(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 655 137**

(51) Int. CI.:

H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.08.2012 E 12005971 (2)**

(97) Fecha y número de publicación de la concesión europea: **18.10.2017 EP 2701340**

(54) Título: **Método para monitorizar la operación de un sistema de energía eléctrica y sistema de monitorización**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.02.2018

(73) Titular/es:

OMICRON ELECTRONICS GMBH (100.0%)
Oberes Ried 1
6833 Klaus, AT

(72) Inventor/es:

KLIEN, ANDREAS y
MARINESCU, CRISTIAN

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método para monitorizar la operación de un sistema de energía eléctrica y sistema de monitorización

Campo de la invención

La invención se relaciona con un método y un sistema de monitorización para monitorizar el funcionamiento de un sistema de energía eléctrica. La invención se relaciona en particular a dicho método y sistema de monitorización que está configurado para realizar una monitorización de automatización de subestaciones para detectar un evento crítico, tal como una intrusión de seguridad, durante el funcionamiento del sistema de energía eléctrica.

Antecedentes de la invención

Los sistemas de energía eléctrica para altos y medios voltajes son ampliamente utilizados. La necesidad de transmitir potencia a distancias más largas, para realizar conversiones de voltaje en una subestación transformadora o distribuir energía requiere sistemas eléctricos complejos. En los últimos años, los llamados sistemas de automatización se han vuelto cada vez más populares, lo que aumenta el grado de automatización logrado en un sistema de energía eléctrica. Por ejemplo, las subestaciones para distribución de energía en redes de energía de alto y medio voltaje incluyen dispositivos primarios o de campo tales como cables eléctricos, líneas, barras colectoras, conmutadores, interruptores, transformadores de potencia y transformadores de instrumentos dispuestos en patios y/o bahías. Estos dispositivos primarios se pueden operar de forma automatizada a través de un sistema de automatización de subestación (SA) responsable del control, protección y monitorización de las subestaciones. El sistema SA comprende dispositivos secundarios programables, denominados dispositivos electrónicos inteligentes (IED), interconectados en una red de comunicación de SA e interactuando con los dispositivos principales a través de una interfaz de proceso. De manera similar, una amplia variedad de sistemas de energía eléctrica puede tener un sistema de automatización de la red de energía asociado que incluye IEDs que realizan funciones de control, protección y monitorización del funcionamiento del respectivo sistema de energía eléctrica. La comunicación entre los IEDs se puede realizar de acuerdo con protocolos estandarizados. A modo de ilustración, el estándar IEC 61850 "Redes y sistemas de comunicación en subestaciones" desacopla la funcionalidad de la aplicación específica de subestación de los problemas específicos de comunicación de la subestación y para esto, define un patrón de objeto abstracto para subestaciones compatibles y un método para acceder a estos objetos una red a través de una interfaz de servicio de comunicación abstracta (ACSI).

Con un grado cada vez mayor de automatización y con el uso creciente de IEDs, también existe una necesidad cada vez mayor de detectar con fiabilidad situaciones críticas en el sistema de automatización de la red de energía. Ejemplos de tales eventos críticos incluyen intrusiones de seguridad, errores del operador, problemas de temporización, fallas de hardware o cualquier estado crítico o incorrecto del sistema de energía eléctrica y/o su sistema de automatización de la red de energía.

Hadeli Hadeli et al.: "Generación de configuración para detector de tráfico faltante y medidas de seguridad en sistemas de control industrial con base en los archivos de descripción del sistema", TECNOLOGÍAS PARA LA SECURIDAD NACIONAL, 2009. HST ’09. EN CONFERENCIA IEEE, IEEE, PISCATAWAY, NEW JERSEY, ESTADOS UNIDOS, 11 de Mayo de 2009 (2009-05-11), páginas 503-510, ISBN: 978-1-4244-4178-5, el cual sirve de base para el preámbulo de las reivindicaciones independientes, se relaciona con un detector de tráfico faltante. Se puede extraer una hipótesis temprana sobre una violación de un patrón de tráfico predefinido, para detectar de ese modo una anomalía o intrusión.

El documento EP 1 850 447 A1 se relaciona con una inspección de configuración de IED. Los mensajes enviados por un IED se interceptan, se analizan mediante información de configuración sobre un sistema de automatización de subestación, y los datos extraídos analizados se muestran a un usuario.

El documento EP 2 109 204 A1 se relaciona con técnicas para un análisis de un sistema de automatización de subestaciones. Se capturan los mensajes que incluyen los valores primer y segundo de una cantidad de proceso. Se emite un indicador de discontinuidad que marca gráficamente un cambio en el valor de la cantidad de proceso. El documento EP 2 362 577 A1 se relaciona con técnicas de análisis de la configuración de comunicación para sistemas de automatización de subestaciones. Se generan representaciones gráficas de los IEDs emisores y receptores.

El documento de los Estados Unidos 2011/0196627 A1 describe métodos y dispositivos en los que se detectan transmisiones de datos en tiempo real y se pueden evaluar con relación a la información con respecto al tiempo. Dicho enfoque permite detectar situaciones críticas cuando, por ejemplo, se utilizan protocolos de comunicación que requieren mensajes que se transmiten entre IEDs para cumplir ciertos requisitos de temporización.

En el campo de las redes informáticas, los sistemas de detección de intrusiones (IDSs) se utilizan para monitorizar la red o la actividad de los sistemas con el fin de detectar intrusiones o actividades maliciosas de terceros no autorizados. Los IDSs están diseñados para identificar posibles incidentes, registrar información e informar posibles

intentos. La función principal de los IDS es alertar al operador del perímetro asegurado, para que pueda tomar medidas para impedir la intrusión, minimizar los impactos de los ataques o realizar análisis posteriores al incidente. Los IDS con base en la firma usan firmas predefinidas de ataques conocidos (como firmas de escáner de virus) para detectar intrusiones. Esto se puede ver como un enfoque de lista negra, donde el IDS alerta al operador si se observa un comportamiento que está explícitamente prohibido en el sentido de que está incluido en la lista negra.

Dichos enfoques con base en firmas son ampliamente utilizados para los IDS en los sistemas clásicos de tecnología de la información (IT). Si bien el enfoque de la lista negra se puede utilizar para detectar eventos críticos en los sistemas de automatización de la red de energía, puede haber problemas asociados con dicho enfoque. El enfoque de la lista negra requiere una firma para cada evento crítico que se debe identificar. Los ataques nuevos o desconocidos no pueden ser detectados. En el contexto de los sistemas de energía eléctrica, es muy baja la cantidad de ataques y vulnerabilidades conocidas para los sistemas de control y automatización y sus protocolos especiales. Por lo tanto, los IDS con base en listas negras aplicados a los sistemas de energía eléctrica serían, en gran medida, solo capaces de detectar ataques conocidos del dominio de IT. La utilidad de los enfoques de lista negra es, por lo tanto, especialmente limitada para IDS en sistemas de energía eléctrica.

Resumen de la invención

De acuerdo con esto, existe la necesidad de un método y sistema para monitorizar el funcionamiento de un sistema de energía eléctrica que tenga un sistema de automatización de la red de energía asociado, por ejemplo, un sistema de automatización de subestaciones. También existe la necesidad de dichos métodos y sistemas que no solo se basan en una lista de firmas de eventos críticos y, por lo tanto, también pueden detectar nuevos eventos críticos que no están incluidos en una lista negra.

De acuerdo con las realizaciones, se proporcionan un método y un sistema de monitorización como se define en las reivindicaciones independientes. Las reivindicaciones dependientes definen las realizaciones.

Se realiza un método de monitorización del funcionamiento de un sistema de energía eléctrica mediante un sistema de monitorización. El sistema de energía tiene un sistema de automatización de la red de energía. El sistema de automatización de la red de energía comprende una diversidad de dispositivos electrónicos inteligentes (IEDs) que se comunican a través de una red de comunicación. El sistema de monitorización usa información de configuración que especifica las propiedades de la diversidad de IEDs. El método comprende, durante el funcionamiento del sistema de potencia eléctrica, las propiedades de monitorización del sistema de potencia eléctrica, comprendiendo las propiedades monitorizadas los mensajes de datos monitorizados que se transmiten por la diversidad de IEDs a través de la red de comunicación. El método comprende evaluar los mensajes de datos monitorizados para detectar un evento crítico durante el funcionamiento del sistema de energía eléctrica, donde la evaluación comprende analizar un contenido de datos de al menos algunos de los mensajes de datos monitorizados para determinar, con base en la información de configuración, si el contenido de datos corresponde a un comportamiento válido. El método comprende generar una señal de alerta en respuesta a la detección de datos no conformes o el estado del sistema.

El método aprovecha el hecho de que los sistemas de energía eléctrica y sus sistemas de automatización son en gran medida deterministas. La cantidad de dispositivos, sus direcciones, protocolos e incluso los servicios que realiza el sistema de energía eléctrica en su conjunto se conocen de antemano y no cambian mucho con el tiempo.

En consecuencia, la información de configuración que especifica el comportamiento de los IEDs se usa para determinar si las propiedades del sistema monitorizado están en conformidad con la información de configuración. El sistema de monitorización puede verificar, con base en las propiedades monitorizadas, si las propiedades monitorizadas cumplen con la información de configuración. El sistema de monitorización usa un enfoque que no necesariamente requiere una lista negra que incluye firmas de eventos críticos. En lugar de esto, el sistema de monitorización usa la información de configuración para verificar, con base en la información de configuración, si los eventos observados son un comportamiento válido del sistema. De este modo, el sistema de monitorización identifica eventos que no están en conformidad con un patrón del sistema de energía eléctrica y su sistema de automatización de la red de energía.

El sistema de energía eléctrica puede ser o puede incluir una subestación.

El sistema de automatización de la red de energía puede ser o puede incluir un sistema de automatización de subestaciones.

El sistema de monitorización puede configurarse para realizar la monitorización de las propiedades de forma pasiva, sin interferir activamente con el funcionamiento de ninguno de los IEDs o componentes del sistema de energía eléctrica. El sistema de monitorización puede configurarse de modo que monitorice las propiedades sin enviar mensajes a uno de los IEDs durante el funcionamiento del sistema de energía eléctrica.

El sistema de monitorización puede generar un patrón del sistema para el sistema de energía eléctrica y su sistema de automatización de la red de energía con base en la información de configuración. El sistema de monitorización puede parecerse a un enfoque con base en una lista blanca que utiliza un patrón del sistema generado automáticamente para un sistema de energía eléctrica con especificaciones de comportamiento detalladas para juzgar si las propiedades monitoreadas están de acuerdo con el funcionamiento normal que se define por las especificaciones de comportamiento en el patrón del sistema.

El sistema de monitorización puede generar el patrón del sistema en función de la información de configuración y el conocimiento de la aplicación. El conocimiento de la aplicación puede incluir información sobre los protocolos de comunicación utilizados por los IEDs para comunicarse a través de la red de comunicación. El conocimiento de la aplicación puede incluir información sobre el funcionamiento del(los) protocolo(s) de comunicación. El conocimiento de la aplicación puede incluir información sobre cuándo y qué datos se transmiten de acuerdo con el(los) protocolo(s) de comunicación. El conocimiento de la aplicación puede incluir información sobre patrones de datos de IEDs u otros dispositivos, respectivamente para diferentes IED o dispositivos. El conocimiento de la aplicación puede incluir información sobre qué funciones son críticas. El conocimiento de la aplicación puede almacenarse en una base de datos, a partir de la cual el sistema de monitorización recupera información para generar el patrón del sistema.

El patrón del sistema generado debe cubrir las características de comunicación. El patrón del sistema generado puede definir qué IEDs se comunican entre sí y los parámetros de la comunicación respectiva. Además, el patrón del sistema también puede usar el conocimiento de la aplicación sobre el sistema de energía eléctrica. De este modo, el sistema de monitorización también está configurado para analizar el contenido de datos de los mensajes transferidos. El sistema de monitorización se puede configurarse para relacionar mensajes de datos de diferentes fuentes. Esto también puede incluir la observación de valores de medición transferidos digitalmente (por ejemplo, voltajes, formas de onda de señal, eventos binarios/activadores, que incluyen, entre otros, mensajes la IEC 61850).

Dado que los sistemas de automatización a menudo tienen requisitos en tiempo real, también las propiedades de tiempo de los mensajes pueden ser parte del patrón del sistema. El sistema no solo puede inspeccionar el tráfico de red y los valores de medición transferidos a través de la red, sino que también puede tener puertos de entrada eléctricos (análogos) para poder comparar las señales eléctricas del sistema de potencia con el patrón del sistema interno. El contenido de los datos de los mensajes de datos monitorizados y las señales eléctricas se pueden poner en relación directa y se pueden comparar con el patrón del sistema. El conocimiento de la aplicación se puede usar para generar el patrón del sistema.

El patrón del sistema puede incluir además información sobre la interconexión lógica entre los IEDs. Por ejemplo, el patrón del sistema puede incluir información sobre la topología del sistema de automatización de la red de energía. El patrón del sistema puede incluir además información sobre los conmutadores que se utilizan en la red de comunicación. Esto permite que el sistema de monitorización determine qué mensajes de datos se esperan en ciertas ubicaciones dentro de la red de comunicación para un comportamiento válido del sistema de automatización de la red de energía. El patrón del sistema puede incluir información sobre las capacidades de al menos los IEDs en el sistema de automatización de la red de energía. El patrón del sistema puede incluir información sobre los mensajes de datos transmitidos por los IEDs.

El patrón del sistema puede tener un formato que define un conjunto de restricciones que se imponen sobre el comportamiento válido del sistema de automatización de la red de energía mediante la información de configuración y/o el conocimiento de la aplicación. El conjunto de restricciones puede incluir restricciones con respecto a los mensajes de datos esperados en una determinada ubicación de la red de comunicación para la topología dada del sistema de automatización de la red de energía. Por ejemplo, un mensaje de datos a partir de un primer IED a un segundo IED monitorizado en una determinada ubicación de la red de comunicación representa un comportamiento válido solo si la topología define que el primer IED se comunica con el segundo IED y que los mensajes de datos pasan a cierta ubicación en que se monitoriza el mensaje de datos es. Para una mayor ilustración, un mensaje de datos enviado a un IED puede representar un comportamiento válido solo si le solicita al IED que realice una acción de acuerdo con sus capacidades y funciones. Dichas verificaciones pueden formularse como un conjunto de restricciones. Mediante el uso de un conjunto de restricciones para definir el patrón del sistema, el proceso de verificar si los mensajes de datos monitorizados corresponden a un comportamiento válido se puede realizar de manera eficiente.

El patrón del sistema puede proporcionar así una especificación para al menos el sistema de automatización de la red de energía, que incluye la red de comunicación. El patrón del sistema puede proporcionar una especificación tanto para el sistema de automatización de servicios públicos como para el sistema de energía eléctrica. El patrón del sistema permite que el sistema de monitorización monitorice el cumplimiento con la especificación según lo que se define por el patrón del sistema.

Si se detecta una desviación del comportamiento esperado de acuerdo con el patrón del sistema, se activa una alerta. Las desviaciones del comportamiento especificado no solo pueden ser causadas por intrusiones de seguridad, sino también por fallas de hardware, errores del operador, problemas de sincronización o errores de

configuración. Por lo tanto, el sistema de monitorización no solo está configurado para detectar intrusiones de seguridad, sino también cualquier estado crítico o incorrecto del sistema de energía eléctrica que pueda observarse a través de la red de comunicación. El sistema de monitorización es capaz de monitorizar la "salud" del sistema de automatización de la red de energía y alertar al operador si ocurren condiciones críticas.

El sistema de monitorización no solo puede usarse durante el funcionamiento normal del sistema de energía eléctrica, sino que también puede usarse durante la fase de configuración del sistema de automatización. El método puede comprender en consecuencia realizar pruebas de campo o de aceptación, con el fin de evaluar si el sistema de automatización de la red de energía se comporta o no según lo especificado en la información de configuración. Alternativamente o adicionalmente, el método puede usarse para evaluar si la información de configuración es correcta y corresponde al estado real del sistema. Alternativamente o adicionalmente, el método se puede usar para monitorizar el estado real y generar la información de configuración del tráfico de red real.

La etapa de evaluación puede comprender la predicción de mensajes de datos anticipados entre la diversidad de IEDs con base en el patrón del sistema, y la comparación de los mensajes de datos monitorizados con los mensajes de datos previstos anticipados. El conocimiento sobre el sistema de energía eléctrica y su sistema de automatización de la red de energía así como el comportamiento específico de estos sistemas se usa para determinar si el sistema de energía eléctrica y su sistema de automatización de la red de energía muestran un comportamiento esperado según el patrón del sistema.

La etapa de predicción puede comprender: predecir el contenido de datos de los mensajes de datos transmitidos por un IED con base en la información de configuración y con base en al menos un mensaje de datos previamente transmitido por al menos uno de la diversidad de IEDs. El contenido de datos de un mensaje de datos transmitido por un IED puede predecirse con base en la información de configuración y en función del contenido de datos de otro mensaje de datos previamente transmitido por el mismo IED. El contenido de datos de un mensaje de datos transmitido por un IED puede predecirse con base en la información de configuración y con base en el contenido de datos de otro mensaje de datos previamente transmitido por otro IED de la diversidad de IEDs. De este modo, el conocimiento de los componentes del sistema de energía eléctrica y su sistema de automatización de la red de energía asociada se puede utilizar para discriminar los eventos normales de los eventos críticos.

La etapa de evaluación puede comprender: determinar si la diversidad de IEDs se comporta según lo especificado por la información de configuración. Puede detectarse el evento crítico si la diversidad de IEDs no se comporta como lo especifica la información de configuración. Esta verificación se puede realizar sin requerir una lista negra de eventos críticos.

La información de configuración incluye información sobre los componentes de los sistemas de energía eléctrica y sus interconexiones. El paso de evaluación comprende: determinar si el sistema de potencia eléctrica y el sistema de automatización de la red de energía se comportan como se especifica en la información de configuración.

El sistema de monitorización puede tener un puerto de acceso de prueba de Ethernet (TAP) para monitorizar los mensajes de datos. El sistema de monitorización puede tener una diversidad de TAPs para controlar los mensajes de datos. Cuando la red de comunicación tiene una topología en estrella, como es el caso de muchas redes de comunicación conmutadas, la diversidad de TAPs puede proporcionarse respectivamente en las conexiones de datos entre los IEDs y el conmutador. Los TAPs pueden estar situados en diferentes ubicaciones en toda la red de comunicación y construir un TAP distribuido virtualmente.

Alternativamente o adicionalmente, el sistema de monitorización puede usar un conmutador de la red de comunicación para monitorizar los mensajes de datos. El sistema de monitorización puede tener una interfaz que funciona como un puerto espejo, y el conmutador puede configurarse para transmitir una copia de los mensajes de datos recibidos en el conmutador a partir de la diversidad de IEDs al puerto espejo en el sistema de monitorización. Alternativamente o adicionalmente, el sistema de monitorización puede estar integrado en un conmutador de la red de comunicación.

El método puede comprender una etapa de recepción, por el sistema de monitorización, de la información de configuración. El método puede comprender una etapa de procesamiento automático, por parte del sistema de monitorización, de la información de configuración recibida para generar el patrón del sistema.

La información de configuración recibida puede comprender al menos un archivo de datos de configuración del sistema de energía eléctrica y su sistema de automatización de la red de energía. El archivo de datos de configuración puede ser un archivo de lenguaje de descripción de la configuración de la subestación (SCL), como se usa para los sistemas que cumplen con la IEC 61850. El archivo SCL puede ser el archivo SCL para una subestación y su sistema de automatización de subestaciones.

Las propiedades monitorizadas pueden comprender además señales análogas del sistema de energía eléctrica. La etapa de evaluación puede comprender: evaluar tanto los mensajes de datos monitorizados como las señales análogas en función de la información de configuración para detectar el evento crítico. Las señales análogas pueden

compararse con la especificación del sistema de energía eléctrica y el sistema de automatización de la red de energía tal como se define en el archivo SCL.

El proceso para crear automáticamente un patrón del sistema de automatización de la red de energía puede combinar información de diferentes fuentes de datos. Se pueden usar los datos de configuración del sistema de energía eléctrica y sus componentes del sistema de automatización, como los archivos SCL, como se define en la IEC 61850-6.

Adicionalmente o alternativamente, la observación pasiva de la comunicación de red también se puede usar para generar el patrón del sistema. Dicha observación pasiva puede incluir la observación de la comunicación entre dispositivos del sistema de automatización de la red de energía y/o la observación de la comunicación entre el equipo de la red (por ejemplo, el protocolo de árbol de expansión rápida). Adicionalmente o alternativamente, la comunicación activa con dispositivos (por ejemplo, IEDs o equipo de red) también se puede usar para generar el patrón del sistema. Adicionalmente o alternativamente, los datos de configuración de los conmutadores de red pueden usarse para generar el modo del sistema. Dichos datos de configuración pueden incluir tablas MAC de los conmutadores. Alternativamente o adicionalmente, se puede usar la entrada del usuario. Por ejemplo, se puede recibir una entrada de usuario que define la ubicación de los sensores que proporcionan señales análogas a los puertos de entrada del sistema de monitorización.

En una implementación, el proceso para crear automáticamente un patrón del sistema puede comenzar con los archivos SCL u otros archivos de datos de configuración para determinar el patrón de datos interno de los dispositivos del sistema de automatización de la red de energía. Esto se puede usar para deducir el tipo de dispositivo, la información del proveedor y, por lo tanto, sus capacidades. También se puede determinar qué dispositivos se comunicarán entre sí y qué mensajes se esperan en ciertas ubicaciones del SAS. Como se conoce la función o el propósito de un dispositivo, también se puede deducir su criticidad, lo que permite la generación de ACLs (listas de control de acceso) para el patrón de datos de un dispositivo.

Esta información puede combinarse con la monitorización pasiva de la red para hacer coincidir el tráfico que se produce con los dispositivos del archivo de configuración con el fin de rellenar espacios de información (por ejemplo, la ubicación de un dispositivo en la red, información de direccionamiento). Durante la fase de configuración de la red de comunicación del sistema de automatización de la red de energía, la información generada a partir del archivo de configuración se puede comparar con el tráfico existente, para encargar la red o realizar pruebas de aceptación de campo o sitio. Además, los socios de comunicación no mencionados en el archivo de datos de configuración, como las estaciones de interfaz hombre-máquina, se pueden identificar y se pueden crear las especificaciones para estos dispositivos (por ejemplo, solicitando la entrada del usuario).

El método puede comprender una etapa de marcar en tiempo las propiedades monitorizadas y almacenar las propiedades monitorizadas marcadas en tiempo en respuesta a la detección del evento crítico. Esto permite que las propiedades monitorizadas se analicen posteriormente. Al almacenar selectivamente las propiedades monitorizadas con marcas de tiempo solo si se detecta un evento crítico, los requisitos de espacio de almacenamiento pueden mantenerse más moderados.

El método puede comprender además una etapa de generación, por el sistema de monitorización, de una lista negra que define firmas de estados de funcionamiento anormales. Las propiedades monitorizadas se pueden comparar con la lista negra, además de verificar el comportamiento del sistema frente a los datos de configuración, para detectar el evento crítico. El sistema de monitorización puede generar la lista negra en función de la información de configuración.

El método se puede usar para detectar una intrusión no autorizada. El sistema de monitorización puede operar como IDS. Alternativamente o adicionalmente, el método puede usarse para detectar fallas de hardware. Alternativamente o adicionalmente, el método puede usarse para detectar el error del operador. Alternativamente o adicionalmente, el método puede usarse para detectar errores de configuración durante una fase de configuración de la subestación o del sistema de automatización de la red de energía. Alternativamente o adicionalmente, el método puede usarse para detectar una violación de las políticas de seguridad, como el establecimiento de una conexión de datos entre un dispositivo informático no autorizado y el sistema de automatización de la red de energía.

El método se puede usar para monitorizar y analizar propiedades de un sistema de energía eléctrica para detectar y alertar sobre estados operativos críticos o intrusiones de seguridad.

Las propiedades monitorizadas pueden incluir el tráfico de red de un sistema de energía eléctrica o un sistema de automatización. La red analizada puede incluir una red de comunicación para transmitir datos relevantes de la potencia o del sistema de automatización.

El sistema de monitorización puede monitorizar el estado del sistema de energía eléctrica o el sistema de automatización de la red de energía mediante la monitorización del tráfico de la red y/o las señales eléctricas, análogas disponibles.

El sistema de monitorización puede operar como un sistema de detección de intrusos (IDS). El sistema de monitorización puede usar el conocimiento de la aplicación del sistema de potencia.

El análisis del tráfico de la red puede comprender un análisis pasivo del tráfico de la red para determinar si el sistema de potencia eléctrica o el sistema de automatización de la red de energía se comporta de acuerdo con la especificación.

El sistema de monitorización puede informar si el sistema de automatización de la red de energía se comporta o no según lo especificado por el patrón del sistema del sistema de automatización de la red de energía.

El sistema de monitorización también puede informar errores de configuración en la fase de configuración del sistema de potencia o automatización.

El sistema de monitorización puede detectar e informar intrusiones de seguridad con base en el conocimiento del sistema de potencia. Las decisiones se toman teniendo en cuenta el estado del sistema de potencia, los datos específicos de la aplicación, los patrones de comportamiento específicos, y/o similares, sin limitarse a ellos.

El sistema de monitorización puede detectar e informar errores de operador y fallas de hardware del sistema de potencia. La información recopilada puede tener un sello de tiempo y se puede usar para realizar análisis y depuración de eventos posteriores.

El sistema de monitorización puede combinar enfoques de IDS con base en listas negras (por ejemplo, con base en firmas) y en listas blancas dentro de un sistema, en donde el enfoque con base en listas blancas incluye la verificación de que los mensajes de datos monitorizados representan un comportamiento válido.

El sistema de monitorización puede configurarse para generar automáticamente el patrón del sistema para un IDS con base en lista blanca a partir de los datos de configuración del sistema de potencia. Los datos de configuración pueden incluir archivos SCL, sin limitarse a ellos.

El sistema de monitorización puede configurarse para generar automáticamente el patrón del sistema para un IDS con base en la firma a partir de los datos de configuración del sistema de potencia. Los datos de configuración pueden incluir archivos SCL, sin limitarse a ellos.

De acuerdo con otra realización, se proporciona un sistema de monitorización para un sistema de energía eléctrica, el sistema de energía eléctrica que tiene un sistema de automatización de la red de energía, el sistema de automatización de la red de energía que comprende una diversidad de dispositivos electrónicos inteligentes (IED) que se comunican a través de una red de comunicación. El sistema de monitorización comprende una interfaz para controlar, durante el funcionamiento del sistema de energía eléctrica, las propiedades del sistema de energía eléctrica, comprendiendo las propiedades monitorizadas mensajes de datos monitorizados que se transmiten por la diversidad de IEDs a través de la red de comunicación. El sistema de monitorización comprende un dispositivo de procesamiento configurado para evaluar los mensajes de datos monitorizados con base en la información de configuración para detectar un evento crítico durante el funcionamiento del sistema de energía eléctrica. El dispositivo de procesamiento está configurado para analizar el contenido de datos de al menos algunos de los mensajes de datos monitorizados para detectar el evento crítico. El dispositivo de procesamiento está configurado para generar una señal de alerta en respuesta a la detección del evento crítico.

El sistema de monitorización puede configurarse para realizar el método de cualquiera de los aspectos o formas de realización.

El sistema de monitorización puede comprender una diversidad de dispositivos de monitorización separados instalados en diferentes ubicaciones. Los dispositivos de monitorización pueden configurarse para comunicarse entre sí. El sistema de monitorización puede configurarse como un sistema distribuido. En dicha implementación distribuida del sistema de monitorización, los dispositivos de monitorización distribuidos del sistema de monitorización pueden sincronizarse a través de un protocolo de sincronización (tal como IEEE 1588, PTP, IRIG-B, etc.).

Características adicionales del sistema de monitorización y los efectos logrados corresponden por lo tanto a las características del método de acuerdo con las realizaciones. El procesamiento de la información de configuración y/o las propiedades monitorizadas pueden realizarse respectivamente por el dispositivo de procesamiento del sistema de monitorización.

De acuerdo con otra realización, se proporciona un sistema que comprende un sistema de energía eléctrica y el sistema de monitorización de un aspecto o realización. El sistema de energía eléctrica tiene un sistema de automatización de la red de energía, el sistema de automatización de la red de energía comprende una diversidad de dispositivos electrónicos inteligentes (IEDs) que se comunican a través de una red de comunicación.

Los métodos y sistemas de monitorización de realizaciones pueden usarse, en particular, para monitorizar sistemas de automatización de subestaciones durante el funcionamiento de la subestación. Los métodos y sistemas de monitorización de las realizaciones se pueden usar en particular para detectar intrusiones, sin limitarse a ellas.

Breve descripción de los dibujos

Las realizaciones de la invención se explicarán a continuación con referencia a los dibujos. A lo largo de los dibujos, los números de referencia similares se refieren a elementos similares.

La Figura 1 muestra, en forma de diagrama, elementos de un sistema de energía eléctrica en el cual se puede usar un sistema de monitorización y un método de realización.

La Figura 2 muestra, en forma de diagrama, una subestación en la cual se puede usar un sistema de monitorización y un método de realización.

La Figura 3 muestra, en forma de diagrama, aún otra subestación a modo de ejemplo en la cual se puede usar un sistema de monitorización y un método de realización.

La Figura 4 es un diagrama de bloques de un sistema de monitorización de acuerdo con una realización.

La Figura 5 es un diagrama de bloques que ilustra la generación de un patrón del sistema de acuerdo con las realizaciones.

La Figura 6 muestra una técnica mediante la cual un sistema de monitorización de una realización puede monitorizar mensajes de datos transmitidos por dispositivos de un sistema de automatización de la red de energía.

La Figura 7 es un diagrama de flujo de un método de una realización.

La Figura 8 ilustra mensajes de datos transmitidos por dispositivos de un sistema de automatización de la red de energía los cuales se evalúan por un sistema de monitorización de una realización.

La Figura 9 ilustra un diagrama de bloques funcional de un sistema de monitorización de una realización.

La Figura 10 ilustra un diagrama de flujo de un método de una realización.

La Figura 11 ilustra un sistema de automatización de la red de energía que tiene un sistema de monitorización de acuerdo con una realización.

La Figura 12 ilustra un sistema de automatización de la red de energía que tiene un sistema de monitorización de acuerdo con otra realización.

La Figura 13 ilustra un sistema de automatización de la red de energía que tiene un sistema de monitorización de acuerdo con otra realización.

Descripción de las realizaciones

Las realizaciones de la invención se describirán con más detalle con referencia a los dibujos. Aunque algunas de las realizaciones se describirán en contextos específicos, tales como subestaciones de un sistema de energía eléctrica que son transformadores o plantas de energía, los métodos y sistemas de monitorización no se limitan a estos contextos. Las realizaciones se pueden utilizar en particular para la operación de monitorización, y en particular para detectar intrusiones, en subestaciones de sistemas de energía eléctrica que tienen un sistema de automatización de la red de energía en forma de un sistema de automatización de subestación.

La Figura 1 a la Figura 3 muestran en forma esquemática y muy simplificada componentes fundamentales de un sistema de energía eléctrica en el que se puede usar un sistema 10 de monitorización de una realización.

En general, y como se explicará con más detalle a continuación, un sistema 10 de monitorización de una realización comprende una interfaz 11 para la comunicación con una red de comunicación de un sistema de automatización de la red de energía. Usando la interfaz, los mensajes de datos que se transmiten a través de la red de comunicación son recibidos y monitorizados. El sistema 10 de monitorización comprende un dispositivo 12 de procesamiento que procesa los mensajes de datos monitorizados. El dispositivo 12 de procesamiento puede evaluar al menos el contenido de algunos de los mensajes de datos monitorizados, para determinar si el sistema de energía eléctrica y su sistema de automatización de la red de energía muestran un comportamiento que está de acuerdo con un patrón 13 del sistema del sistema de automatización de la red de energía. El contenido de datos de los mensajes de datos monitorizados que se analiza mediante el dispositivo 12 de procesamiento del sistema 10 de monitorización incluye procesar parámetros de sistemas de energía eléctrica. El dispositivo 12 de procesamiento puede comprender un

procesador, puede comprender una diversidad de procesadores que se comunican entre sí, o puede incluir circuitos especiales. A modo de ilustración, el dispositivo 12 de procesamiento puede incluir una matriz de puertas programables de campo (FGPA) o múltiples FGPA que se comunican entre sí. El dispositivo 12 de procesamiento puede incluir uno o diversos procesadores de señal digital (DSPs). El patrón 13 del sistema puede almacenarse en un dispositivo de almacenamiento del sistema 10 de monitorización. El patrón 13 del sistema puede ser un patrón del sistema que incluye información sobre dispositivos en al menos el sistema de automatización de la red de energía, la comunicación entre estos dispositivos y las estructuras de datos de estos dispositivos. El patrón 13 del sistema puede ser un patrón del sistema que adicionalmente incluye información sobre elementos primarios del sistema de energía eléctrica. El sistema 10 de monitorización puede tener características adicionales, tales como puertos de entrada para recibir datos del sensor a partir del sistema de energía eléctrica. El sistema 10 de monitorización también puede configurarse para generar automáticamente el patrón 13 del sistema con base en un archivo de configuración para un sistema de automatización de la red de energía, por ejemplo, con base en un archivo de datos SCL.

La Figura 1 muestra, en forma diagramática y altamente simplificada, elementos de un subsistema de ejemplo de un sistema de potencia eléctrica. La potencia eléctrica fluye en la Figura 1 de izquierda a derecha, a partir de una planta 1000 de energía, una denominada "central eléctrica", a través de líneas 1501, 1502 de transmisión de alto voltaje a una planta 1600 transformadora, una denominada "estación transformadora". La energía eléctrica se produce en los generadores 1001 y 1002 y se transforma en alto voltaje en los transformadores 1201 y 1202 de salida. Estos transformadores de salida asociados con un generador también se denominan transformadores unitarios o transformadores de generador. La energía eléctrica pasa a partir de los transformadores 1201, 1202 unitarios a una barra 1401 colectora, a partir de donde se distribuye adicionalmente en las líneas 1501, 1502 de transmisión de alto voltaje. La línea 1501, 1502 de transmisión de alto voltaje está aquí en forma de una doble línea. En la práctica, en la mayoría de los casos esta doble línea se guía conjuntamente en un sistema de mástil. En la planta 1600 transformadora, las líneas 1501, 1502 entrantes se combinan de nuevo en una barra 1411 colectora. La potencia eléctrica presente en la barra 1411 colectora se transforma a un nivel de voltaje diferente mediante un transformador 1211 de salida y se entrega a una barra 1412 colectora. A partir de la barra 1412 colectora, la potencia se distribuye adicionalmente a través de las líneas 1701, 1702. La Figura 1 muestra un denominado diagrama de circuito equivalente de una sola línea. Sin embargo, el sistema de energía eléctrica es convencionalmente un sistema trifásico. De acuerdo con esto, los elementos que se muestran representan formas trifásicas; por ejemplo, la línea 1501 que se muestra como una línea en realidad consta de tres cables.

La producción, transmisión y distribución de la energía eléctrica tiene lugar en los denominados elementos primarios descritos anteriormente, es decir, los elementos principales guían las corrientes primarias y los voltajes primarios, que juntos se denominan parámetros primarios. Los elementos primarios juntos también se conocen como el sistema primario. Paralelo al sistema primario, existe otro sistema llamado secundario, que consiste en dispositivos de protección y control. Los elementos por encima de una línea 2000 divisoria simbólica en la Figura 1 pertenecen al sistema primario, a la vez que los elementos por debajo de la línea 2000 divisoria pertenecen al sistema secundario de protección y control. Los transformadores 1903, 1911, 1952 y 1961 ocupan una posición intermedia. Están conectados, por un lado, al sistema primario y, por otro lado, al sistema secundario y, en consecuencia, no se pueden clasificar de manera inequívoca.

Por debajo de la línea 2000 divisoria, se muestran diversos dispositivos de protección, por ejemplo, un sistema 2001 de protección de generador (GS), un sistema 2002, 2012 de protección diferencial de transformador (TS) y un sistema 2003, 2011, 2013 de protección de línea (LS). Solo los dispositivos de protección se muestran en la Figura 1 para mantener la claridad; los dispositivos de control estarían dispuestos en el mismo nivel. Los dispositivos de protección y control no pueden conectarse directamente a los elementos primarios que transportan alto voltaje para adquirir información sobre los parámetros en el sistema primario. Por lo tanto, los transformadores entregan imágenes estandarizadas de los parámetros primarios, los denominados parámetros secundarios, a los dispositivos de protección y control. Las relaciones de los transformadores 1903, 1911 de corriente, por ejemplo, son tales que entregan corrientes secundarias de 1A o 5A cuando la corriente nominal fluye en el sistema primario. Los transformadores 1952, 1961 de voltaje, por ejemplo, entregan un voltaje secundario de 100 V (en algunas partes del mundo también 110 V, 115 V, 120 V) con voltaje nominal en el sistema primario.

Otros elementos del sistema primario también se operan a través de los dispositivos de protección y control. En particular, cuando se identifica una falla, los dispositivos de protección pueden activar interruptores de circuito, por ejemplo, y así interrumpir el flujo de corriente. En la Figura 1, esto se muestra a modo de ejemplo para los dos dispositivos 2003 y 2011 de protección de línea y sus interruptores 1103 y 1111 de circuito asociados. Puede haber interruptores 1104 de circuito adicionales. Los interruptores 1103, 1111 de circuito pueden interrumpir el flujo de corriente a través de los elementos primarios. Esto también es cierto en particular en el caso de una falla, por ejemplo cuando fluyen corrientes de falla que exceden significativamente las corrientes normales de operación. No se muestran los interruptores de aislamiento, que también están presentes en instalaciones reales.

Los dispositivos de protección evalúan las corrientes y los voltajes y, cuando sea apropiado, también información adicional del sistema primario y secundario y determinan si está presente un estado operativo normal o un fallo. En caso de falla, una parte de la instalación identificada como defectuosa debe desconectarse lo más rápido posible

activando los interruptores automáticos correspondientes. Los dispositivos de protección pueden estar especializados para diferentes tareas. El sistema 2001 de protección del generador, además de evaluar las corrientes y los voltajes en el generador, también evalúa muchos otros parámetros. El sistema 2002, 2012 de protección diferencial de transformador aplica la regla nodal de Kirchhoff a las corrientes en el transformador 1201, 1211 de salida. El sistema 2003, 2011, 2013 de protección de línea puede examinar corrientes y voltajes en los extremos de línea y realiza por ejemplo, una medición de impedancia. También se puede proporcionar un sistema de protección de barras colectoras (no se muestra), que se puede usar para proteger las barras 1401, 1411, 1412 colectoras. Los dispositivos de protección pueden ser multifuncionales, es decir que pueden incorporar una diversidad de funciones de protección y también pueden llevar a cabo funciones de control (dispositivos combinados de protección y control).

Más recientemente, los dispositivos electrónicos inteligentes (IEDs) se han vuelto cada vez más populares. Como se muestra en la planta 1600 de transformador, se pueden proporcionar los IEDs 1981, 1984, 1991 y 1994. Estos IEDs tienen acceso a los parámetros principales y se comunican con los dispositivos de protección y control a través de protocolos de red. Los IEDs 1981, 1984, 1991 y 1994 se pueden conectar tan directamente como sea posible a los elementos principales. Las denominadas unidades 1981, 1984 de fusión digitalizan los valores medidos de los sensores 1961, 1964 de corriente y voltaje y los ponen a disposición de los dispositivos de protección como valores muestreados a través de una interfaz de red. Las unidades 1991, 1994 de control inteligentes detectan el estado de los elementos principales y accionan actuadores en los elementos principales. Los IEDs pueden comunicarse utilizando una red de comunicación. La comunicación entre los IEDs puede hacerse de acuerdo con un protocolo de comunicación. Por ilustración, la interconexión entre las unidades 1981, 1984 de fusión y los sistemas 2011, 2013 de protección de línea (LS) se puede realizar a través de una red de comunicación. De manera similar, la comunicación entre otros IEDs puede hacerse a través de una red de comunicación.

El patrón 13 del sistema del sistema de monitorización se puede generar con base en los datos de configuración para los IEDs del sistema de automatización de la red de energía. El patrón 13 del sistema puede incluir por ejemplo patrones de datos de los IEDs.

En el funcionamiento del sistema de energía eléctrica, el sistema 10 de monitorización monitoriza los mensajes de datos transmitidos por los IEDs. Los mensajes de datos son datos digitales generados de acuerdo con un protocolo, tal como IEC 61850, sin limitarse a este. El sistema 10 de monitorización verifica, con base en el patrón 13 del sistema, si el sistema de automatización de la red de energía muestra una operación como se esperaba de acuerdo con el patrón del sistema. Si se detecta una desviación del comportamiento esperado que se define por el patrón 13 del sistema, el sistema 10 de monitorización puede generar una señal de alerta.

Adicionalmente o alternativamente, pueden usarse IED adicionales o alternativos en el sistema de automatización de la red de energía, como se ilustra en la Figura 2.

La Figura 2 muestra una subestación configurada como una planta transformadora, en la cual se han reemplazado interfaces aún más convencionales. Con ese fin, los IEDs 1981-1984, 1991-1994 que, por un lado, tienen acceso a los parámetros principales y, por otro lado, se proporcionan los dispositivos de protección y control a través de protocolos de red. La Figura 2 muestra una arquitectura de este tipo para el sistema de conmutación de la Figura 1. Las unidades 1981-1984 fusionadas digitalizan los valores medidos de los sensores 1911-1914, 1961 y 1964 de corriente y voltaje y los ponen a disposición de los dispositivos de protección como valores muestreados a través de una interfaz de red. Los sensores pueden basarse en los principios físicos deseados. Un protocolo estandarizado entre la unidad de fusión y el dispositivo de protección establece la interoperabilidad. Los valores muestreados pueden ser, por ejemplo, valores muestreados de acuerdo con la norma IEC 61850 o de acuerdo con la guía de implementación "Guía de implementación para la interfaz digital para transformadores de instrumento usando IEC 61850-9-2". Las unidades 1991-1994 de control inteligente detectan estados de los elementos principales y accionan actuadores en los elementos primarios. La Figura 2 muestra, a modo de ejemplo, dispositivos de control de interruptores en los que los estados detectados son el ajuste del interruptor y, por ejemplo, la capacidad de corte instantáneo y los actuadores accionados son las bobinas de disparo y los dispositivos de conmutación. Con el fin de transmitir estados detectados a los dispositivos de protección y control o para recibir comandos a partir de los dispositivos de protección y control, las unidades de control inteligentes también utilizan protocolos a través de interfaces de red. Los telegramas controlados por eventos, cuyo contenido de información se actualiza y transmite únicamente cuando cambian los estados y comandos, son adecuados para el intercambio de dicha información. Dichos telegramas controlados por eventos pueden ser, por ejemplo, los denominados mensajes GANSO de acuerdo con la norma IEC 61850.

A la vez que en la Figura 2 se intercambia información entre las unidades 1981-1984 de fusión y las unidades 1991-1994 de control inteligentes, por un lado, y los dispositivos 2011-2013 de protección y control, por otro lado, a través de conexiones punto a punto, la Figura 3 muestra una arquitectura en la que se recoge y se distribuye la información y a través de otra red 2211. La red 2211 también se denomina "bus de proceso", a la vez que una red 2111 también se denomina a menudo "bus de estación". La distinción entre estas redes (buses) y la naturaleza de la información intercambiada no siempre es totalmente nítida e inequívoca. De este modo, los mensajes accionados por eventos (mensajes GANSO) se pueden usar igualmente de manera conveniente en el bus de estación, incluso en

arquitecturas de acuerdo con la Figura 1. Incluso es posible fusionar el bus de proceso y el bus de estación en una red física si se puede gestionar el tráfico de datos. En cualquier caso, la red 2211 proporciona relaciones de comunicación más significativas que las establecidas mediante las conexiones punto a punto de la Figura 2. Por lo tanto, se hacen posibles nuevas aplicaciones para las funciones de protección y control. Por ejemplo, el sistema 2012 de protección de transformadores podría examinar los voltajes en las barras 1411 y 1412 de bus a través de los valores muestreados de las unidades 1981 y 1984 de fusión y hacer que la conexión del transformador 1211 dependa de su fase mutua.

Para los sistemas de energía eléctrica y los sistemas de automatización asociados que se ilustran en la Figura 2 y la Figura 3, el sistema 10 de monitorización puede controlar nuevamente las propiedades del sistema de potencia eléctrica. Las propiedades monitorizadas pueden incluir mensajes de datos transmitidos por los IEDs. El sistema de monitorización puede aplicarse en la red de comunicación de un sistema de potencia como se representa en el ejemplo en la Figura 3, donde la interfaz 11 del sistema de monitorización actúa como un sensor de comunicación. El sensor de comunicación está acoplado al bus 2211 de proceso y al bus 2111 de estación. El sistema descrito aquí puede usar sensores de comunicación para observar el bus de estación y la comunicación del bus de proceso. Sensores adicionales podrían monitorizar señales eléctricas, como parámetros secundarios. El patrón 13 del sistema del sistema de monitorización se puede generar con base en los datos de configuración para los IEDs del sistema de automatización de la red de energía. El patrón 13 del sistema puede incluir nuevamente patrones de datos de los IEDs, por ejemplo. En funcionamiento de la subestación respectiva, el sistema 10 de monitorización monitoriza los mensajes de datos transmitidos por los IEDs. El sistema 10 de monitorización verifica, con base en el patrón 13 del sistema, si el sistema de automatización de la red de energía muestra una operación como se esperaba de acuerdo con el patrón del sistema. Si se detecta una desviación del comportamiento esperado que se define por el patrón 13 del sistema, el sistema 10 de monitorización puede generar una señal de alerta. El sistema 10 de monitorización puede detectar si el estado real del sistema corresponde al patrón del sistema.

La Figura 4 muestra un diagrama de bloques esquemático de un sistema 10 de monitorización de una realización. El sistema 10 de monitorización incluye una interfaz 11 para recibir mensajes de datos transmitidos por un IED a otro IED. La interfaz 10 puede ser una interfaz de red. El sistema 10 de monitorización comprende un dispositivo 12 de procesamiento que evalúa los mensajes de datos monitorizados y, opcionalmente, otras propiedades del sistema de energía eléctrica. La evaluación de los mensajes de datos incluye la evaluación del contenido de datos de al menos algunos de los mensajes de datos monitorizados. El contenido de datos incluye los parámetros de proceso de los componentes principales del sistema de energía eléctrica. De este modo, el dispositivo 12 de procesamiento puede determinar si el sistema de energía eléctrica y el sistema de automatización de la red de energía se comportan de acuerdo con el patrón 13 del sistema. Si el sistema 10 de monitorización detecta un comportamiento que no está de acuerdo con el patrón 13 del sistema, se puede generar una señal de alerta.

El dispositivo 12 de procesamiento puede usar el patrón 13 del sistema para determinar si el contenido de datos de dos mensajes de datos transmitidos por diferentes IEDs del sistema de automatización de la red de energía está de acuerdo con el patrón 13 del sistema. El dispositivo 12 de procesamiento puede poner mensajes de diferentes IEDs en relación entre sí. Por ejemplo, un parámetro de proceso de un elemento primario que se incluye en el mensaje de datos transmitido por un primer IED puede usarse para predecir qué valor para otro parámetro de proceso debe incluirse en otro mensaje de datos transmitido por un segundo IED. De este modo, se puede usar el comportamiento determinista del sistema de potencia eléctrica y el sistema de automatización de la red de energía. Se puede usar una amplia variedad de otras implementaciones en las que el sistema 10 de monitorización usa la información de configuración del sistema de automatización de la red de energía para verificar si las propiedades monitorizadas corresponden al comportamiento normal del sistema o al comportamiento anormal del sistema. En este último caso, se puede activar una señal de alerta.

El dispositivo 12 de procesamiento puede evaluar información adicional para verificar si el sistema de potencia eléctrica y el sistema de automatización de la red de energía muestran un comportamiento que está de acuerdo con el patrón del sistema. A modo de ilustración, el sistema 10 de monitorización puede tener uno o diversos puertos 15 de entrada para recibir señales análogas. Estas señales análogas del sistema de potencia también pueden verificarse contra el patrón del sistema interno que se define por el patrón 13 del sistema.

El patrón 13 del sistema puede generarse automáticamente con base en la información de configuración. La información de configuración se puede recibir monitorizando mensajes de datos entre IEDs o puede incluirse en al menos un archivo de datos que se proporciona al sistema de monitorización. Se puede usar otra información para generar el patrón 13 del sistema con base en la información de configuración. En particular, el conocimiento de la aplicación que define el funcionamiento de uno o diversos protocolos de comunicación utilizados por los IEDs y/o las capacidades de diferentes IEDs puede combinarse con la información de configuración para generar el patrón 13 del sistema. El conocimiento de la aplicación puede almacenarse en una base de datos para usar en la generación del patrón 13 del sistema.

La Figura 5 ilustra la generación del patrón del sistema. El sistema de monitorización usa la información 16 de configuración y puede combinar la información 16 de configuración con el conocimiento 17 de la aplicación para generar el patrón 13 del sistema. El sistema de monitorización puede recibir la información 16 de configuración de

cualquiera de una variedad de formas. Para ilustración, un archivo de datos de configuración del sistema de automatización de la red de energía puede proporcionarse al sistema de monitorización como información 16 de configuración. Alternativamente o adicionalmente, el sistema de monitorización puede controlar mensajes de datos transmitidos por IEDs durante una fase de configuración o durante la operación para adquirir la información 16 de configuración. El conocimiento de la aplicación 17 puede incluir información sobre el (los) protocolo (s) de comunicación que utilizan o utilizan los IED. El conocimiento 17 de la aplicación también puede incluir información sobre las funcionalidades y capacidades del dispositivo, para cada uno de la diversidad de diferentes IEDs. Esta información puede almacenarse en el conocimiento 17 de la aplicación como una función del vendedor y el identificador del dispositivo, por ejemplo.

El patrón 13 del sistema puede generarse de manera que incluya la información 131 en la interconexión lógica entre los IEDs. Es decir, el patrón del sistema puede incluir información 131 acerca de la topología del sistema de automatización de la red de energía. El patrón del sistema puede incluir además información sobre los conmutadores que se utilizan en la red de comunicación. Esto permite que el sistema de monitorización determine qué mensajes de datos se esperan en ciertas ubicaciones dentro de la red de comunicación para un comportamiento válido del sistema de automatización de la red de energía. El patrón 13 del sistema puede incluir información 132 sobre la funcionalidad y capacidades de al menos los IEDs en el sistema de automatización de la red de energía. El patrón del sistema puede incluir información 133 sobre los mensajes de datos transmitidos por los IEDs.

El patrón 13 del sistema puede tener un formato que define un conjunto de restricciones que se imponen sobre el comportamiento válido del sistema de automatización de la red de energía mediante la información de configuración y/o el conocimiento de la aplicación. El conjunto de restricciones puede incluir restricciones con respecto a los mensajes de datos esperados en una determinada ubicación de la red de comunicación para la topología dada del sistema de automatización de la red de energía. Para ilustración, un mensaje de datos a partir de un primer IED a un segundo IED monitorizado en una determinada ubicación de la red de comunicación representa un comportamiento válido solo si la topología define que el primer IED se comunica con el segundo IED y que los mensajes de datos pasan a cierta ubicación en que se monitoriza el mensaje de datos. Para una ilustración adicional, un mensaje de datos enviado a un IED puede representar un comportamiento válido solo si le solicita al IED que realice una acción de acuerdo con sus capacidades y funciones. Dichas verificaciones pueden formularse como un conjunto de restricciones. Al usar un conjunto de restricciones para definir el patrón del sistema, el proceso de verificar si los mensajes de datos monitorizados corresponden a un comportamiento válido se puede realizar de manera eficiente.

Para cualquier mensaje de datos que se identifique como que representa un comportamiento válido del sistema, el mensaje de datos puede analizarse con base en una diversidad de restricciones. Por ejemplo, el mensaje de datos puede analizarse para determinar si cumple con una restricción con respecto a la topología del sistema (por ejemplo, que el mensaje de datos se espere en la ubicación donde fue monitorizado), si cumple con otra restricción con respecto a la funcionalidad del IED (por ejemplo, que el IED receptor pueda realizar realmente la función solicitada por el mensaje de datos), y si cumple con otra restricción con respecto a la estructura de los mensajes de datos (por ejemplo, que el contenido de datos esté en conformidad con el protocolo de comunicación). El contenido de datos del mensaje de datos puede usarse para determinar si el mensaje de datos cumple con la restricción con respecto a la funcionalidad IED y la restricción con respecto a la estructura de los mensajes de datos. Se pueden usar más de tres restricciones para analizar el mensaje de datos.

El patrón 13 del sistema puede generarse de manera que defina un conjunto de restricciones que se utilizan para verificar si el mensaje de datos monitorizado está en conformidad con las restricciones.

A la vez que un sistema 10 de monitorización implementado como un único dispositivo se ilustra en la Figura 4, el funcionamiento del sistema 10 de monitorización también puede implementarse en un sistema distribuido que comprende una diversidad de dispositivos físicos separados. La diversidad de dispositivos puede instalarse en diversas ubicaciones en el sistema de automatización de la red de energía, lo que ayuda a controlar diferentes vistas de tráfico de la red. Los dispositivos distribuidos pueden sincronizarse entre sí, e idealmente también para el sistema o la subestación de energía eléctrica. Los dispositivos distribuidos del sistema de monitorización pueden comunicarse a través de la red de comunicación del sistema de monitorización. Los dispositivos distribuidos del sistema de monitorización se pueden sincronizar entre sí y con el sistema de automatización de la red de energía mediante cualquier protocolo adecuado, tal como IEEE 1588, técnicas de pulso por segundo o IRIG-B. Un dispositivo de reloj que genera una señal de reloj puede ser, por ejemplo, el dispositivo de reloj de la subestación. El análisis de fallas se facilita usando dicha sincronización. Además, se logra el orden cronológico utilizado para identificar el comportamiento válido del sistema.

Las redes de bus de proceso y de bus de estación no necesitan ser topologías físicas de bus, pero con frecuencia pueden ser topologías físicas estrella construidas usando conmutadores de red. En este caso, los sensores de comunicación del sistema de monitorización pueden aplicarse utilizando un puerto de acceso de prueba de Ethernet (TAP) o configurando conmutadores de red de automatización para enviar una copia de todo el tráfico de red a un puerto espejo. La interfaz 11 del sistema de monitorización puede estar conectada en el puerto espejo.

La Figura 6 ilustra dicha configuración. El TAP o el conmutador 23 se proporciona en las líneas 21, 22 de red. Las líneas 21, 22 de red pueden ser líneas de un bus de proceso o de un bus de estación. El TAP o el conmutador 23 envían una copia de todo el tráfico de la red al sensor 24 de comunicación, que es un puerto espejo para el tráfico de la red. El sensor 24 de comunicación puede ser la interfaz 11 o puede estar conectado a la interfaz 11 del sistema 10 de monitorización.

Otras realizaciones pueden implementar directamente un conmutador de red o funcionalidad TAP dentro de un dispositivo para poder observar el tráfico de red sin un TAP separado. Es decir, el funcionamiento del sistema 11 de monitorización puede integrarse en un conmutador del bus de proceso o la red de bus de estación. Se pueden usar diversos de dichos conmutadores de red o dispositivos TAP que tienen funciones integradas para monitorizar el funcionamiento del sistema de automatización de la red de energía. Estos dispositivos pueden estar sincronizados entre sí.

Como no se puede acceder a todo el tráfico de red a partir de una sola ubicación, también se pueden aplicar diferentes dispositivos físicos del sistema de monitorización o sus sensores, varias veces dentro de un sistema de energía eléctrica. Los dispositivos implementados pueden entonces cooperar para formar un sistema de monitorización distribuido.

La Figura 7 es un diagrama de flujo de un método 30 de una realización. El método 30 puede realizarse automáticamente usando un sistema de monitorización de una realización. El método 30 puede realizarse para detectar eventos críticos durante el funcionamiento de un sistema de potencia eléctrica y su sistema de automatización de la red de energía.

En la etapa 31, se genera un patrón del sistema de al menos el sistema de automatización de la red de energía. El patrón del sistema se puede basar en la información de configuración para una diversidad de IED del sistema de automatización de la red de energía. El patrón del sistema también puede definir elementos principales del sistema de energía eléctrica. El patrón del sistema puede ser un patrón del sistema que describe el comportamiento del sistema de automatización de la red de energía.

El sistema de monitorización puede generar el patrón del sistema automáticamente y en función de un archivo de configuración del sistema de automatización de la red de energía. La etapa 31 para crear automáticamente el patrón del sistema de automatización de la red de energía puede combinar información de diferentes fuentes de datos, tales como, pero no se limitan a:

- Datos de configuración del sistema de potencia y sus componentes del sistema de automatización (como archivos SCL, como se define en el IEC 61850-6);

- Observación pasiva de la comunicación de red, tal como comunicación entre dispositivos del sistema de automatización y/o comunicación entre equipos de red (por ejemplo, Protocolo de árbol de expansión rápida);

- Comunicación activa con dispositivos (por ejemplo, IEDs o equipos de red);

- Datos de configuración de los conmutadores de red (si son accesibles, por ejemplo, tablas MAC); o

- Entrada del usuario.

En algunas implementaciones, la etapa 31 de creación automática del patrón del sistema de automatización de la red de energía puede comenzar con los archivos SCL u otros archivos de configuración para determinar el patrón de datos interno de los IEDs. Esto se puede usar para deducir el tipo de dispositivo, la información del proveedor y, por lo tanto, sus capacidades. La búsqueda de tabla se puede usar para deducir el tipo de dispositivo u otra información similar con base en el archivo de configuración. El sistema de monitorización también puede determinar qué dispositivos se comunicarán entre sí y qué mensajes se esperan en ciertas ubicaciones del SAS. Dado que se conoce la función y el propósito de un IED, también se puede deducir su criticidad, lo que permite la generación de ACLs (listas de control de acceso) para el patrón de datos de un dispositivo.

Esta información se puede combinar con la monitorización pasiva de la red para hacer coincidir el tráfico que se produce con los IEDs del archivo de configuración con el fin de rellenar espacios de información (por ejemplo, la ubicación de un dispositivo en la red, información de direccionamiento). Durante la fase de configuración de la red SAS, la información generada a partir del archivo de configuración se puede comparar con el tráfico existente actualmente, para encargar la red o para ejecutar pruebas de aceptación de campo o sitio. La entrada del usuario puede definir una configuración adicional de la red de energía eléctrica o el sistema de automatización de la red de energía que no se incluye en el archivo de configuración. A modo de ejemplo, pueden identificarse los socios de comunicación no mencionados en el archivo de configuración, como las estaciones de interfaz hombre-máquina, y pueden crearse las especificaciones para estos dispositivos a través de una entrada de usuario dedicada.

La generación del patrón del sistema en la etapa 31 también se puede realizar de forma diferente. Por ejemplo, la monitorización pasiva de la red durante una fase de configuración puede usarse para generar el patrón del sistema sin requerir los archivos de configuración.

En 32, se recuperan los mensajes de datos transmitidos por IEDs en la red de comunicación. Para una red de comunicación que tiene una topología estrella, esto se puede hacer usando cualquiera de las técnicas descritas con referencia en la Figura 6.

En 33, se determina el contenido de datos de los mensajes de datos. El contenido de datos puede incluir información diferente de la información de dirección del IED transmisor y receptor. El contenido de datos incluye un parámetro de proceso de un elemento primario del sistema de energía eléctrica.

En 34, se determina si el contenido de datos coincide con el patrón del sistema. Si el contenido de datos coincide con el patrón del sistema, se determina que el comportamiento del sistema es normal. El método vuelve a la monitorización en el paso 32. De lo contrario, se genera una señal de alerta en el paso 35. El método puede entonces volver al paso 32 para continuar la monitorización.

Se puede evaluar información adicional en el método de monitorización de la Figura 7. A modo ilustrativo, los valores análogos recibidos por el sistema de monitorización en puertos de entrada análogos también pueden evaluarse para determinar si están en conformidad con el comportamiento esperado de acuerdo con la especificación del sistema.

Los sistemas de monitorización y los métodos de monitorización de las realizaciones pueden analizar el contenido de los mensajes transferidos y pueden poner en relación mensajes de diferentes fuentes.

La Figura 8 ilustra los mensajes 41, 44 y 47 de datos monitorizados por el sistema de monitorización de una realización. Los mensajes 41 y 47 de datos se transmiten por un IED del sistema de automatización. El mensaje 44 de datos se transmite por otro IED. El mensaje 41 de datos incluye datos 42 de encabezado, que pueden incluir un identificador para el IED transmisor y receptor. El mensaje 41 de datos incluye además el contenido 43 de datos. De manera similar, el mensaje 44 de datos incluye datos 45 de encabezado, que pueden incluir un identificador para el IED transmisor y receptor. El mensaje 44 de datos incluye además el contenido 46 de datos. El mensaje 47 de datos incluye datos 48 de encabezado, que pueden incluir un identificador para el IED transmisor y receptor. El mensaje 47 de datos incluye además el contenido 49 de datos.

El contenido 43, 46 y 49 de datos, de los mensajes de datos respectivamente se relaciona con los parámetros del proceso del sistema de energía eléctrica. Por ejemplo, el contenido de datos de algunos mensajes de datos puede incluir valores de medición transferidos digitalmente, por ejemplo, voltajes, señales en formas de onda, señales binarias o eventos desencadenantes.

Los sistemas y métodos de monitorización de cualquier realización pueden usar el contenido 43 de datos de un mensaje 41 de datos transmitido por un IED para determinar si el contenido 46 de datos del mensaje 44 de datos transmitido por otro IED corresponde a un comportamiento válido del sistema. El patrón del sistema se utiliza para establecer el contenido 43, 46 de datos de los mensajes 41, 44 de datos transmitidos por diferentes IED con relación entre sí. De manera similar, el contenido 46 de datos del mensaje 44 de datos se puede usar para determinar si el contenido 49 de datos del mensaje 47 de datos corresponde a un comportamiento válido del sistema.

Los sistemas y métodos de monitorización de las realizaciones pueden usar no solo el contenido de datos, sino también el tiempo de las transmisiones de datos para verificar si el comportamiento del sistema es normal, es decir, que no ha ocurrido ningún evento crítico. Por ejemplo, la velocidad a la que un IED transmite mensajes de datos puede depender del valor de un parámetro de proceso. Las velocidades de transmisión para diversos valores de parámetros de proceso o rangos de valores de parámetros de proceso pueden incluirse en los datos de configuración para el IED respectivo, el cual se usa para generar el patrón del sistema. Esto permite que los sistemas y métodos de monitorización también identifiquen eventos críticos con base en la temporización de los mensajes de datos transmitidos, cuando la temporización se evalúa con base en el patrón del sistema y el contenido de datos de un mensaje de datos transmitido por un IED.

De regreso a la Figura 8, un intervalo 50 de tiempo o velocidad de transmisión a la que un IED transmite los mensajes 41 y 47 de datos, puede variar dependiendo de un parámetro de proceso del sistema de potencia eléctrica. El sistema de monitorización puede determinar un valor del parámetro del proceso en función del contenido de datos de un mensaje de datos transmitido por uno de los IEDs. El sistema de monitorización puede usar el patrón del sistema para determinar a qué intervalos 50 de tiempo deben transmitirse mensajes de datos para este valor del parámetro del proceso. El sistema de monitorización puede verificar si los mensajes 41 y 47 de datos se transmiten a la temporización esperada. Con base en esto, se puede determinar si el sistema se encuentra en su estado de operación normal.

Los sistemas y métodos de monitorización y de las realizaciones pueden usar enfoques del tipo lista negra para detectar eventos críticos, además de una verificación del comportamiento normal del sistema con base en patrón del

sistema de automatización de la red de energía. Esto puede ser beneficioso en particular cuando el sistema de automatización de subestaciones también utiliza tecnologías y protocolos IT clásicos. Estos a menudo muestran un comportamiento no determinista que no se puede especificar con suficiente detalle. Los sistemas de monitorización y los métodos de realización pueden, por lo tanto, usar adicionalmente métodos tradicionales de detección de intrusos con base en listas negras para detectar ataques de seguridad dirigidos a aquellas tecnologías IT clásicas.

La Figura 9 esboza la estructura lógica de dicho sistema de monitorización, y la Figura 10 es un diagrama de flujo de un método realizado por dicho sistema de control.

La Figura 9 muestra un diagrama de bloques funcional de un sistema 60 de monitorización de una realización. El sistema 60 de monitorización funciona en general con base en un patrón del sistema 62 del sistema de automatización de la red de energía y con base en las firmas 64 de eventos críticos. Las intrusiones son un ejemplo de eventos críticos para los cuales se pueden almacenar las firmas 64. Las firmas 64 pueden formar una lista negra, de modo que se detecta un evento crítico y se activa una alerta cuando se observa una de las firmas 64 en el sistema de automatización de la red de energía.

El sistema 60 de monitorización tiene un componente 61 de recopilación de datos. El componente 61 de recopilación de datos puede recibir mensajes de datos transmitidos por IEDs. Estos mensajes de datos pueden recuperarse usando un sensor 67 de comunicación instalado en o acoplado a la red 69 de comunicación del sistema de automatización. El componente 61 de recopilación de datos también puede recoger señales análogas recibidas en puertos de entrada análoga del sistema de monitorización.

El sistema 60 de monitorización tiene un componente 63 de comparación de patrón del sistema que compara las propiedades monitorizadas del sistema de potencia eléctrica con el comportamiento esperado de acuerdo con el patrón 62 del sistema. Si se detecta que el sistema de potencia eléctrica no muestra un comportamiento esperado de acuerdo con el patrón 62 del sistema, un componente 66 de generación de alerta genera una alerta. El funcionamiento del componente 63 de comparación de patrón del sistema puede funcionar como se describe con referencia a cualquiera de las otras realizaciones en este documento.

El sistema 60 de monitorización tiene un componente 63 de detección de firma que compara firmas, por ejemplo, el contenido de datos en uno o diversos mensajes de datos, a las firmas 64 almacenadas. Si se detecta una coincidencia, el componente 66 de generación de alertas genera una alerta.

Las firmas 64 pueden proporcionarse al sistema de monitorización a partir de una red externa. Las firmas 64 pueden incluir firmas de intrusiones para protocolos IT que se usan en los componentes IT del sistema de automatización de la red de energía. Dichas firmas pueden ser independientes del patrón 62 del sistema.

En otra implementación, las firmas 64 pueden incluir firmas de eventos críticos que se generan con base al patrón 62 del sistema. En este caso, el sistema de monitorización puede generar las firmas 64 automáticamente con base por ejemplo, en la información de configuración para los IEDs del sistema de automatización.

La Figura 10 es un diagrama de flujo de un método 70 de una realización. El método 70 puede realizarse mediante un sistema de monitorización que también usa firmas de eventos críticos, tales como el sistema 60 de monitorización de la Figura 9.

En la etapa 71, se captura un paquete. El paquete puede ser un mensaje de datos transmitido por un IED del sistema de automatización. En 72, se decodifica el paquete. La decodificación del paquete puede incluir recuperar el contenido de datos del mensaje de datos. La decodificación puede incluir leer un parámetro de proceso transmitido digitalmente a partir del mensaje de datos.

En el paso 73, se determina si el mensaje de datos monitorizado coincide con el patrón del sistema. Esto puede implementarse como se explica con referencia a cualquiera de las realizaciones de la Figura 1 a la Figura 8. Si el mensaje de datos monitorizados coincide con el patrón del sistema, el método puede volver al paso 71. De lo contrario, se genera una señal de alerta en el paso 75.

En el paso 74, se determina si el mensaje de datos monitorizado coincide con una de las firmas de eventos críticos. Estas firmas pueden incluir firmas para intrusiones. Si hay una coincidencia, se genera una señal de alerta en el paso 75. De lo contrario, el método puede volver al paso 71.

Los sistemas de monitorización de las realizaciones pueden tener cualquiera de una diversidad de configuraciones. A modo de ilustración, el sistema de monitorización puede integrarse en otro dispositivo, como un conmutador de la red de comunicación. Alternativamente o adicionalmente, el sistema de monitorización puede ser un sistema de monitorización distribuido que tiene diversos dispositivos de monitorización distribuidos a través de la red de comunicación. Para ilustración en lugar de limitación, algunas configuraciones se explicarán con referencia a la Figura 11 a la Figura 13. En cada una de estas configuraciones, el sistema de monitorización puede funcionar como

se describió anteriormente, verificando si el contenido de datos de los mensajes de datos representa un comportamiento válido del sistema como lo define un patrón del sistema.

La Figura 11 a la Figura 13 respectivamente muestra un sistema de automatización de la red de energía con una diversidad de IEDs 82-85. Los IEDs 82-85 se comunican entre sí a través de una red de comunicación. La red de comunicación puede ser una red de comunicación conmutada. La red de comunicación puede tener una topología estrella. Se puede usar un interruptor o diversos interruptores en la red de comunicación. Se puede usar un generador 86 de reloj para generar señales de sincronización para sincronizar los IEDs 82-85. Además, el generador 86 de reloj también se puede usar para sincronizar el sistema 10 de monitorización con los IEDs 82-85.

La Figura 11 muestra un sistema 80 de automatización de la red de energía de acuerdo con una realización. En el sistema 80 de automatización de la red de energía, el sistema 10 de monitorización está integrado en el conmutador 81. Si la red de comunicación tiene diversos conmutadores, el sistema 10 de monitorización puede integrarse en uno de los conmutadores o puede distribuirse a través de diversos conmutadores.

La Figura 12 muestra un sistema 90 de automatización de la red de energía de acuerdo con otra realización. En el sistema 90 de automatización de la red de energía, el sistema de monitorización incluye una pluralidad de dispositivos 92-95 de monitorización instalados en diferentes ubicaciones. Por ilustración, un primer dispositivo 92 de monitorización puede ser un primer TAP instalado entre el IED 82 y el conmutador 91. Un segundo dispositivo 93 de monitorización puede ser un segundo TAP instalado entre otro IED 83 y el conmutador 91. En la implementación de la Figura 12, cada uno de los dispositivos 92-95 de monitorización puede incluir el patrón 13 del sistema completo. Cada uno de los dispositivos 92-95 de monitorización puede, por lo tanto, tener un conocimiento completo del comportamiento válido del sistema. Cada uno de los dispositivos 92-95 de monitorización puede determinar si los mensajes de datos recibidos en el TAP respectivo están en conformidad con el patrón del sistema. Los dispositivos 92-95 de monitorización pueden comunicarse entre sí a través de la red de comunicación. Por ejemplo, si el primero de los dispositivos 92-95 de monitorización usa el contenido de datos de un mensaje de datos recibido en un segundo dispositivo 92-95 de monitorización para verificar si el sistema 90 de automatización de la red de energía muestra un comportamiento válido, el segundo de los dispositivos de monitorización pueden notificar al primero de los dispositivos de monitorización de este contenido de datos.

La Figura 13 muestra un sistema 100 de automatización de la red de energía de acuerdo con otra realización. En el sistema 100 de automatización de la red de energía, el sistema de monitorización incluye una diversidad de TAPs 102-104 instalados en diferentes ubicaciones y operativos para recibir mensajes de datos. Por ilustración, puede instalarse un primer TAP 102 entre el IED 82 y el conmutador 101. Se puede instalar un segundo TAP 103 entre otro IED 83 y el conmutador 101. Los TAPs 102-104 pueden reenviar respectivamente los mensajes de datos recibidos a un dispositivo 105 de monitorización que incluye el patrón del sistema y evalúa los mensajes de datos recibidos en cualquiera de los TAPs 102-104. Los TAPs 102-104 sirven como sensores de comunicación para el dispositivo 105 de monitorización. El dispositivo 105 de monitorización se puede integrar en otro TAP 105 o puede ser un dispositivo separado. En la implementación de la Figura 13, no todos los dispositivos 102-105 necesitan almacenar el patrón 13 del sistema completo. Por ejemplo, solo el dispositivo 105 de monitorización o solo algunos de los dispositivos de monitorización pueden tener un conocimiento completo del comportamiento válido del sistema.

El(los) dispositivo(s) 105 de monitorización el cual almacena(n) el patrón del sistema para verificar si el sistema 100 de automatización de la red de energía, muestra un comportamiento válido.

Pueden usarse otras diversas configuraciones. Por ejemplo, el sistema de monitorización puede tener más de un dispositivo de monitorización que almacena el patrón del sistema.

A la vez que los sistemas y métodos de monitorización de acuerdo con las realizaciones se han descrito con referencia a los dibujos, se pueden realizar muchas modificaciones y variaciones de las realizaciones anteriores sin apartarse del alcance de la invención tal como se define en las reivindicaciones adjuntas. A modo de ilustración, aunque algunas realizaciones se han descrito en el contexto de detección de intrusión, los métodos y sistemas de realizaciones también se pueden usar para detectar un error de componente, un error de operador u otros eventos críticos en sistemas de energía eléctrica.

REIVINDICACIONES

1 Método de monitorización de la operación de un sistema (1000, 1600) de energía eléctrica que tiene un sistema (1981-1984, 1991-1994) de automatización de la red de energía,

comprendiendo el sistema (1981-1984, 1991-1994) de automatización de la red de energía una diversidad de dispositivos electrónicos inteligentes (IEDs) que se comunican a través de una red de comunicación,

comprendiendo el método las siguientes etapas realizadas por un sistema (10; 92-95; 102-105) de monitorización el cual utiliza información (16) de configuración que especifica las propiedades de la diversidad de IEDs (1981-1984; 82-85) y además incluye información en componentes del sistema (1000, 1600) de energía eléctrica y sus interconexiones:

monitorizar, durante el funcionamiento del sistema (1000, 1600) de energía eléctrica, propiedades del sistema (1000, 1600) de energía eléctrica, comprendiendo las propiedades monitorizadas mensajes (41, 44, 47) de datos monitorizados que se transmiten por la diversidad de IEDs (1981-1984; 82-85) en la red de comunicación; y

evaluar los mensajes (41, 44, 47) de datos monitorizados con base en la información (16) de configuración para detectar un evento crítico durante el funcionamiento del sistema (1000, 1600) de energía eléctrica, en donde la evaluación comprende analizar un contenido (43, 46, 49) de datos de al menos algunos de los mensajes (41, 44, 47) de datos monitorizados que incluyen un parámetro de proceso de un elemento primario del sistema (1000, 1600) de energía eléctrica para determinar, con base en la información (16) de configuración, si el contenido (43, 46, 49) de datos corresponde a un comportamiento válido tanto del sistema (1000, 1600) de energía eléctrica como para el sistema (1981-1984, 1991-1994) de automatización de la red de energía;

en donde el sistema (10; 92-95; 102-105) de monitorización genera un patrón (13) del sistema para el sistema (1000, 1600) de energía eléctrica y su sistema (1981-1984, 1991-1994) de automatización de la red de energía con base en la información (16) de configuración; y

en donde la etapa de evaluación comprende:

predecir mensajes de datos anticipados entre la diversidad de IEDs (1981-1984; 82-85) con base en el patrón (13) del sistema, y la comparación de los mensajes (41, 44, 47) de datos monitorizados con los mensajes (41, 44, 47) de datos anticipados previstos,

caracterizado porque

la etapa de predicción comprende usar el patrón del sistema y el parámetro de proceso del elemento primario que se incluye en el mensaje de datos transmitido por un primer IED para predecir qué valor para otro parámetro de proceso debe incluirse en otro mensaje de datos transmitido por un segundo IED; y

el método comprende además generar una señal de alerta en respuesta a la detección del evento crítico.

2. El método de una cualquiera de las reivindicaciones precedentes, en donde la evaluación comprende: determinar si la diversidad de IEDs (1981-1984; 82-85) se comporta según lo especificado por la información (16) de configuración, en donde se detecta el evento crítico si la diversidad de IEDs (1981-1984; 82-85) no se comporta como se especifica en la información (16) de configuración.

3. El método de una cualquiera de las reivindicaciones precedentes,

en el que el sistema (10; 92-95; 102-105) de monitorización tiene un puerto (23; 92-95; 102-105) de acceso de prueba de Ethernet (TAP) para monitorizar los mensajes (41, 44, 47) de datos.

4. El método de una cualquiera de las reivindicaciones 1-3,

en donde el sistema (10; 92-95; 102-105) de monitorización usa un conmutador (81; 91) de la red de comunicación para monitorizar los mensajes (41, 44, 47) de datos.

5. El método de una cualquiera de las reivindicaciones precedentes, comprendiendo además el método:

recibir, por el sistema (10; 92-95; 102-105) de monitorización, al menos un archivo de datos de configuración, en particular un archivo SCL, del sistema (1000, 1600) de energía eléctrica y su sistema (1981- 1984, 1991-1994) de automatización de la red de energía.

6. El método de una cualquiera de las reivindicaciones precedentes,

en el que las propiedades monitorizadas comprenden además señales análogas del sistema (1000, 1600) de energía eléctrica, y

en donde la evaluación comprende: evaluar tanto los mensajes (41, 44, 47) de datos monitorizados como las señales análogas en función de la información (16) de configuración para detectar el evento crítico.

7. El método de una cualquiera de las reivindicaciones precedentes,

en el que el sistema (92-95; 102-105) de monitorización es un sistema (92-95; 102-105) de monitorización distribuido que comprende una diversidad de dispositivos (92-95; 102-105) de monitorización, la diversidad de dispositivos (92-95; 102-105) de monitorización que están siendo instalados para ser distribuidos a través de la red de comunicación, estando la diversidad de dispositivos (92-95; 102-105) de monitorización sincronizados entre sí y el sistema (1981-1984, 1991-1994) de automatización de la red de energía.

8. El método de una cualquiera de las reivindicaciones precedentes, que comprende además:

generar, mediante el sistema (10; 92-95; 102-105) de monitorización, una lista negra que define firmas de estados de operación anormales, en donde el sistema (10; 92-95; 102-105) de monitorización genera la lista negra en función de la información (16) de configuración, y

comparar las propiedades monitorizadas con la lista negra para detectar el evento crítico, de modo que el sistema (10; 92-95; 102-105) de monitorización usa el comportamiento del sistema válido determinado con base en la información (16) de configuración y la lista negra para detectar el crítico evento.

9 El método de una cualquiera de las reivindicaciones precedentes, en el que el método se usa para detectar un evento crítico seleccionado de al menos uno de los siguientes:

- intrusión no autorizada,

- violación de la política de seguridad,

- fallo de hardware,

- problema de tiempo,

- error del operador, y/o

- error de configuración durante una fase de configuración de la subestación o sistema (1981-1984, 1991-1994) de automatización de la red de energía.

10. Un sistema (10; 92-95; 102-105) de monitorización para un sistema (1000, 1600) de energía eléctrica,

el sistema (1000, 1600) de energía eléctrica que tiene un sistema (1981-1984, 1991-1994) de automatización de la red de energía, el sistema (1981-1984, 1991 1994) de automatización de la red de energía comprende una diversidad de dispositivos (1981-1984; 82-85) electrónicos inteligentes (IEDs) que se comunican a través de una red de comunicación,

comprendiendo el sistema (10; 92-95; 102-105) de monitorización:

una interfaz (11; 15) para monitorizar, durante el funcionamiento del sistema (1000, 1600) de energía eléctrica, las propiedades del sistema (1000, 1600) de energía eléctrica, las propiedades de monitorización que comprenden mensajes (41, 44, 47) de datos monitorizados que se transmiten por la diversidad de IEDs (1981-1984; 82-85) a través de la red de comunicación;

un dispositivo (12) de procesamiento configurado para evaluar los mensajes (41, 44, 47) de datos monitorizados con base en la información (16) de configuración para detectar un evento crítico durante el funcionamiento del sistema (1000, 1600) de energía eléctrica, en donde la información (16) de configuración especifica propiedades de la diversidad de IEDs (1981-1984; 82-85) e incluye además información de los componentes del sistema (1000, 1600) de energía eléctrica y sus interconexiones, en donde el dispositivo (12) de procesamiento está configurado para analizar el contenido (43, 46, 49) de datos de al menos algunos de los mensajes (41, 44, 47) de datos monitorizados que incluye un parámetro de proceso de un elemento primario del sistema (1000, 1600) de energía eléctrica para determinar, con base en la información (16) de configuración, si el contenido (43, 46, 49) de datos corresponde a un comportamiento válido tanto del sistema (1000, 1600) de energía eléctrica como del sistema (1981-1984, 1991-1994) de automatización de la red de energía; y

en donde el sistema (10; 92-95; 102-105) de monitorización está configurado para generar un patrón (13) del sistema para el sistema (1000, 1600) de energía eléctrica y su sistema (1981-1984, 1991-1994) de automatización de la red de energía con base en la información (16) de configuración; y en el que el dispositivo (12) de procesamiento está configurado para evaluar los mensajes (41, 44, 47) de datos monitorizados de la siguiente manera:

predecir los mensajes de datos anticipados entre la diversidad de IEDs (1981-1984; 82-85) con base en el patrón (13) del sistema, y

comparar los mensajes (41, 44, 47) de datos monitorizados con los mensajes (41, 44, 47) de datos anticipados previstos,

caracterizado porque

el dispositivo (12) de procesamiento está configurado para predecir los mensajes de datos anticipados utilizando el patrón del sistema y el parámetro de proceso del elemento primario que se incluye en el mensaje de datos transmitido por un primer IED para predecir qué valor para otro parámetro de proceso debe incluirse en otro mensaje de datos transmitido por un segundo IED; y

el dispositivo (12) de procesamiento está configurado para generar una señal de alerta en respuesta a la detección del evento crítico.

11. El sistema de monitorización de la reivindicación 10, en el que el sistema (10; 92-95; 102-105) de monitorización está configurado para realizar el método de una cualquiera de las reivindicaciones 1-9.

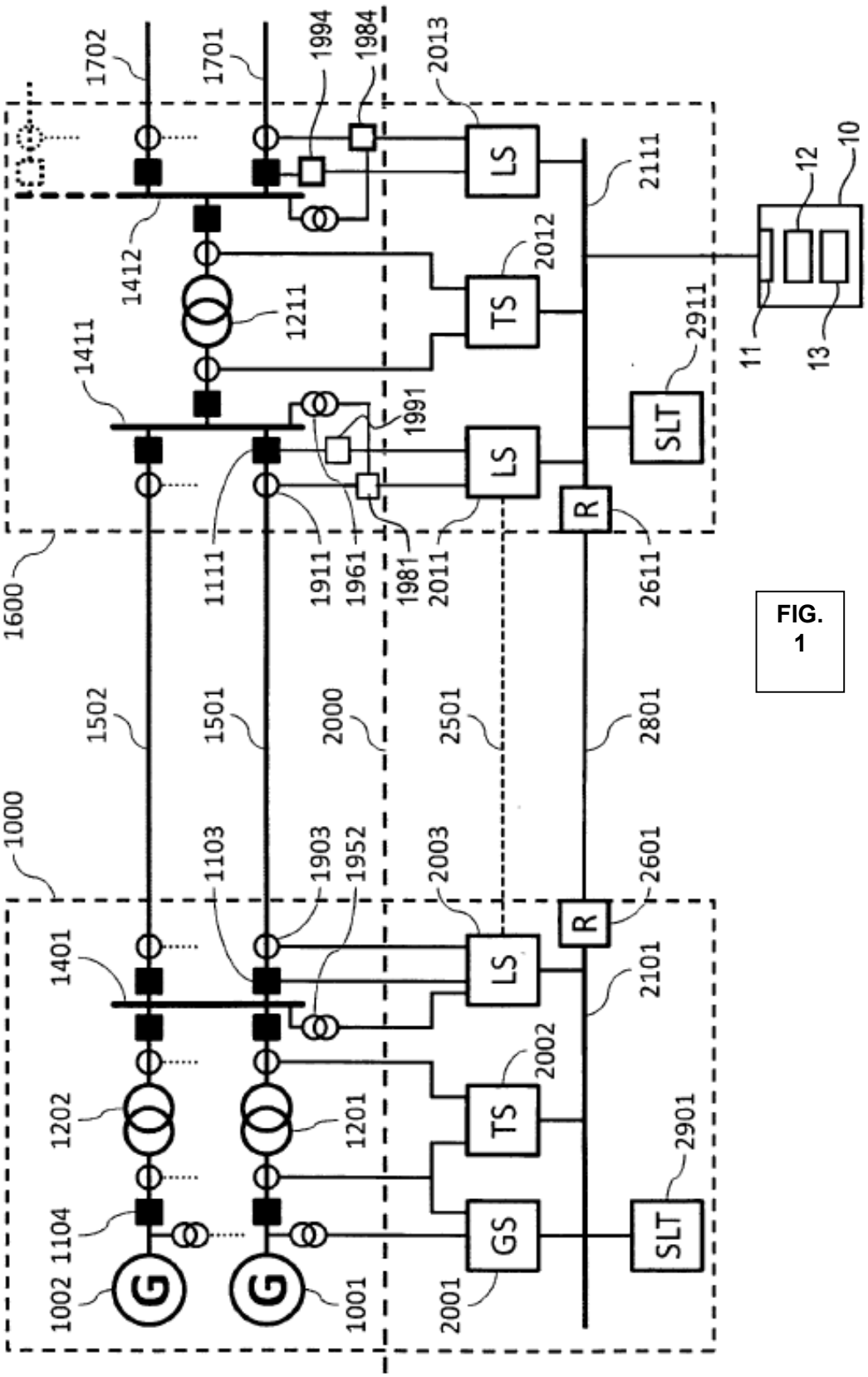
1702
1701
1994
1984
2013
1412
1211
1411
1991
1111
1911
1961
1981
2011
2611
1600
1502
1501
2000
2501
2801
1000
1103
1903
1952
2003
2601
1401
2101
1202
1201
2002
1104
2901
1002
1001
2001
LS
TS
GS
SLT
R
2111
2012
2911
12
10
11
13

FIG. 1

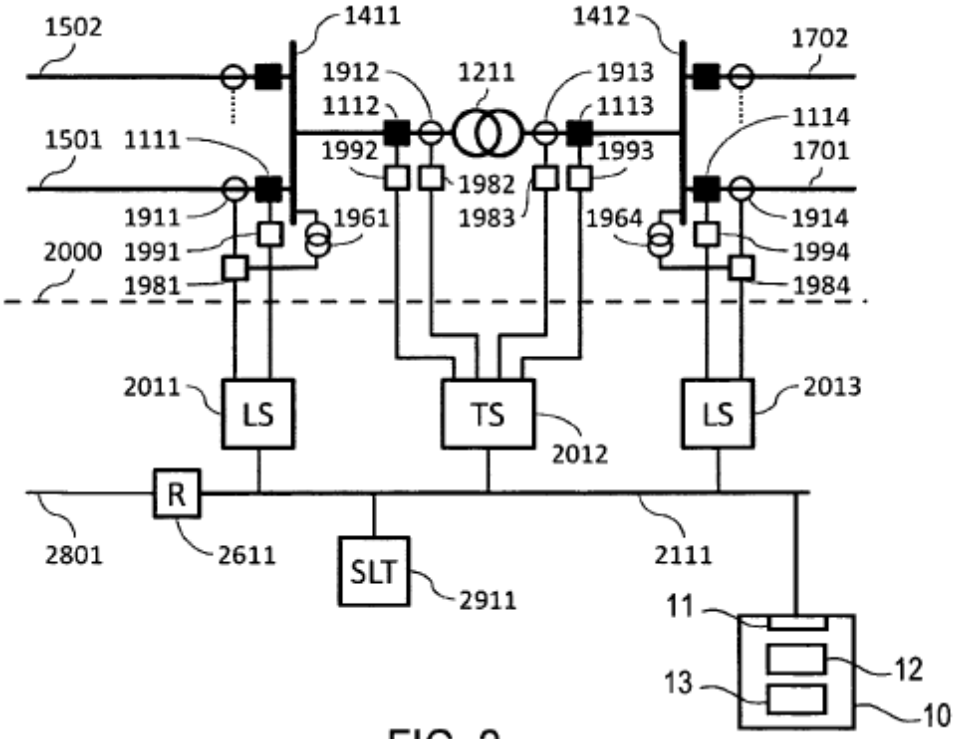
1502
1411
1412
1702
1912
1211
1913
1112
1113
1114
1501
1111
1992
1993
1701
1982
1911
1961
1983
1964
1914
2000
1991
1994
1981
1984
2011
LS
TS
LS
2013
2012
R
2801
2611
2111
SLT
2911
11
12
13
10

FIG. 2

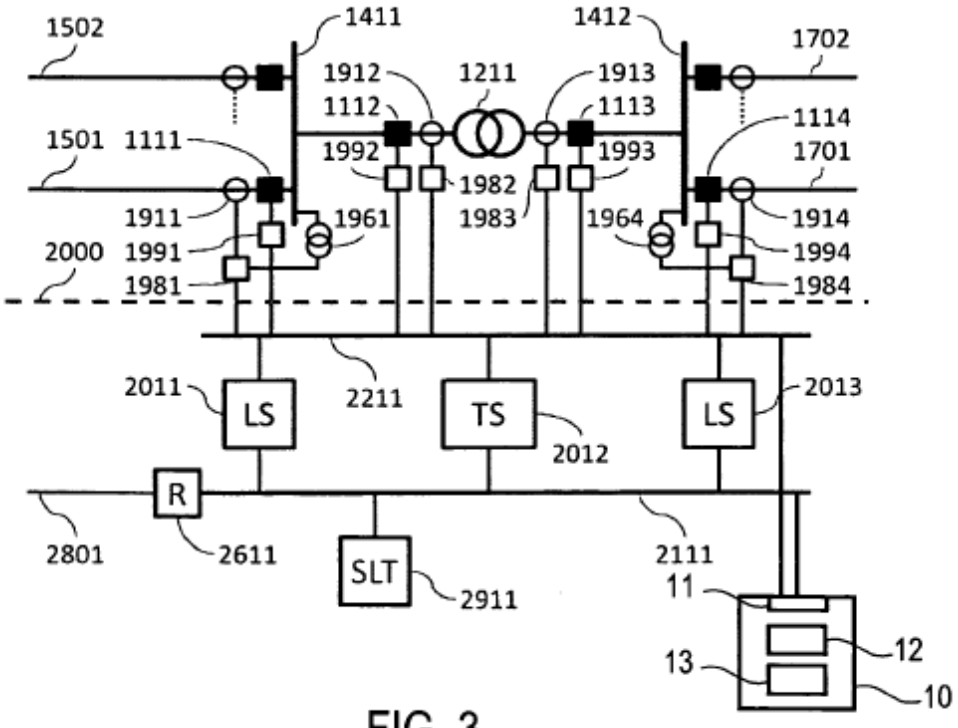
1502
1411
1412
1702
1912
1211
1913
1112
1113
1114
1501
1111
1992
1993
1701
1982
1911
1961
1983
1964
1914
2000
1991
1994
1981
1984
2011
LS
2211
TS
LS
2013
2012
R
2801
2611
2111
SLT
2911
11
12
13
10

FIG. 3

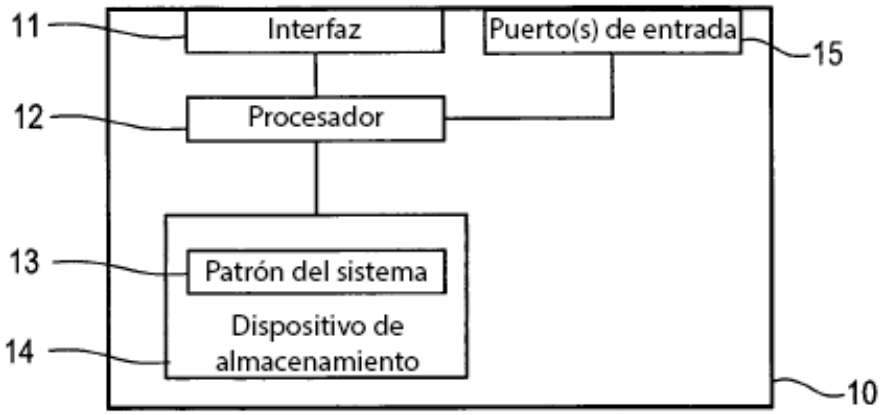

FIG. 4

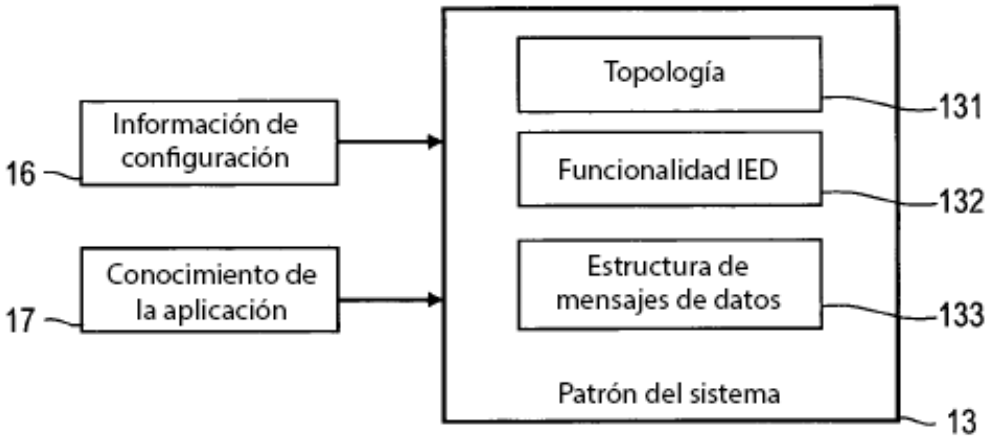

FIG. 5

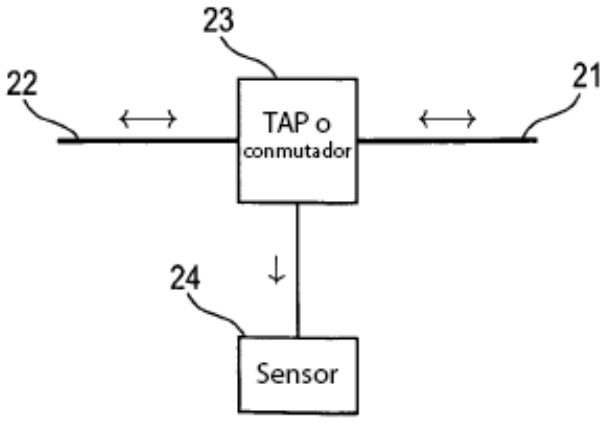

FIG. 6

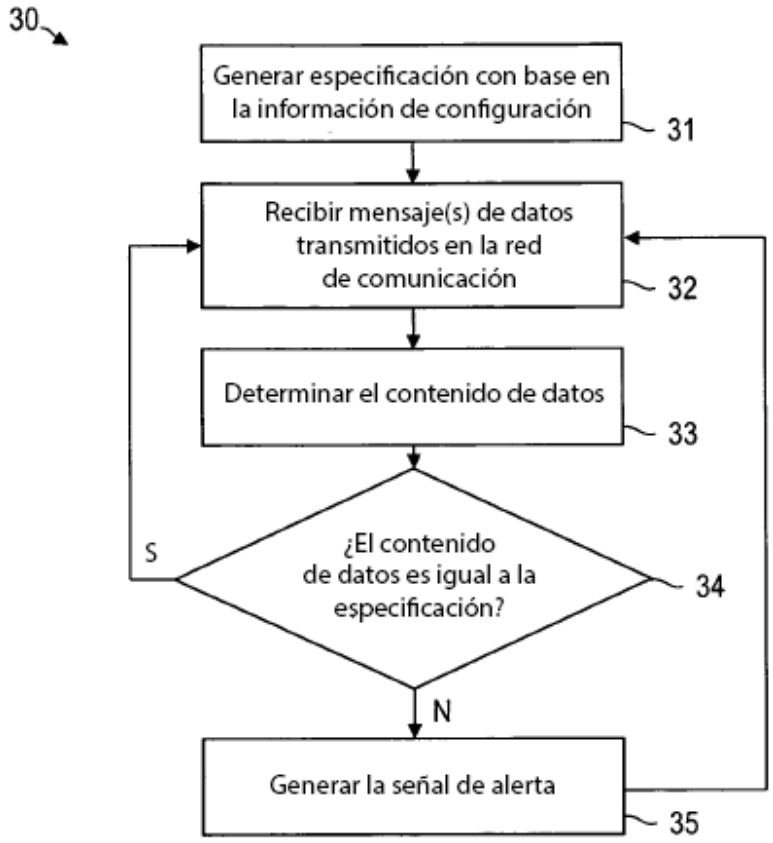
30
Generar especificación con base en la información de configuración
31
Recibir mensaje(s) de datos transmitidos en la red de comunicación
32
Determinar el contenido de datos
33
¿El contenido de datos es igual a la especificación?
34
S
N
Generar la señal de alerta
35

FIG. 7

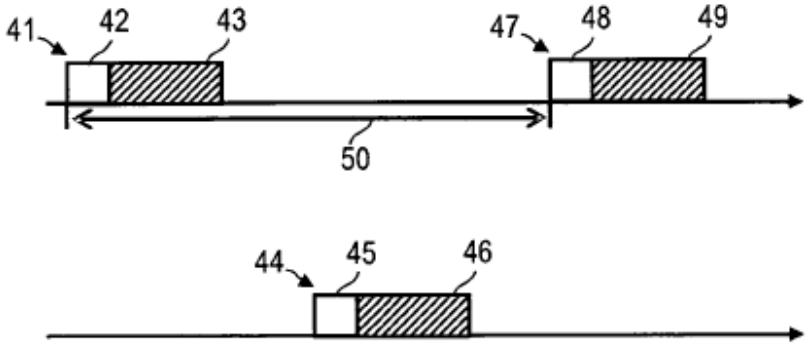
41
42
43
47
48
49
50
44
45
46

FIG. 8

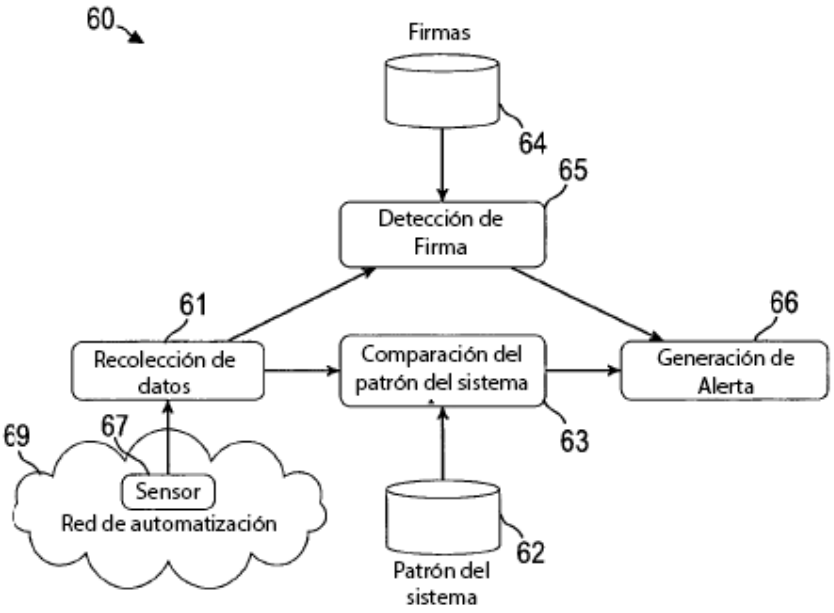
60
Firmas
64
65
Detección de Firma
61
66
Recolección de datos
Comparación del patrón del sistema
Generación de Alerta
63
69
67
Sensor
Red de automatización
62
Patrón del sistema

FIG. 9

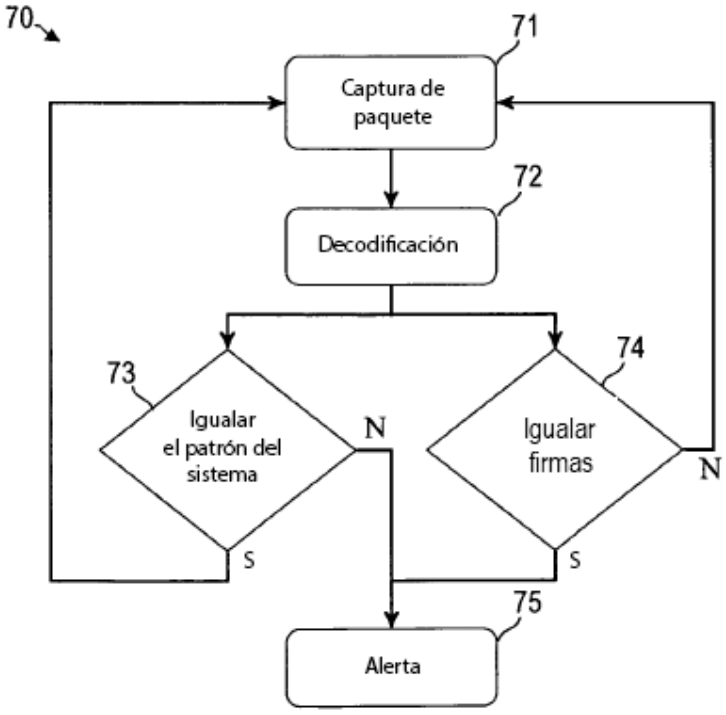
70
71
Captura de paquete
72
Decodificación
73
Igualar el patrón del sistema
N
S
74
Igualar firmas
N
S
75
Alerta

FIG. 10

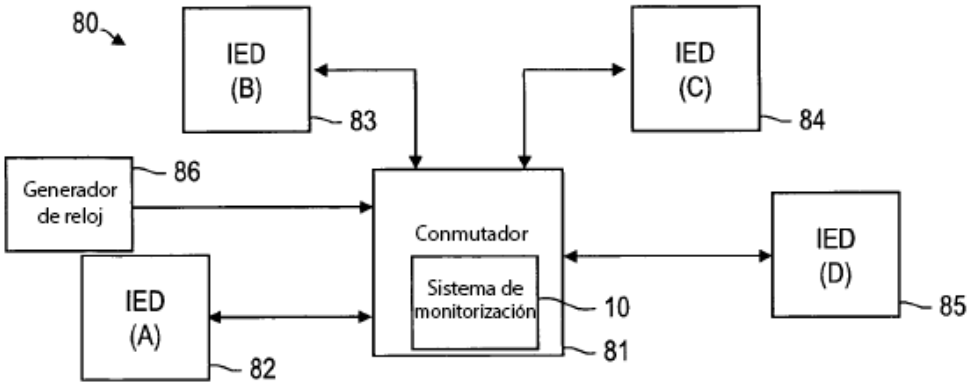
80
IED
(B)
83
IED
(C)
84
Generador
de reloj
86
Conmutador
Sistema de
monitorización
10
81
IED
(D)
85
IED
(A)
82

FIG. 11

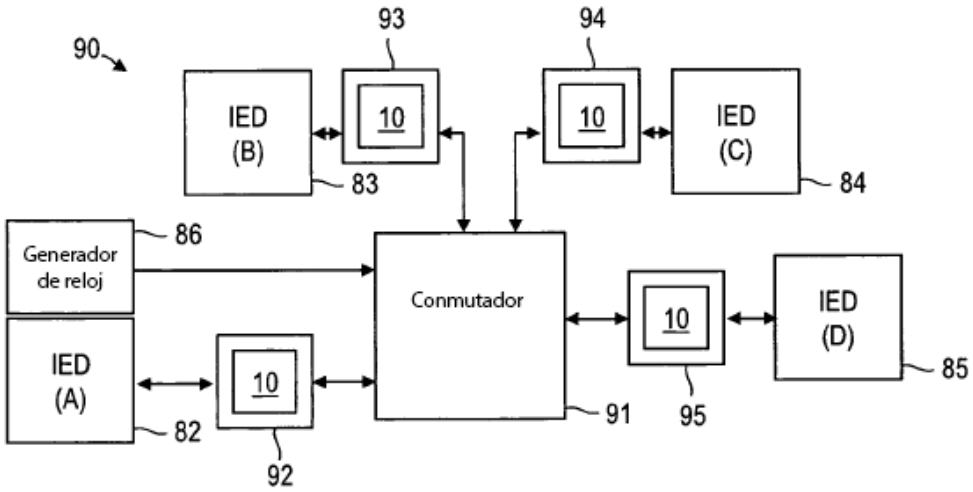
90
93
94
IED
(B)
10
10
IED
(C)
83
84
Generador
de reloj
86
Conmutador
IED
(A)
10
10
IED
(D)
85
82
92
91
95

FIG. 12

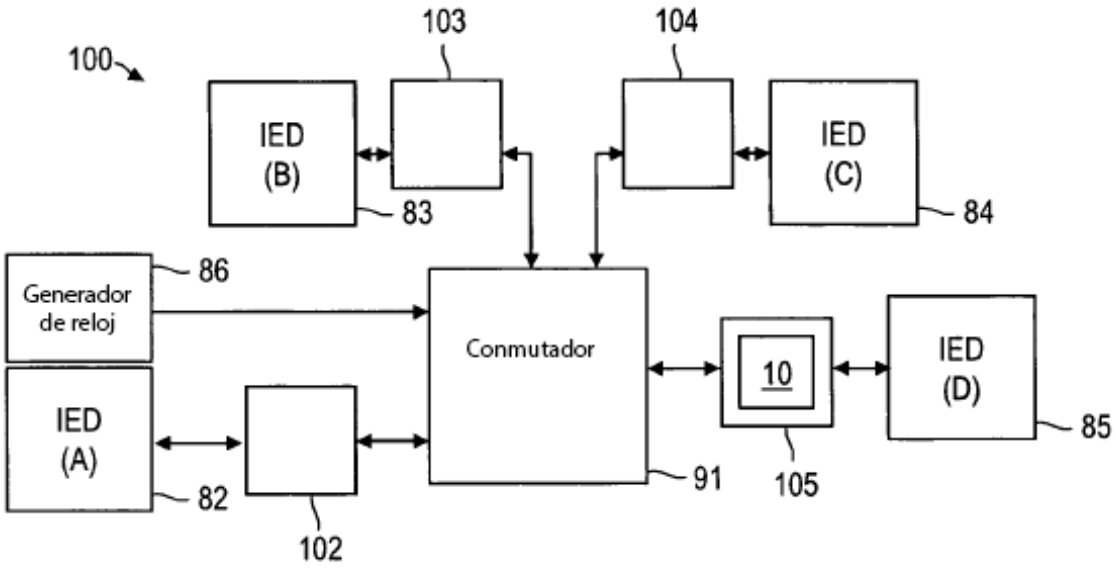
100
103
104
IED
(B)
83
IED
(C)
84
Generador
de reloj
86
Conmutador
10
IED
(D)
85
IED
(A)
82
102
91
105

FIG. 13