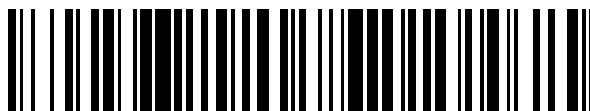


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 459 119**

51 Int. Cl.:

**H04L 12/24** (2006.01)

**H04L 29/06** (2006.01)

**G06F 21/00** (2013.01)

**H04L 29/08** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **31.08.2011 E 11179613 (2)**

97 Fecha y número de publicación de la concesión europea: **26.03.2014 EP 2566102**

54 Título: **Registro de eventos de seguridad y conversión de mensajes de eventos de seguridad en control de procesos**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**08.05.2014**

73 Titular/es:

**ABB TECHNOLOGY AG (100.0%)**  
**Affolternstrasse 44**  
**8050 Zürich, CH**

72 Inventor/es:

**ALVAREZ, FERNANDO;**  
**HOHLBAUM, FRANK y**  
**HILPERT, GUNNAR**

74 Agente/Representante:

**UNGRÍA LÓPEZ, Javier**

ES 2 459 119 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Registro de eventos de seguridad y conversión de mensajes de eventos de seguridad en control de procesos

5 **Campo de la invención**

La invención se refiere a sistemas de automatización industrial y de control, en particular, a sistemas de automatización de subestaciones con una representación de configuración estandarizada. Más particularmente, se refiere a la manipulación y al registro de eventos de seguridad en dichos sistemas.

10

**Antecedentes de la invención**

Los sistemas de automatización de subestaciones (SA) supervisan, monitorizan, protegen y controlan subestaciones en redes de energía eléctrica de alta y media tensión. Esto normalmente se realiza por medio de dispositivos de protección y control asignados a los módulos y/o al equipo principal de la subestación, así como mediante dispositivos de nivel de la estación, incluyendo puerta de enlaces e interfaces hombre-máquina (HMI). Los dispositivos de protección y control del sistema de SA cercanos al proceso generan eventos, incluyendo advertencias y señales de alarma, relativos al equipo principal o a equipos secundarios o relativos a funciones de protección o de control. Los mensajes de informes correspondientes se formatean de acuerdo con un protocolo adecuado y se transmiten en una red de comunicación del sistema de SA a los dispositivos de nivel de la estación para su registro, archivo y/o evaluación. Por otra parte, las alarmas se pueden proporcionar para la representación gráfica inminente en un operador HMI, por ejemplo, para la visualización óptica en una imagen de resumen de una sola línea, para que un operador investigue el origen de una perturbación.

15

20

25

30

Los requisitos de seguridad y normas introducidos recientemente dirigidos a las empresas de servicios públicos que operan los sistemas distribuidos como los sistemas de transmisión y distribución de energía eléctrica, agua o gas, requieren que los eventos relevantes de seguridad son asimismo almacenados y están disponibles para su posterior recuperación. En el contexto de la presente invención, los eventos relevantes de seguridad relacionados con la seguridad informática o a la seguridad de la tecnología de la información (IT) y como tal no están directamente vinculados a los aspectos operativos de la subestación. Reglamentos, tales como SOX ("Sarbanes-Oxley Act"), NERC-CIP ("North American Electric Reliability Corporation-Critical Infrastructure Protection"), y otros están exigiendo a las organizaciones implementar medidas de seguridad integrales, que pueden incluir la recogida y el análisis de los registros, es decir, informes de eventos de seguridad básica almacenados en un archivo de registro y originarios de muchas fuentes diferentes.

35

El registro de eventos se llevó a cabo inicialmente a nivel local y más tarde la necesidad de almacenamiento centralizado y la visión central de los eventos se convirtió en una característica estándar en los sistemas distribuidos. En este contexto, el protocolo Syslog (incluyendo un protocolo de comunicación simple y una definición de formato de datos rudimentaria) como se documenta en la solicitud de comentarios (RFC) 3164 y 5424 del Internet Engineering Task Force (IETF) es el estándar de facto en el área de IT para los datos de eventos de registro para su posterior recuperación. Syslog permite la separación del software que genera los mensajes del sistema que los almacena y el software que los informa y analiza. El protocolo Syslog se utiliza para transmitir los mensajes de notificación de eventos, e incluye un formato de mensaje que permite que se proporcione a las extensiones específicas de los proveedores de una manera estructurada.

40

45

La solicitud de patente US 2007/0283194 divulga la recopilación de datos de registro utilizando el registro de red estándar y protocolos de mensajería como Syslog, SNMP, Sntp y generando gran número de registros en diferentes formatos para su posterior análisis.

50

55

Un estándar de comunicación para comunicación entre los dispositivos secundarios de una subestación ha sido introducido por la Comisión Electrotécnica Internacional (IEC) como parte de la norma IEC 61850, titulada "redes y sistemas de comunicación en subestaciones". Para los mensajes no críticos en tiempo, la norma IEC 61850-8-1 especifica el protocolo de especificación de mensajes de fabricación (MMS, ISO/IEC 9506) basado en una pila de protocolo de interconexión de sistemas abiertos reducidos (OSI) con el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP) en el transporte y la capa de red, respectivamente, y Ethernet como medio físico. Como cualquier otro protocolo de automatización de procesos con la semántica de aplicaciones estandarizadas, la norma IEC 61850 proporciona para eventos relacionados con procesos un formato especial para eventos relacionados con la seguridad.

60

65

Los sistemas SA basados en la norma IEC 61850 se configuran y se describen por medio de una representación de configuración estándar o descripción formal del sistema llamada descripción de configuración de subestaciones (SCD). Un archivo SCD comprende el flujo lógico de datos entre los dispositivos electrónicos inteligentes (IEDs) y la relación entre los IEDs, así como la funcionalidad que los IEDs ejecutan en nombre de la subestación. Además de los sistemas SA para subestaciones en los sistemas de energía eléctrica de alta y media tensión, otros sistemas de control de procesos para, por ejemplo centrales hidroeléctricas, sistemas de energía eólica y recursos energéticos distribuidos (DER), pueden igualmente describirse mediante una descripción formal del sistema, al menos

parcialmente idéntica a la descripción de la norma IEC 61850 SA.

A pesar de la existencia de los protocolos de la norma IEC 61850, existen dispositivos SA, como sensores, equipos de redes de comunicación y ordenadores de propósito general, que no se adhieren a la norma IEC 61850 que todavía necesitan incluirse en un sistema SA junto con los IEDs que cumple con la norma IEC 61850. Estos dispositivos SA implementan una serie de protocolos de transmisión utilizados anteriormente para el intercambio de datos operativos, denominados colectivamente como protocolos pre-IEC 61850. De acuerdo con la solicitud de patente EP-A 1976218, un IED proxy está configurado como un dispositivo de puerta de enlace para la conversión de datos entre protocolos de comunicación pre-IEC 61850 e IEC 61850. El IED proxy se configura en base a un conjunto de asignaciones que se codifican en el archivo de descripción de configuración SA (SCD).

### Descripción de la invención

Es un objetivo de la invención proporcionar una mayor flexibilidad en la ingeniería y en la configuración de un sistema de control de procesos industriales, con gestión de eventos de seguridad. Este objetivo se consigue mediante un procedimiento de gestión de eventos de seguridad y mediante un dispositivo de puerta de enlace de acuerdo con las reivindicaciones independientes. Las realizaciones preferidas son evidentes a partir de las reivindicaciones dependientes de la patente.

Según la invención, los eventos relevantes de seguridad en un sistema de control de procesos (PC) se gestionan de una manera que no requiere que los dispositivos del sistema de PC utilicen un único protocolo para la notificación de eventos de seguridad. Por lo tanto, los diversos dispositivos del sistema de PC, tales como dispositivos electrónicos inteligentes (IED), sensores, ordenadores de propósito general, dispositivos de puerta de enlace que están conectados a una red de comunicación, así como los elementos de red de esta última, pueden continuar la radiodifusión de mensajes de eventos de seguridad de acuerdo con su protocolo preferido a través de la red de comunicación.

Específicamente, los mensajes de eventos de seguridad que comprenden información de eventos de seguridad de acuerdo con un primer protocolo se reciben mediante un dispositivo receptor diferente del dispositivo de origen del mensaje, por ejemplo, mediante un dispositivo de puerta de enlace o un archivo de registro conectado a la red de comunicación. La información de eventos de seguridad es extraída por el dispositivo receptor, y se asigna a un segundo protocolo que está configurado para ser utilizado por otros dispositivos de origen del sistema de PC para reportar eventos de seguridad. El sistema de PC puede ser un sistema de automatización de subestaciones SA para una subestación en un sistema de energía eléctrica, o un sistema de control de procesos para una planta hidroeléctrica, un sistema de energía eólica, o recursos de energía distribuidos (DER) que se describen mediante una descripción formal del sistema, al menos en parte idéntica a la descripción SA de la norma IEC 61850, siendo el primer protocolo un protocolo IEC 61850-7-4 y siendo el segundo protocolo un protocolo Syslog, o viceversa.

En una primera variante preferida de la invención, un dispositivo de puerta de enlace está conectado a la red de comunicación del sistema de PC, y está adaptado para asignar, o convertir, un mensaje que comprende información de eventos de seguridad según la norma IEC 61850-7-4 en un mensaje que incluye información de eventos de seguridad de acuerdo con un protocolo de registro. Este último mensaje es posteriormente enviado a un archivo o a un servidor Syslog, o a otra aplicación de evaluación de eventos remotos o de archivo. En paralelo, el dispositivo de puerta de enlace puede emitir sin asignar aún más cualquier mensaje de seguridad que comprende información de eventos de seguridad de acuerdo con el protocolo Syslog.

Ventajosamente, el dispositivo de puerta de enlace está adaptado además para identificar alarmas, sobre la base de una indicación de la severidad de eventos de seguridad comprendida en la información de eventos de seguridad de acuerdo con la norma IEC 61850-7-4, y para asignar, o convertir, el mensaje a un protocolo del centro de control de red (NCC) como IEC 60870-101, IEC 60870-104, o DNP.

En una segunda variante preferida de la invención, un archivo Syslog está conectado a la red de comunicación de un sistema de automatización de subestaciones, y además está adaptado para recibir, como un cliente de la norma IEC 61850, mensajes IEC 61850-7-4 que comprenden información de eventos de seguridad. Esta última información se extrae, y se asigna o se convierte en un protocolo Syslog para generar un registro de eventos de seguridad Syslog. Este último se almacena en el archivo Syslog de forma consolidada junto con otros registros de eventos de seguridad y, eventualmente se ofrecen, como un servidor Syslog, a clientes adicionales.

En una tercera variante preferida de la invención, un dispositivo de puerta de enlace está conectado a la red de comunicación de un sistema de automatización de subestaciones, y está adaptado para asignar o convertir un mensaje que comprende información de eventos de seguridad de acuerdo con un protocolo de registro en un mensaje que incluye la información de eventos de seguridad de acuerdo con la norma IEC 61850-7-4, en lugar de un protocolo convencional del centro de control de red (NCC). Este último mensaje es reenviado posteriormente más allá de la red de comunicaciones SA, por ejemplo, a un NCC para la evaluación de la alarma, junto con cualquier mensaje de seguridad que comprende información de eventos de seguridad de acuerdo con la norma IEC 61850 y se recibe y se comunica mediante la puerta de enlace en formato no asignado.

Ventajosamente, una identificación del primer mensaje de eventos de seguridad de acuerdo con el protocolo de registro se consigue mediante el análisis del mensaje y de los caracteres comparando con la cadena de caracteres del identificador positivo/negativo desde una biblioteca.

- 5 En resumen, esta invención propone extraer eventos de seguridad relevantes desde eventos IEC 61850 generales y asignar adecuadamente lo anterior a la vista de una consolidación con el estándar TI u otros eventos de seguridad a nivel de estación o niveles del sistema aún más altos. De este modo, se permite la coexistencia de dos protocolos de seguridad en el bus de la subestación, y se consigue una mayor flexibilidad en el diseño del sistema SA, en particular de los sistemas SA con una mezcla de IEDs compatibles con la norma IEC 61850 y dispositivos SA que no se adhieren a los protocolos de comunicación IEC 61850.

**Breve descripción de los dibujos**

- 15 El objeto de la invención se explicará con más detalle en el siguiente texto con referencia a realizaciones de ejemplo preferidas que se ilustran en el dibujo adjunto, donde:

La figura 1 muestra esquemáticamente dos trayectorias de transmisión de información de eventos de seguridad.

**Descripción detallada de las realizaciones preferidas**

- 20 La figura 1 representa un sistema de automatización de subestaciones (SA) con dos dispositivos electrónicos inteligentes (IEDs) 10, 11 y un dispositivo de puerta de enlace 20 conectado a una red de comunicación de subestaciones 15. El sensor 12 como un dispositivo no compatible con la norma IEC 61850 de ejemplo también está conectado a la red 15. Unos interruptores 151, 152 como elementos de la red de comunicación de ejemplo son parte del sistema SA. El dispositivo de puerta de enlace está conectado comunicativamente a un centro de control de red (NCC) 30 de una red de transmisión de energía eléctrica que comprende la subestación, y/o a un archivo Syslog 31. El dispositivo de puerta de enlace, básicamente, está adaptado para transportar señales de estado, eventos, alarmas, medidas y registros de perturbaciones del sistema SA al NCC y/o al archivo Syslog. Para tal fin, la puerta de enlace es por sí misma un cliente Syslog e IEC 61850 adaptado para reunir todos los eventos relacionados con la seguridad a partir de IEDs IEC 61850 y dispositivos no IEC 61850. La línea de trazos en la figura 1 indica la transmisión de información de eventos de seguridad que implica la conversión de IEC 61850 a Syslog, mientras que la línea de puntos y trazos indica el flujo de información correspondiente incluida una asignación de Syslog a IEC 61850.

- 35 Alternativamente, el archivo Syslog puede estar conectado a la red de comunicación de la subestación sin pasar a través del dispositivo de puerta de enlace, por ejemplo como un dispositivo de nivel de la estación independiente o incrustado en una estación de trabajo del operador o un sistema microScada.

- 40 Según la norma IEC 61850, el nodo lógico GSAL (aplicación de seguridad genérica) se puede usar para gestionar los datos de eventos de seguridad, en particular, para vigilar violaciones de seguridad en la autorización de las categorías, el control de acceso, los privilegios de servicio y las asociaciones inactivas. GSAL contiene diferentes contadores para las diferentes categorías, y es capaz de ofrecer eventos con textos de estado individuales apropiados. Los objetos de datos obligatorios DO correspondientes a las categorías son designados AuthFail (fallos de autorización), SvcViol (violaciones de privilegio de servicio), AcsCtlFail (fallos de control de acceso detectados) e Ina (asociaciones inactivas), todos usando la clase de datos SEC (clase de datos común del contador de seguridad). Este último, a su vez, consta de los siguientes atributos de datos

- 50 cnt número de veces que sucedió un evento de esta categoría  
 sev gravedad, (desconocida 0, crítica 1, importante 2, menor 3, aviso 4)  
 t marca de tiempo  
 addr dirección IP desde la que llega la solicitud, o identificador de usuario, si está disponible  
 addinfo información del texto del evento desde la fuente del evento, con los siguientes datos de texto opcionales:

- 55 ID vendedor por ejemplo: ABB  
 versión de formato por ejemplo: ABB: 02  
 id evento vendedor por ejemplo: ABB: 02:3590  
 fuente sec de ev por ejemplo: ABB: 02:3590:987  
 tipo de dispositivo por ejemplo: ABB: 02:3590:987: RTU560  
 info extra datos de texto adicionales relevantes para el evento correspondiente  
 60 origen de eventos nombre del IED IEC 61850 o dirección IP

- 65 La siguiente tabla muestra unos pocos tipos de eventos de seguridad de ejemplo y definidos por el usuario o de alarma junto con los correspondientes objetos de datos (DO) de acuerdo con la norma IEC 61850, en la tercera columna. En la segunda columna titulada *Severidad*, la letra S designa los tipos de alarma de seguridad (con una severidad = "crítica" en términos de la norma IEC 61850), mientras que la letra W designa los tipos de eventos de seguridad que indican posibles advertencias en términos de la norma IEC 61850.

ID y definición de evento/alarma de seguridad	Gravedad	IEC 61850 DO
...		
1120 Fallo de registro – Usuario desconocido	S	GSAL.Fallo Aut.
1140 Fallo de registro – Contraseña incorrecta	W	GSAL.Fallo Aut.
1150 Fallo de registro – Contraseña caducada	W	GSAL.Fallo Aut.
1170 Fallo de registro 3 veces	S	GSAL.Fallo Aut.
...		
1460 Fallo de parámetro cambiado – sin derechos	S	GSAL. Fallo AcsCtl
1470 Fallo de parámetro cambiado – fuera de rango	W	GSAL.SvcViol
1480 Fallo de parámetro cambiado – tipo incorrecto	W	GSAL.SvcViol
...		

Dispositivos tales como el dispositivo de puerta de enlace o el servidor de registro de recepción de las comunicaciones IEC 61850 pueden asignar o codificar la información de eventos de seguridad a partir de un paquete IEC 61850 a un paquete Syslog. Cualquier formato de texto Syslog compatible puede ser utilizado para ese fin. Los identificadores de eventos numéricos (id evento vendedor) permiten la localización del texto de la descripción de eventos, mediante la asignación del número ID de eventos en el texto de descripción de eventos en cualquier idioma local. A modo de ejemplo, los siguientes datos de muestra de eventos del mensaje GSAL IEC 61850

```

5 cnt: 1
  sev: 4 (aviso)
  t: 28 de septiembre 11:59:18 (UTC)
  addr: Anónima
  addinfo: "ABB: 02:1140:3567: RTU560: Dispositivo 01"

```

15 puede asignarse en el paquete de mensajes Syslog <13> Sep28 11:59:18 | ABB: 02 | Fallo registro-Contraseña incorrecta | 1140 | 3567 | Dispositivo01 | RT U560 | Anónimo, donde <13> indica una prioridad Syslog que para el evento específico de seguridad "Fallo de registro - Contraseña incorrecta" corresponde al nivel de severidad IEC 61850 "4" (aviso).

20 Antes de la incorporación de la información del suceso de seguridad recibida de acuerdo con un protocolo Syslog en un mensaje de acuerdo con la norma IEC 61850, el anterior puede tener que ser debidamente identificado, ya que por lo general hay un gran número de eventos Syslog que no son de seguridad que deben ser descartados. En este contexto, surge una dificultad debido al hecho de que el protocolo Syslog utilizado hoy en día no impone ningún formato o especificación directriz sobre los datos del paquete Syslog. Cada vendedor tiene su propio estilo Syslog y mensajes de texto propios. Por lo tanto, el evento de seguridad Syslog y los datos de alarma deben ser primero filtrados/capturados y posteriormente asignados/dirigidos al IEC 61850.

30 Para extraer/filtrar eventos de seguridad Syslog relevantes y alarmas, un motor basado en reglas de una biblioteca analiza los paquetes entrantes Syslog y sólo los paquetes que están identificados como relacionados con la seguridad son asignados a la IEC 61850. Cada regla de la biblioteca incluye una o varias cadenas de identificadores que empiezan con un signo "+" o "-" que indica si la cadena se encuentra en el paquete Syslog, o si la cadena no debe ser encontrada en el paquete Syslog. Una cadena de identificador positivo de ejemplo lee "Fallo de registro - contraseña incorrecta" y recita la correspondiente información de texto sin formato, publicada por el fabricante del dispositivo de origen. Son posibles varios criterios de valoración de coincidencias de cadenas individuales, por ejemplo, paquetes Syslog que consiguen una puntuación positiva en exceso de uno (tres "+" frente a un "-") son retenidos para su posterior procesamiento. El alcance de la invención se define mediante las reivindicaciones adjuntas.

**REIVINDICACIONES**

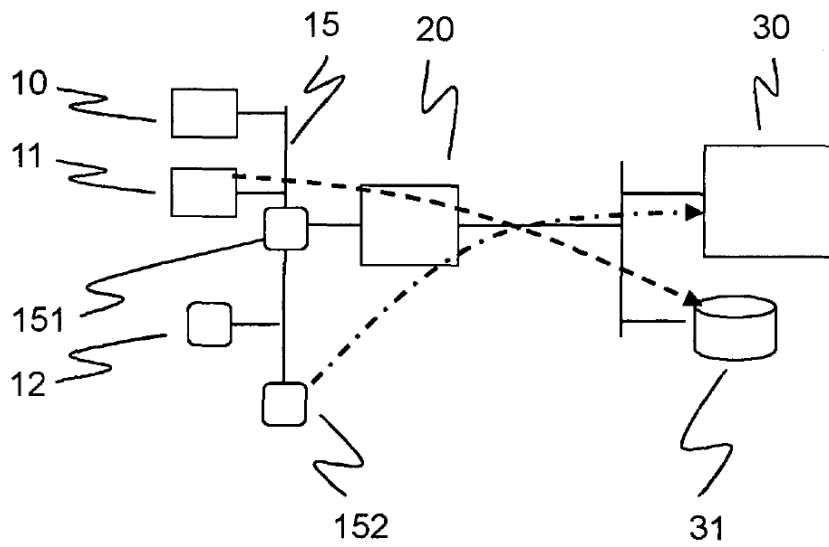
1. Un procedimiento de gestión de eventos de seguridad en un sistema de Control de Procesos, PC, siendo dicho sistema de PC un sistema de Automatización de Subestaciones, SA, para una subestación de un sistema de energía eléctrica, con una red de comunicación (15) que interconecta los dispositivos del sistema de PC (10, 11; 12; 151, 152; 20), donde un primer y segundo dispositivos del sistema de PC transmiten, en la red de comunicación, mensajes de eventos de seguridad que comprenden información de eventos de seguridad de acuerdo con un primer y segundo protocolos, respectivamente, siendo el primer y segunda protocolos uno y el otro de un protocolo del Comité Electrotécnico Internacional, IEC, 61850-7-4 y un protocolo Syslog, comprendiendo el procedimiento
- 5 10
- recibir un primer mensaje de eventos de seguridad de acuerdo con el primer protocolo, y extraer información de eventos de seguridad del primer mensaje, y
  - asignar la información de los eventos de seguridad extraída al segundo protocolo.
- 15 2. El procedimiento de acuerdo con la reivindicación 1, donde el primer protocolo es el protocolo IEC 61850-7-4 y el segundo protocolo es el protocolo Syslog, que comprende
- 20
- mediante un dispositivo de puerta de enlace (20) conectado a la red de comunicación, convertir la información de eventos de seguridad extraída en un mensaje Syslog, y
  - proporcionar el mensaje Syslog a un archivo Syslog (31).
3. El procedimiento de acuerdo con la reivindicación 2, que comprende
- 25
- mediante el dispositivo de puerta de enlace, y en base a una indicación de gravedad de los eventos de seguridad del primer mensaje que indica una alarma, convertir la información de eventos de seguridad extraída en un mensaje de Centro de Control de Red, NCC, de acuerdo con un protocolo NCC, y
  - proporcionar el mensaje NCC a un NCC (30) del sistema de energía eléctrica.
4. El procedimiento de acuerdo con la reivindicación 1, donde el primer protocolo es el protocolo IEC 61850-7-4 y el segundo protocolo es el protocolo Syslog, que comprende
- 30
- mediante un archivo de registro (31) conectado a la red de comunicación, codificar la información de eventos de seguridad extraída como una entrada de registro de eventos de seguridad de acuerdo con el protocolo Syslog, y
  - almacenar la entrada de registro en el archivo de registro.
- 35 5. El procedimiento de acuerdo con la reivindicación 2 o 4, que comprende
- 40
- convertir una indicación de gravedad de los eventos de seguridad comprendidos en un Atributo de Datos de una Aplicación de Seguridad Genérica, GSAL, un Nodo Lógico alojado por un Dispositivo Electrónico Inteligente, IED, de origen del primer mensaje en una indicación de prioridad Syslog.
6. El procedimiento de acuerdo con la reivindicación 1, donde el primer protocolo es el protocolo Syslog y el segundo protocolo es el protocolo IEC 61850-7-4, que comprende
- 45
- mediante un dispositivo de puerta de enlace (20) conectado a la red de comunicación, convertir el mensaje Syslog en un mensaje IEC 61850, y
  - enviar el mensaje IEC 61850 a un Centro de Control de Red, NCC (30).
- 50 7. El procedimiento de acuerdo con la reivindicación 6, que comprende
- 55
- comparar, mediante el dispositivo de puerta de enlace, extractos de un mensaje de evento Syslog con una pluralidad de cadenas de caracteres de identificador, e
  - identificar el primer mensaje de eventos de seguridad en base a un resultado de la comparación.
- 60 8. Un dispositivo de puerta de enlace (20) en un sistema de Automatización de Subestaciones, SA, que automatiza una subestación de energía eléctrica, estando adaptado dicho dispositivo de puerta de enlace (20) para conectarse a una red de comunicación de subestaciones (15) que interconecta Dispositivos Electrónicos Inteligentes, IEDs (10, 11), que transmiten mensajes de eventos de seguridad de acuerdo con un protocolo del Comité Electrotécnico Internacional, IEC 61850-7-4, así como dispositivos de SA (12, 151, 152) que transmiten mensajes de eventos de seguridad de acuerdo a un protocolo Syslog, estando adaptado el dispositivo de puerta de enlace para recibir un mensaje de eventos de seguridad desde un IED o desde un dispositivo SA, y para asignar la información de eventos de seguridad extraída del mensaje al otro protocolo respectivo.
- 65 9. El dispositivo de puerta de enlace de acuerdo con la reivindicación 8, **caracterizado por que** está adaptado, en base a una indicación de la gravedad del evento de de seguridad del mensaje que indica una alarma, para convertir la información de eventos de seguridad extraída en un mensaje del Centro de Control de Red, NCC, de acuerdo con

## ES 2 459 119 T3

un protocolo NCC, y para proporcionar el mensaje NCC a un NCC (30) de la subestación de energía eléctrica.

10. El dispositivo de puerta de enlace de acuerdo con la reivindicación 8, **caracterizado por que** está adaptado para

- 5       - comparar los extractos de un mensaje recibido desde un dispositivo SA a una pluralidad de cadenas de caracteres de identificador,
- identificar el mensaje como un mensaje de eventos de seguridad basado en el resultado de la comparación,
- convertir el mensaje de eventos de seguridad identificados en un mensaje según el protocolo IEC 61850-7-4, y
- 10       - enviar el mensaje IEC 61850 convertido a un Centro de Control de Red, NCC (30), de la subestación de energía eléctrica.



**Fig. 1**