de enlace) recibe

datos de una o más de una variedad de fuentes. Por ejemplo, los datos recolectados de los detectores de los sectores upstream, midstream y downstream que son procesados por los sistemas SCADA son pasados a lo largo de la interfaz de la

5 puerta de enlace. En una modalidad alternativa, la puerta de enlace reemplaza el sistema de control industrial (como SCADA) y recolecta datos directamente de los detectores de los sectores upstream, midstream, y downstream otras fuentes, como desde el sistema de administración de

10 suministro global (el cual usa el dispositivo observador seguro mencionado anteriormente). La interfaz de la puerta de enlace transforma (por ejemplo, clasifica, da formato y modifica) los datos recolectados en datos seguros y con formato que son compatibles con el sistema, en particular

15 al módulo de integración de datos, antes de ser enviados al sistema de administración de datos para el análisis por el sistema de administración global o en el sistema de administración de la integridad.

Las Figuras 11A-11D ilustran mediciones de

20 detectores ejemplares y detectores que recolectan datos a lo largo de una cadena de suministro de acuerdo con una modalidad de la descripción. Los datos recolectados son procesados por el sistema de administración de integridad a datos agrupados y estructurados generados o reportados

25 directamente como un reporte de impuestos, reporte

financiero, reporte de KPI, forma de impuestos seguros o cualquier reporte útil para preparar una declaración de impuestos final. Una vez que una secuencia particular de mediciones (o secuencia de eventos) asociada con una descripción del evento es conocida (es decir aprendida por la aplicación de predicción y prescripción), los eventos pueden ser marcados en tiempo real con un puntaje de probabilidad indicando la probabilidad de que una secuencia de desglose de mediciones dé como resultado un evento identificable (como un evento gravable o secuencia de eventos gravables). En las Figuras, los cuadros sombreados representan los valores recibidos desde un detector dado. La Figura 11A muestra un número ejemplar de detectores 1...m que son configurados para capturar una secuencia de eventos. Las Figuras 11B, 11C y 11D muestran una secuencia ejemplar de eventos en la cual los datos capturados durante el curso del tiempo t representan una probabilidad débil, una probabilidad media y una probabilidad alta, respectivamente, de que el evento haya ocurrido (llamada aquí, la probabilidad del evento). La probabilidad del evento es enviada al sistema de administración de datos de DMS, a la interfaz de la plataforma de impuestos especiales y a la plataforma de recuperación de impuestos especiales que identifica un evento gravable, como "500 barriles de combustible vendidos en un lugar X en una fecha dada".

Para mejorar la eficiencia, usando el módulo predictivo y prescriptivo, sobre la base de eventos pasados contenidos en los datos históricos de mediciones y eventos, pueden ser generados y usados patrones desde los datos históricos para ayudar a predecir eventos futuros (es decir, eventos gravables) antes de que los detectores y recolectores de datos comiencen a registrar datos. Usando estos datos predictivos, la plataforma de recuperación de impuestos especiales (la cual se interconecta con el DMS en el sistema IMS como se describe en la Figura 5) y el personal que opera la plataforma de recuperación de impuestos especiales podría ser alertado a áreas previstas por eventos gravables identificados por el sistema usando los datos en el sistema, como la hora del día, día de la semana, mes o fechas específicas, secuencias de eventos anteriores, y similares. Debe apreciarse de lo anterior que el sistema de administración de integridad IMS es capaz de registrar la evolución de eventos relacionados con impuestos, y vincularlos para proporcionar una historia para analizar y mejorar el análisis de datos en el sistema de administración de datos DMS. Sobre la base del conocimiento previo de eventos que han ocurrido en el pasado, los datos históricos y la verificación de que los eventos ocurrieron realmente, como la entrega de volumen de bombeo, cantidad de combustible transportado y número de

barriles de combustible, pago, administración de efectivo y generación de una factura, los eventos futuros pueden ser pronosticados con mayor exactitud y los eventos en sí pueden ser interpretados durante la verificación y el análisis. Adicionalmente, el sistema de administración de integridad IMS en virtud de su naturaleza predictiva y prescriptiva es capaz de mitigar la corrupción de personas, por ejemplo, es menos probable que el personal de operación en una subsidiaria, tercero, franquicia, etc., proporcione documentos fiscales falsificados dada la verificación y control de la plataforma de recuperación de impuestos especiales. En consecuencia, se vuelve cada vez más difícil, para las personas implicadas en las actividades ilegales evitar la detección suprimiendo datos, cambiando datos, pagando al personal que verifique los datos, etc.

De manera significativa, para evitar que ocurran esos tipos de situaciones, el sistema de administración de integridad proporciona: datos seguros e inolvidables los cuales no pueden ser borrados, alertas basadas en la correlación de eventos agrupados que dan una alta probabilidad de actividad falsificada (por ejemplo, la falsificación de información relacionada con impuestos), actividad la cual puede ser presentada a un operador y ser registrada como alertas que son también inolvidables y no pueden ser borradas. De manera alternativa o adicional, el

sistema en sí puede intervenir en lugar del personal para identificar y enviar información urgente a autoridades externas, como una administración tributaria, entidad gubernamental corporativa, etc. En consecuencia, una parte
5 del sistema suministra una alternativa al error e insuficiencias humanas en la detección de esa información falsificada.

Los ejemplos no limitantes adicionales del sistema de administración de integridad IMS, son
10 proporcionados más adelante con respecto a los sectores de midstream y downstream. En el sector midstream, las actividades relacionadas con impuestos típicamente ocurren modificando los datos recolectados y/o falsificando registros y materiales, como reportes de impuestos y
15 declaraciones de impuestos. Por ejemplo, tras la recepción de una transacción gravable, como la recepción del pago por la compra de 500 barriles de petróleo, la recepción puede ser forjada de modo que el impuesto especial se minimice. Al hacer esto, cuando está siendo preparando un reporte de
20 impuestos, la información relacionada con la transacción gravable reflejará la recepción forjada. Como contramedida y de acuerdo con los objetivos del sistema de administración de integridad IMS, los barriles pueden ser forrados con varios detectores y/o recolectores de datos
25 que verificarán y recolectarán datos de los mismos. Por

ejemplo, cada barril puede tener un detector que detecte cuándo un barril sea llevado de un centro de distribución a un punto de venta, lo que significa que ha ocurrido una compra del barril. El sistema de administración de integración IMS puede ser usado para verificar y recolectar datos relacionados con la transacción cuando ocurra ésta. Los datos recolectados de los detectores y recolectores de datos serán enviados a la puerta de enlace correspondiente (Figura 8) o sistema de control industrial ICS o escalado al sistema de administración de datos DMS y al centro de control CCC, como se describió aquí anteriormente. Adicionalmente, los datos recolectados deberán ser actualizados de tal manera que pueden ser interpretados para proporcionar conclusiones y recomendaciones. Por ejemplo, si los detectores o recolectores de datos únicamente detectan la compra de un barril una vez a la semana, los detectores y recolectores de datos pueden no captar la actividad de compra durante los seis días restantes de la semana. Si, por otro lado, la compra de un barril es medida dos veces al día, los detectores y recolectores de datos serán capaces de detectar y calcular de manera más exacta la compra de los barriles (o cualquier otro tipo de datos) indicando que está ocurriendo una transacción o actividad gravable. Vinculado con la ubicación de los detectores y recolectores de datos, un

dron no personal podría de manera alternativa o simultánea verificar la ubicación regional, podrían ser capturadas imágenes de una cámara local, y el sistema podría ser notificado de que las actividades están en proceso.

5 Otro ejemplo no limitante de datos en el sector midstream es un camión cisterna que transporta petróleo crudo y petróleo. En este ejemplo, los datos recolectados son información GPS generada por el viaje efectuado por el camión, y el volumen del contenido del tanque del camión.

10 Si los datos recolectados sobre el tiempo indican, por ejemplo, que el camión se está deteniendo en un lugar más de lo anticipado, o existe una variación de volumen del contenido del tanque, esto puede indicar que están ocurriendo o han ocurrido actividades ilegales. Por

15 ejemplo, la variación del volumen del contenido en el tanque puede ser una indicación de que alguien está intentado evitar reportar el evento como una transacción gravable. En otro ejemplo, el camión puede estar parado en un área de reposo nocturno. Puesto que esas áreas son una

20 parada regular conocida durante un período prolongado, los detectores de volumen en el camión pueden ser activados para verificar variaciones en el contenido del tanque. Cualquier cambio en la variación detectada por los detectores puede ser escalado a través del sistema de

25 administración de datos DMS al centro de control CCC

después de que los datos hayan sido analizados. Los motores de aprendizaje del sistema conocerán la región y la expectativa de las actividades en el área, y aplicarán ese conocimiento en análisis futuros. Nuevamente, estas 5 actividades podrían ser indicativas de que alguien está intentando evitar un evento específico que tenga consecuencias gravables.

En el sector downstream, es proporcionado un ejemplo no limitante en el cual los datos recolectados 10 incluyen el volumen producido en una fábrica de refinación. Los datos de volumen pueden ser vinculados, por ejemplo, con el número de camiones requeridos para transportar el contenido (combustible) del camión a tiendas o estaciones minoristas. Como se comprende, una vez que el combustible 15 alcanza las tiendas o estaciones minoristas, es descargado en los tanques de la tienda o estación para su almacenamiento. Aquí, el volumen es transferido y el combustible distribuido. Los detectores y recolectores de datos pueden entonces ser utilizados para medir los 20 volúmenes intercambiados correspondientes, y el efectivo generado por la venta del combustible. Si los volúmenes y las ventas no concuerdan, esto podría indicar actividades ilegales, como que están siendo generados documentos falsificados para evitar o eludir un evento gravable. Esta 25 información también puede ser útil para la recolección o

reconciliación de impuestos, para estimar la cantidad de combustible requerida en una región particular, etc. Como se aprecia, los datos no únicamente son recolectados, sino también almacenados en un depósito y transformados en una suma de eventos agrupados que pueden ser vinculados, utilizados o analizados para una acción prescriptiva o predictiva.

La Figura 12 es un diagrama ejemplar de una interfaz de acuerdo con una modalidad de la descripción. La interfaz, en esta aplicación referida como la Puerta de Enlace o Interfaz de la Puerta de Enlace, interconecta los detectores de datos que se ubican a lo largo de los sectores upstream, midstream y downstream con fuentes externas, como un bus o canal de servicio empresarial ESB o el Sistema de administración de global de datos vía el módulo de integración de datos. Como se ilustra, la puerta de enlace se divide en tres capas que incluyen: (1) la computadora (por ejemplo, para firmar y almacenar) la cual se comunica con los sistemas de control industrial (como SCADA, OPC, AS-i MODBUS y Ethercat). Los controladores pueden ser una combinación de interfaces físicas y software, (2) el motor de reglas comerciales (BRE) el cual correlaciona, asegura, autentifica, filtra, reconcilia, proporciona capacidad de no olvidar, y crea datos de valor clave. El BRE también a partir de los datos recolectados,

efectúa la asociación de los datos recolectados en objetos, crea eventos sobre la base de la falta de integridad de objetos, crea alertas basadas en eventos o umbrales basados en eventos o en reglas comerciales o en tendencias, y (3)
5 en las interfaces que se interconectan con los sistemas externos usando, por ejemplo, HTTPS, SSL o cualquier otro protocolo de software o hardware conocido.

La interfaz de la puerta de enlace proporciona, entre otras características, un mecanismo para transformar
10 los datos recolectados en un formato que sea más seguro y que sea compatible con el sistema externo al cual los datos transformados u objetos o eventos o alertas creadas en la puerta de enlace serán enviados. Por ejemplo, la interfaz de la puerta de enlace asegurará que los datos recolectados
15 entre los detectores y/o recolectores de datos así como el formato de los datos recolectados incompatibles con el sistema de integración de datos antes de ser usados en el sistema de administración global o en el sistema de administración de integridad en especial en el Sistema de
20 Administración de Datos DMS. La interfaz de la puerta de enlace se interconecta con sistemas externos usando, por ejemplo, protocolos como HTTPS, SSL, etc. Las interfaces externas incluyen, pero no se limitan a, un bus o canal de servicio empresarial ESB o un sistema de control industrial
25 ICS, como el sistema de administración de la puerta de

enlace GMS descrito aquí, sistemas de transacción o sistemas de transacción financiera.

En la capa de controladores, los controladores que se comunican con temas externos, como el sistema ICS, pueden ser hardware, software o cualquier combinación de los mismos. El hardware y software son preferiblemente resistentes a la manipulación indebida, y seguidos para evitar ataques sobre el hardware físico así como ataques maliciosos sobre el software, por ejemplo por piratas informáticos, inyección de datos indeseables o similares. Los datos que serán generados y creados en la interconexión de la puerta de enlace serán más seguros y proporcionarán propiedades mejoradas además de aquellos recolectados de los diferentes depósitos de datos, como el SCADA o ICS. Los datos seguros y mejorados serán entonces proporcionados al sistema de administración global o en el sistema de administración de integridad y ayudarán a crear los eventos agrupados. La puerta de enlace también verificará que los datos sean recibidos de los detectores y recolectores de datos, que sean datos auténticos y no hayan sido corrompidos por fuentes externas o de otro modo. Es decir, que la puerta de enlace primero tendrá la capacidad de autenticar los datos que estén siendo recibidos antes de asegurar los datos y agregar propiedades adicionales. Esto asegurará que los datos a ser asegurados y mejorados sean

autenticados antes de ser pasados al sistema de administración global o en el sistema de administración de integridad, y evitará que estén siendo enviados datos corrompidos al sistema de administración global o en el sistema de administración de integridad. Una debilidad de los sistemas existentes en la cadena de suministro de petróleo y gas es el volumen increíblemente grande de datos. Si el sistema es contaminado o infectado con datos falsos o falsificados, fabricados o inexactos, los datos capturados no serán confiables y cualquier evento o eventos agrupados creados en el sistema de administración de integridad global o en el sistema de administración de integridad pueden comprometer potencialmente las alertas generadas de los eventos agrupados. En consecuencia, cualquier dato al que se vaya a tener acceso o sea usado en el sistema de administración global o en el sistema de administración de integridad (vía el módulo de integración de datos), usando la puerta de enlace, deberá ser tan seguro y exacto como sea posible. Un ejemplo de autenticación de los datos que serán insertados en la puerta de enlace, es capturar desde los detectores, especialmente el SOD, o de varias veces, la información que se supone se capturará en un periodo breve de tiempo y verificar que los datos recolectados sean siempre de la misma naturaleza (la temperatura es capturada diez veces

durante 30 segundos y el valor es muy similar, entonces los datos parecen ser correctos). Otro ejemplo de autenticación para asegurarse de que los datos son exactos es agregar al detector un sistema o mecanismo electrónico que lo proteja contra la manipulación indebida o desviación y proteger el acceso al detector por cualquier medio, los datos recolectados del detector y entonces el envío a la puerta de enlace será tan seguro como es posible. Otro ejemplo para asegurarse de que los datos son seguros es: i) usar un detector a prueba de manipulación indebida; ii) comparar los datos con aquellos de otros detectores para asegurarse de que sean coherentes (por ejemplo, ¿si la temperatura se incrementa en un detector también se incrementa en detectores cercanos? ¿La presión cambia como consecuencia?, etc., iii) detección de anomalías: el uso del aprendizaje en máquina en datos pasados para detectar lecturas repetidas de detectores anómalos.

La interfaz de la puerta de enlace recolecta datos ya sea vía las interfaces físicas hacia los detectores industriales utilizando protocolos de comunicación industrial, como OPC o Ethercat, o vía interfaces virtuales (es decir software) a sistemas de verificación y control existentes, como el SCADA. Las interfaces son alimentadas, por ejemplo, usando

controladores de software que pueden ser cargados o descargados dinámicamente dependiendo de los requerimientos físicos o virtuales. Por ejemplo, si existen tres dispositivos alimentados por OPC y un dispositivo Ethercat
5 conectado físicamente, entonces existirían tres controladores de OPC y un solo controlador de Ethercat.

Una vez que los datos alcanzan la interfaz de la puerta de enlace, el Motor de Reglas Comerciales BRE crea nuevos datos de verificación correlacionando los datos
10 capturados, filtrando datos irrelevantes, por ejemplo eventos no relacionados con la seguridad, validando el acceso por lectura/escritura a/de la capa de controladores hacia la capa de integración (en ambas direcciones), y aplicando reglas de seguridad/acceso/autenticación,
15 usando un sistema externo si es necesario. Debe apreciarse, sin embargo, que esas funciones son únicamente ejemplares y el BRE se limita a esas funciones.

En la capa de interfaz, el software en la interfaz de la puerta de enlace también interactúa con
20 sistemas externos sobre la base de los requerimientos de verificación. Por ejemplo, la interfaz puede incluir una interfaz de correo electrónico, una interfaz de red, etc. La capa de interfaz también puede interconectarse con el bus o canal de servicio empresarial ESB como un sistema de
25 mensajería (por ejemplo, utilizando un protocolo como REST

sobre HTTPS) para integrar datos de todas las interfaces de la puerta de enlace y sistemas externos en el componente de almacenamiento de datos del sistema de administración global o en el sistema de administración de integridad.

5 También debe apreciarse que aunque el diagrama ilustra una interfaz para la interfaz de la puerta de enlace, la interfaz de la puerta de enlace también puede ser conectada directamente o ser parte del sistema de administración global o en el sistema de administración de integridad.

10 El software del canal o bus de servicio empresaria ESB es un sistema de mensajería similar a los productos de IBM^{MR} Serie MQueue y control de BMC. El Software de ESB, el cual en la presente modalidad es referido como la parte del módulo de integración de datos
15 del sistema de administración global o el sistema de administración de integridad (aunque debe apreciarse que el ESB también podría ser una entidad separada), podría ser una aplicación como la Open ESB desarrollada por Sun Microsystems^{MR} o WS02 ESB. Puede ser usado un lenguaje de
20 programación basado en JAVA como el lenguaje de programación para lograr ese software.

El Motor de Reglas Comerciales BRE, la segunda capa, actúa como el procesamiento de transformación de los datos capturados y aplica reglas las cuales pueden ser
25 configuradas para representar un elemento particular de

interés, como un incidente de seguridad potencial. El BRE verifica todas las actividades y puntos de medición de todos los controladores cargados, junto con cualquier dispositivo conectado físicamente o virtualmente. Teniendo
5 acceso a todos esos puntos de medición en tiempo real, el BRE puede crear nuevos puntos de medición o datos útiles para crear eventos agrupados en el sistema de administración global o en el sistema de administración de integridad. El BRE también a partir de datos recolectados,
10 efectúa la asociación de los datos recolectados en objetos, crea eventos sobre la base de objetos sin integridad, crea una alerta sobre la base de eventos o umbrales basados en eventos o en reglas comerciales o en tendencias. Por ejemplo, el punto de medición A en un dispositivo conectado
15 físicamente (como un protector de temperatura) y el punto de medición B (como uno disponible de un sistema SCADA de software externo) bajo umbrales específicos que puede crear nuevos datos sobre la base de ambos del punto de medición A y punto de medición B. Por ejemplo pueden ser creados
20 nuevos datos C, donde los nuevos datos C son un apéndice de los puntos de medición A y B y que pueden constituir un evento. Esto emplea el BRE para correlacionar datos para una mejor comprensión de eventos cuando ocurran. Los eventos generados en la puerta de enlace se basan en los
25 datos recolectados de detectores, el recolector de datos y

sistemas ICS. A esos datos que han sido verificados en su exactitud antes de entrar a la puerta de enlace, se les efectúa la adición de atributos de los datos para obtener datos mejorados.

5 En una modalidad, si los detectores, recolectores de datos y sistemas de ICS no están disponibles o no pueden verificar la exactitud de los datos, la verificación es efectuada en la puerta de enlace. Los eventos creados en la puerta de enlace serán útiles en el sistema de
10 administración de datos DMS del sistema de administración global o en el sistema de administración de integridad para crear los eventos agrupados o un reporte de impuestos seguro confiable o KPI seguro o ayudar para propósitos de recolección de impuestos o recuperación de impuestos o
15 corregir asimetrías (sobre la base del sistema, GMS o IMS, a través del cual pasan). Los eventos agrupados o el reporte de impuestos seguro o confiable o el KPI seguro o ayuda para propósitos de recolección de impuestos o recuperación de impuestos o asimetrías de corrección son
20 usados en un sistema de administración global o en el sistema de administración de integridad para crear y/o presentar alertas a nivel de CCC y permitirán en el contexto de la presente invención una intervención de campo deficiente y correspondiente (por ejemplo con la policía
25 cuando se robe material, bomberos si existe una explosión,

etc.). Por otro lado, el BRE también tendrá la capacidad de analizar la relevancia de los datos recolectados de los detectores, recolectores de datos o sistemas ICS, si están bien estructurados como eventos, recolectados de detectores
5 SOD en la cadena de suministro y si esos datos son suficientemente seguros, el BRE se enviará directamente al módulo de integración de datos, para ser tratados entonces en el GMS o IMS para generar eventos agrupados o un reporte seguro confiable o KPI seguro o ayudar al propósito de
10 recolección de impuestos o recuperación de impuestos o corregir asimetrías.

El BRE también puede actuar de manera autónoma si está disponible suficiente información física y/o virtual para determinar sobre la base de datos recolectados eventos
15 útiles para crear el sistema de administración global o en el sistema de administración de integridad eventos agrupados sin depender de ningún sistema externo, los eventos agrupados serán útiles para determinar acciones como notificaciones para identificar o alertar incidentes
20 de seguridad y otras acciones. Las definiciones de los eventos agrupados son administradas vía el módulo de sistema de administración global o en el sistema de administración de integridad como parte de la naturaleza del "aprendizaje" del sistema. El BRE almacena y pone en
25 fila de espera, cuando es necesario, esos datos y encripta

o firma cada dato para asegurar que los datos estén completos, sean auténticos, contables, no repudiados, y protegidos contra el acceso externo, modificación, perturbación y destrucción. Se apreciará que cualquiera de
5 una o más, ninguna o todas esas características pueden ser usadas, además de otra forma de funcionalidad. Entonces puede tenerse acceso a los datos encriptados por medio de sistemas externos sobre la base de, por ejemplo, perfiles de seguridad de peticiones de información del sistema.

10 La Figura 13 es una modalidad ejemplar de un flujo de proceso de la interfaz de acuerdo con una modalidad de la descripción. Los controladores de la interfaz de puerta de enlace recolectan datos de una fuente, incluyendo, pero sin limitarse a, fuentes físicas,
15 control lógico programable (PLC) y unidades terminales remotas (RTU) y cualquier otro tipo de fuente. El motor de reglas comerciales BRE procesa los datos, correlaciona los datos y crea a partir de los datos eventos o secuencias de eventos, como se describió con detalle anteriormente. Los
20 datos y eventos son firmados opcionalmente por un módulo de seguridad de hardware o software (HSM o SSM). Los eventos y datos mejorados pueden ser almacenados en un depósito o almacén de datos seguro. La puerta de entrada verifica entonces para determinar a dónde serán enviados los datos
25 (GMS disponibles), por ejemplo, al sistema de

administración global o en el sistema de administración de integridad u otro sistema externo. Si el sistema de administración global o el sistema de administración de integridad está disponible, entonces a los datos o eventos

5 se les da formato y son validados para ser usados por el sistema de administración global o en el sistema de administración de integridad. Los datos que vayan a un sistema externo pueden o no ser objeto de un formato y validados dependiendo de los requerimientos del sistema

10 externos. Los datos o eventos que estén siendo pasados a través de la puerta de enlace son enviados al módulo de integración de datos, el cual almacena los datos o los eventos, adquiere los datos del almacén, crea por ejemplo una estructura de datos de valor clave a partir de los

15 datos, clasifica los datos de la estructura y analiza los datos estructurados usando modelos y algoritmos computacionales para identificar la correlación entre datos útiles para la creación de eventos agrupados o un reporte de impuestos seguro confiable KPI seguro o ayuda para

20 propósitos de recolección de impuestos o recuperación de impuestos o corrección de asimetrías en el sistema de administración global o en el sistema de administración de integridad IMS. Los datos también son verificados por la integridad de datos estructurados y la seguridad de los

25 datos estructurados para prevenir la manipulación indebida.

La interfaz de datos puede ser una interfaz independiente o parte del sistema de administración de datos. Si se separan, los datos se hacen pasar entonces a lo largo del sistema de administración de datos para su procesamiento de acuerdo con las modalidades descritas anteriormente.

Los ejemplos y descripción siguientes se relacionan con el sistema de administración de suministro global o el sistema de administración de integridad (sistema de seguimiento) como una fuente de recolección de datos como una alternativa al uso de detectores o recolectores de datos. Es decir que, el dispositivo observador seguro (SOD) discutido anteriormente con respecto al sistema de administración de suministro global (seguimiento y rastreo) podría ser reemplazado por los detectores y recolectores de datos descritos con respecto al sistema de administración global o en el sistema de administración de integridad. Por ejemplo, en el sector midstream de la cadena de suministro, los datos seguros D pueden ser generados en una tubería usando los detectores para recolectar los datos, y los datos seguros D pueden ser generados observando y detectando combustible marcado en un camión. Por ejemplo, el marcado estará en el combustible (u otro activo) de modo que una verificación e inspección regular a lo largo de la ruta de un camión generará datos seguros D (los cuales pueden ser pasados a lo largo del

sistema de administración global o en el sistema de administración de integridad). Si, por ejemplo, la dilución de la concentración del producto (por ejemplo combustible), varía a lo largo de la tubería, los detectores (los cuales actúan como un dispositivo observador seguro (SOD)) generarán datos seguros D agregando un algoritmo seguro u otro atributo. Los datos seguros D también pueden ser generados sobre la base de un análisis del mercado del combustible de petróleo crudo contra los datos recolectados en la tubería, y pueden ser insertados en un ERP y pasados a la interfaz de la puerta de enlace. Los datos creados serán usados para crear eventos agrupados seguros dentro del sistema de administración de datos y útiles para crear alertas en el centro de control CCC para ambos sistemas GMS o IMS.

En otra modalidad, en lugar de marcar el producto (por ejemplo combustible), los detectores en la tubería actuarán con un dispositivo observador (SOD) junto con un detector clásico el cual mide los valores especificados y los envía al depósito. El detector enviará los datos con atributos encriptados o seguros, y verificará dos veces los datos antes de enviarlos como datos seguros para asegurarse de que los datos sean auténticos.

Otro ejemplo no limitante de datos seguros D creados ocurre en el sector downstream. Durante el proceso

de refinación, el cual es útil para crear combustible o petróleo, diferentes lotes de combustible pueden ser marcados de manera diferente. Únicamente un combustible correspondiente con un marcado seguro será enviado a una
5 región particular del país. En una modalidad, diferentes marcados químicos en diferentes lugares de diferentes canales de distribución conducen a diferentes minoristas. El marcado químico se basa, por ejemplo, en mezclas específicas de compuestos luminiscentes orgánicos e
10 inorgánicos (IR, IR Cercano, UV), representando cada mezcla específica una llave química específica. En otra modalidad, los diferentes grados o tipos de combustible tienen diferentes marcados. Capturando los datos, puede determinarse si la transacción reportada para un cierto
15 grado de combustible fue realmente para el producto físico correcto a detectar si alguien declaró, por ejemplo, transacciones para un producto de bajo gravamen cuando en realidad se hizo una transacción para un producto de alto gravamen.

20 La captura de datos usando un dispositivo observador seguro (SOD) proporcionará la capacidad de determinar si cualquier actividad ilegal, como el robo o desviación del producto, ha ocurrido durante el transporte. Por ejemplo, en una región de un país (por ejemplo,
25 Sinaloa), un combustible producido será marcado por los

compuestos A, B o C. El combustible marcado será entonces distribuido a una estación de gasolina en Sinaloa. En la región de Zacatecas, por otro lado, el combustible marcado con los compuestos D, E y F se desplazará a lo largo del camino hasta que alcance una estación de gasolina en Zacatecas. Si por alguna razón el combustible marcado con los compuestos marcados D, E y F es recuperado o encontrado en la estación de gasolina de Sinaloa, el sistema de administración global GMS (que ha recibido datos recolectados con respecto al combustible marcado) determinará que el producto ha sido manipulado de manera indebida en algún punto. Por ejemplo, se determinará que el combustible que era generalmente para entregarse en Zacatecas ha sido desviado (ilegalmente) a la región de Sinaloa. Igualmente, una tubería puede ser segregada de acuerdo a la región, y los datos seguros D generados en las regiones de la tubería serán capturados por el dispositivo observador seguro SOD. El sistema de administración global GMS a su vez será alertado sobre la base de eventos agrupados generados con datos seguros específicos D (vinculados con detectores en una región específica de una tubería). El sistema de administración global GMS será capaz de localizar con precisión dónde ocurrirán problemas en una región específica sobre la base de esta información.

Usando el sistema de administración de la cadena

de suministro global para rastrear, seguir y almacenar eventos seguros a lo largo de una cadena de suministro, la información almacenada puede ser almacenada en conjunto con el sistema de administración global GMS; y en particular, con el componente de puerta de enlace. En este contexto, por ejemplo, el sistema de administración de la cadena de suministro global actúa como un sistema industrial ICS para proporcionar esa información a la puerta de enlace o el módulo de integración de datos, como se ilustra en la Figura 8. Como se describió anteriormente, los datos recolectados de cualquier parte de la cadena de suministro de petróleo y gas serán usados para crear eventos adecuados (seguros), notificaciones y alertas en el sistema de administración global en el centro de control CCC y para actuar de manera prescriptiva o predictiva en el campo a nivel de intervención. Esas alertas, por ejemplo, son basadas y obtenidas como los resultados de los eventos agrupados que han sido desarrollados usando procesos de extracción, recolección histórica y verificación de datos y manipulación de datos basados en datos recolectados previamente.

La captura de los datos usando un dispositivo de observador seguro puede proporcionar la capacidad de determinar si cualquier actividad ilegal también tiene un impacto sobre la recolección de impuestos, y será detectada

por el IMS. Por ejemplo, la captura por SOD, del volumen de combustible entregado a una cisterna o un camión para una estación de gasolina también permitirá al sistema tener una estimación correcta del volumen transportado de la planta a la estación de la gasolina y el impuesto correspondiente que deberá ser recuperado por el estado. El volumen correlacionado con el mercado del combustible, como se describió anteriormente, y capturado también por un SOD, permitirá que cuando estaciones de gasolina específicas reciban un combustible específico marcado se estime qué cantidad de impuestos tendrá que pagar al estado la estación de gasolina correspondiente.

Los siguientes ejemplos resaltan la captura de datos e información de la cadena de suministro global que son pasados al sistema de administración global o en el sistema de administración de integridad. Debe apreciarse que los ejemplos no son limitantes.

Marcado del combustible: son usados diferentes marcados (por ejemplo diferentes composiciones químicas) de diferentes regiones y/o diferentes concentraciones de los marcados para marcar el producto, como combustible. Por ejemplo, el combustible con el marcado es transportado en una tubería o en tanques de un camión. Si una variación de la concentración del marcado en el combustible, o una presencia de otro líquido (como agua) es encontrada dentro

del combustible, el sistema (por ejemplo detectores o un dispositivo observador seguro (SOD)) detectará la variación y notificará la diferencia cuando el producto se desplace de una región a otra región. El SOD o detector puede ser
5 usado para capturar el combustible marcado y creará un evento o datos seguros, correspondientes para entregarlos al sistema de administración de la puerta de enlace (a la puerta de enlace o módulo de integración de datos). Esos datos serán entonces usados para detectar la falsificación,
10 desviación, hurto de material, robo, fraude fiscal, etc., como se describió anteriormente.

Verificación de la tubería: a nivel de la tubería, el producto (por ejemplo combustible) puede ser verificado usando detectores o detectores manuales (SOD).
15 Esos detectores son detectores seguros y pueden además reemplazar los detectores convencionales. Un detector convencional no es capaz de detectar cualquiera de los marcados en el producto, mientras que los detectores seguros pueden detectar esos marcados. En consecuencia,
20 cualquier dato recolectado por los detectores seguros puede ser agregado a los datos del detector convencional y verificado o comprobado por un módulo de seguridad de hardware HSM o SSM y enviar los datos verificados/comprobados de manera segura a la puerta de
25 enlace y/o módulo de integración de datos. Cada detector

puede ser único y envía eventos seguros y datos de manera segura. Por otro lado los datos recolectados del SOD son comprobados de manera redundante, o adquiridos varias veces y promediados y verificados para comprobar la exactitud de la información en los datos recolectados antes de ser transferidos a la puerta de enlace y/o el módulo de integración de datos. Adicionalmente, los datos pueden incluir una marca única que refleje su posición a lo largo de la tubería, y almacenados como tales en el depósito correspondiente o en los eventos agrupados generados a nivel del sistema de administración de datos en el sistema de administración global o en el sistema de administración de integridad. La recuperación de la información a lo largo de la tubería, junto con su ubicación, puede entonces ser lograda cuando ocurra un problema y/o mantenimiento a nivel de la tubería.

Verificación de la bomba de la estación de gasolina: la generación de eventos seguros también puede ocurrir para verificar el consumo y distribución de petróleo al nivel de estación de gasolina. Por ejemplo, cada bomba en la estación de gasolina puede ser equipada con un dispositivo observador seguro SOD, (por ejemplo detector), capaz de determinar el marcado dentro del combustible y transmitir la información de manera segura. Esto dará la certidumbre que para un mercado específico, la

estación de gas está autorizada para distribuir combustible (petróleo), asegurando por lo tanto la entrega apropiada y no adulterada del producto a la estación de gasolina. El SOD también puede ser usado para crear eventos y datos
5 seguros vinculados con el volumen de petróleo consumido o petróleo entregado en conjunto con la cantidad de petróleo vendido en la estación de gasolina. Estos datos, creados por el SOD pueden ser usados para varios propósitos, por ejemplo, incluyendo la recolección de impuestos y para
10 determinar si la cantidad de ingresos en la estación de gasolina y el volumen de petróleo entregado en los vehículos en la estación de gasolina son consistentes. Como en el ejemplo de la tubería, la información del SOD puede ser asegurada por el HSM o SSM y comunicada de manera única
15 seguramente con la puerta de enlace del módulo de integración de datos.

En consecuencia, la presente invención proporciona varios sistemas, servidores, métodos, medios y programas. Aunque la descripción ha sido descrita con
20 referencia a varias modalidades ejemplares, debe comprenderse que las palabras que han sido usadas son palabras de descripción e ilustración, más que palabras de limitación. Pueden hacerse cambios dentro del punto de vista de las reivindicaciones anexas, como se establece
25 actualmente y según son enmendadas, sin apartarse del

alcance y espíritu de la invención en sus aspectos. Aunque la invención ha sido descrita con referencia a medios, materiales y modalidades particulares, la invención no pretende ser limitada a los particulares descritos; más
5 bien la invención se extiende a todas las estructuras, métodos y usos funcionalmente equivalentes, que estén dentro del alcance de las reivindicaciones anexas.

Aunque el medio legible por computadora puede ser descrito como un solo medio, el término "medio legible por
10 computadora" incluye un solo medio o medios múltiples, como una base de datos centralizada o distribuida, y/o cambios de servidores asociados que almacenan uno o más conjuntos de instrucciones. El término "medio legible por computadora" también incluirá cualquier medio que sea capaz
15 de almacenar, codificar o contener un conjunto de instrucciones para su ejecución por un procesador o que hagan que un sistema de computadora realice cualquiera de una o más de las modalidades descritas aquí.

El medio legible por computadora puede comprender
20 un medio o medios legibles por computadora no transitorios y/o comprender un medio o medios legibles por computadoras transitorios. En una modalidad ejemplar, particularmente no limitante, el medio legible por computadora puede incluir una memoria de estado sólido, como una tarjeta de memoria u
25 otro paquete que aloje una o más memorias de sólo lectura

no volátiles. Además, el medio legible por computadora puede ser una memoria de acceso aleatorio u otra memoria reescribible volátil. Adicionalmente, el medio legible por computadora puede incluir un medio magnetoóptico u óptico, como un disco o cintas u otro dispositivo de almacenamiento para capturar señales de onda portadora como una señal comunicada sobre un medio de transmisión. En consecuencia, se considera que la descripción incluye cualquier medio legible por computadora u otros equivalentes y medios sucesores, en el los cuales pueden ser almacenados datos o instrucciones.

Aunque la presente solicitud describe modalidades específicas las pueden ser implementadas como segmentos de código en medios legibles por computadora, debe comprenderse que implementaciones de hardware dedicadas, como circuitos integrados específicos de la aplicación, arreglos lógicos programables y otros dispositivos de hardware, pueden ser contruidos para implementar una o más de las modalidades descritas aquí. Las aplicaciones que pueden incluir las diferentes modalidades expuestas aquí pueden incluir ampliamente una variedad de sistemas electrónicos de computadora. En consecuencia, la presente solicitud puede abarcar implementaciones de software, firmware y hardware, o combinaciones de las mismas.

Aunque la presente especificación describe

componentes y funciones que pueden ser implementadas en modalidades particulares, con referencia a estándares y protocolos particulares, la descripción no se limita a esos estándares y protocolos. Esos estándares son sustituidos
5 periódicamente por equivalentes más rápidos o más eficientes que tienen esencialmente las mismas funciones. En consecuencia, los estándares y protocolos de reemplazo que tienen las mismas o similares funciones son considerados equivalentes de los mismos.

10 Las ilustraciones de las modalidades descritas aquí pretenden proporcionar una comprensión general de las diferentes modalidades. Las ilustraciones no pretenden servir como una descripción completa de todos los elementos y características de los aparatos y sistemas que utilizan
15 las estructuras o métodos descritos aquí. Muchas otras modalidades pueden ser evidentes a aquellos expertos en la técnica tras la revisión de la descripción. Otras modalidades pueden ser utilizadas y derivadas de la descripción, de modo que las sustituciones y cambios
20 estructurales y lógicos pueden ser efectuadas sin apartarse del alcance de la descripción. Adicionalmente, las ilustraciones son meramente representativas y pueden no estar dibujados a escala. Ciertas proporciones dentro de las ilustraciones están exageradas, mientras que otras
25 proporciones pueden estar minimizadas. En consecuencia, la

descripción y las Figuras deben considerarse como ilustrativas más que restrictivas.

Una o más modalidades de la descripción pueden ser referidas aquí, individualmente y/o colectivamente, por el término "invención" meramente por conveniencia y sin pretender limitar voluntariamente el alcance de esta solicitud a ninguna invención o concepto inventivo particular. Además, aunque han sido ilustradas y descritas aquí modalidades específicas, deberá apreciarse que cualquier diseño de arreglo subsecuente para lograr el mismo o un propósito similar puede ser sustituido por las modalidades específicas mostradas. Esta descripción comprende cubrir cualesquiera y todas las adaptaciones o variaciones subsecuentes de varias modalidades. Las combinaciones de las modalidades anteriores, y otras modalidades no descritas específicamente aquí, serán evidentes al experto en la técnica tras la revisión de la descripción.

El Resumen de la descripción es proporcionado para cumplir con 37 CFR §1.72 (b) y es presentado comprendiendo que no será usado para interpretar o limitar el alcance o significado de las reivindicaciones. Además en la descripción detallada anterior, las diferentes características pueden ser agrupadas juntas o descritas en una sola modalidad para el propósito de ponerlas en línea

con la descripción. Esta descripción no debe ser interpretada como si reflejara la intención de que las modalidades reclamadas requieran más características que las expresamente expuestas en cada reivindicación. En su
5 lugar, como lo reflejan las siguientes reivindicaciones, la materia objeto inventiva puede ser dirigida a menos de todas las características de cualquiera de las modalidades descritas. De este modo, las siguientes reivindicaciones son incorporadas en la descripción detallada, con cada
10 reivindicación por sí misma definiendo materia objeto reclamada por separado.

La materia objeto descrita anteriormente debe ser considerada ilustrativa y no restrictiva, y las reivindicaciones anexas pretenden cubrir todas aquellas
15 modificaciones, mejoras y otras modalidades que caigan dentro del espíritu y alcance verdadero de la presente descripción. De este modo, en el grado máximo permitido por la ley, el alcance de la presente descripción, debe ser determinado por la interpretación más amplia permisible de
20 las siguientes reivindicaciones y sus equivalentes, y no deberá ser restringido o limitado por la descripción detallada anterior.