(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 913 434**

(51) Int. CI.:

G06F 21/55 (2013.01)
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.12.2018 E 18209769 (1)**

(97) Fecha y número de publicación de la concesión europea: **23.02.2022 EP 3663948**

(54) Título: **Reconociendo desviaciones en el comportamiento de la seguridad de unidades automatizadas**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2022

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

MAKUTH, JENS y
SCHIMMER, JÜRGEN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Reconociendo desviaciones en el comportamiento de la seguridad de unidades automatizadas

La presente invención se refiere a un método, así como a un interruptor, dispositivo y red inteligente para reconocer desviaciones en el comportamiento de comunicación de la red, según las reivindicaciones independientes. Alcances detallados adicionales se definen en las reivindicaciones dependientes. En particular, las características de la comunicación son monitoreadas y evaluadas con respecto al comportamiento de seguridad de la red utilizando un modelo de comportamiento de comunicación de la red.

La tecnología de automatización solía tener una estructura simple. Un controlador de una unidad de automatización controlaba unidades funcionales de la unidad de automatización. En sitios de automatización más grandes, varias unidades de automatización se comunicaban al estar conectadas entre sí mediante una red industrial. Sin embargo, hoy en día, la mayoría de las unidades de automatización, desde simples electrodomésticos hasta hogares inteligentes y plantas de fabricación industrial, no están aisladas sino conectadas de forma lateral a otras entidades, especialmente a través de Internet. En el curso de la creciente digitalización y, en particular, en el curso de la tendencia de Internet de las cosas (IoT), casi todas las unidades de automatización actualizadas se pueden conectar a Internet. Con la creciente interconexión entre el mundo de la tecnología de la información (IT) y el mundo de la automatización (AT) a través de Internet, los problemas antes específicos del mundo de IT también ganan cada vez más influencia en el mundo de AT. Especialmente, los problemas de seguridad se vuelven relevantes para las unidades de automatización tan pronto como estas unidades ya no están cerradas sino conectadas a Internet y, por lo tanto, abiertas a ataques desde el exterior.

Dichos problemas de seguridad son varios. La mayoría del malware (por ejemplo, gusanos informáticos como Stuxnet) se introducen en redes como Internet para realizar manipulaciones en los puntos finales de la red (por ejemplo, unidades de automatización). Pero también se introduce spyware para adquirir conocimientos (procesos, métodos, recetas, factores característicos de producción como tamaño de lote, rendimiento, eficiencia, etc.) de puntos finales (unidades de automatización, etc.). Además, los ataques de “negación de servicio” para bloquear o retrasar las comunicaciones se utilizan para dañar, por ejemplo, la producción en una celda o de una unidad de automatización.

Las contramedidas conocidas son el uso de software antivirus, el endurecimiento del dispositivo en el punto final y el control de los puertos de la terminal. El software antivirus analiza las firmas del software basándose en patrones de virus conocidos o supervisa el comportamiento de los programas. Para controlar las puertas de enlace, se utilizan firewalls, flite, proxies y similares, especialmente en combinación con ciertas arquitecturas de red para evitar infectar una gran red con muchos puntos finales a la vez.

Sin embargo, cada una de las contramedidas conocidas es específica del tipo de problema de seguridad o necesita información sobre el malware/spyware (firma) para poder proteger un punto final y/o una red.

El documento WO 2018/141432 A1 divulga un método realizado por una función de detección de ataques para la detección de un ataque distribuido en una red inalámbrica a la que se conectan múltiples dispositivos inalámbricos a través de nodos de red. Se comprueba si las características de un flujo de tráfico de cada uno de múltiples dispositivos inalámbricos cumplen o no una condición de umbral predefinida relacionada con el tráfico anómalo que se origina en los dispositivos inalámbricos. Al detectar que dichas características de flujo de tráfico cumplen con la condición de umbral, se identifican cambios en los flujos de tráfico desde los dispositivos inalámbricos, por ejemplo, basado en estadísticas sobre el tráfico anterior que se origina en los dispositivos inalámbricos. A continuación, se puede determinar si los dispositivos inalámbricos se utilizan en el ataque distribuido, basándose en dichos cambios identificados de los flujos de tráfico.

El documento US 2017/207949 A1 divulga sistemas y métodos de monitoreo para su uso en aplicaciones de seguridad, protección y procesos comerciales que utilizan un motor de correlación. Los datos sensoriales de uno o más sensores se capturan y analizan para detectar uno o más eventos en los datos sensoriales. Los eventos son correlacionados por medio de un motor de correlación. A continuación, se supervisan los eventos para detectar la ocurrencia de una o más correlaciones de interés, o uno o más eventos críticos de interés. Finalmente, se activan una o más acciones en función de la detección de una o más correlaciones de interés, uno o más eventos anómalos, o uno o más eventos críticos de interés.

El documento US 2012/137361 A1 divulga un sistema de control de seguridad de red que incluye un generador de eventos para generar eventos de red; un dispositivo de procesamiento de eventos de seguridad para recopilar los eventos de red del generador de eventos de red a través de una red y procesar los eventos de red recopilados como datos objetivo para visualización; y un dispositivo de procesamiento de visualización para observar los datos objetivo para mostrar un estado de seguridad como una información de visualización tridimensional (3D) sobre una base de organización.

El documento US 2017/093902 A1 divulga técnicas para detectar incidentes de seguridad basados en eventos de baja confianza. Un servidor de administración de seguridad agrega una colección de eventos de seguridad recibidos de los registros de uno o más dispositivos. El servidor de administración de seguridad evalúa la colección de eventos en función de una puntuación de confianza asignada a cada tipo distinto de evento de seguridad. Cada puntaje de confianza indica la probabilidad de que haya ocurrido un incidente de seguridad. El servidor de administración de seguridad determina, en

base a las puntuaciones de confianza, al menos un umbral para determinar cuándo informar sobre la ocurrencia de un incidente de seguridad a partir de la recopilación de eventos. Al determinar que al menos un evento de seguridad de la colección ha cruzado al menos un umbral, el servidor de administración de seguridad informa la ocurrencia del incidente a un analista.

El objetivo de la presente invención es superar o al menos paliar estos problemas proporcionando un método según la reivindicación independiente 1, así como un interruptor, dispositivo y sistema, de conformidad con las reivindicaciones independientes adicionales.

Otras mejoras de la presente invención son objetivo de las reivindicaciones dependientes.

Según un primer aspecto de la presente invención, un método de reconocimiento de desviaciones en el comportamiento de la comunicación de una red, en particular de una red de automatización, de conformidad con la reivindicación independiente 1, comprende las siguientes etapas:

- Recopilar los metadatos de comunicación en un interruptor de la red, en el que los metadatos de comunicación comprenden datos sobre las características de cada comunicación a través del interruptor.
- Deducir para cada comunicación a través del interruptor como máximo tres valores de seguridad a partir de los metadatos de comunicación de la respectiva comunicación, por medio de un modelo del comportamiento de comunicación de la red.
- Comprobar para cada comunicación si los respectivos como máximo tres valores de seguridad, cumplen los respectivos valores de umbral predeterminados, en donde los valores de umbral se derivan durante la generación del modelo del comportamiento de metadatos de comunicación de capacitación de la red, y en donde se comprueba si el punto de seguridad respectivo, definido por las coordenadas del valor de seguridad derivado, se encuentra dentro del sobre del modelo.
- Generar una advertencia de seguridad en caso de que al menos uno de los valores de seguridad no alcance los respectivos valores de umbral predeterminados, es decir, que los puntos de seguridad de la comunicación se encuentren fuera del sobre del modelo.

Todo o parte de las etapas anteriores se pueden ejecutar en paralelo.

De conformidad con un segundo aspecto de la presente invención, se dispone y configura un interruptor inteligente para reconocer desviaciones en el comportamiento de comunicación de una red, en particular, de una red de automatización, para implementar y ejecutar el método según el primer aspecto de la presente invención. El interruptor inteligente comprende un módulo de metadatos, un modelo del comportamiento de comunicación de la red y un módulo de seguridad. El módulo de metadatos está dispuesto y configurado para recopilar metadatos de comunicación en el interruptor inteligente. Los metadatos de comunicación comprenden datos sobre las características de cada comunicación sobre el interruptor inteligente. El modelo del comportamiento de la comunicación se acopla de forma comunicativa, al módulo de metadatos. El modelo del comportamiento de la comunicación está dispuesto y configurado para derivar para cada comunicación sobre el interruptor inteligente a la mayoría de los tres valores de seguridad de los metadatos de comunicación de la comunicación respectiva. El módulo de seguridad está acoplado de forma comunicativa, al modelo del comportamiento de la comunicación. El módulo de seguridad está dispuesto y configurado para verificar cada comunicación, ya sea que los respectivos en la mayoría de los tres valores de seguridad cumplan con los valores de umbral predeterminados respectivos de acuerdo con el método descrito por la reivindicación independiente 1. El módulo de seguridad está alejado y configurado para generar una advertencia de seguridad, en caso de que al menos uno de los valores de seguridad no cumpla con los valores de umbral predeterminados respectivos.

De acuerdo con un tercer aspecto de la presente invención, un dispositivo para reconocer las desviaciones en el comportamiento de la comunicación de una red, en particular, de una red de automatización, está dispuesta y está configurada para implementar y ejecutar el método de acuerdo con el primer aspecto de la presente invención. El dispositivo está conectado de forma comunicativa, a un interruptor de la red. El dispositivo comprende un modelo del comportamiento de la comunicación de la red y un módulo de seguridad. El modelo del comportamiento de la comunicación está dispuesto y configurado para derivar para cada comunicación sobre el interruptor en la mayoría de los tres valores de seguridad de los metadatos de comunicación de la comunicación respectiva recuperada desde el interruptor. Los metadatos de comunicación comprenden datos sobre las características de cada comunicación sobre el interruptor. El módulo de seguridad está acoplado de forma comunicativa, al modelo del comportamiento de la comunicación. El módulo de seguridad está dispuesto y configurado para verificar cada comunicación, ya sea que los respectivos valores de la seguridad cumplen con los valores de umbral predeterminados respectivos de acuerdo con el método descrito por la reivindicación independiente 1. El módulo de seguridad está dispuesto y configurado para generar una advertencia de seguridad en caso de que al menos uno de los valores de seguridad no cumpla con los valores de umbral predeterminados respectivos.

De acuerdo con un cuarto aspecto de la presente invención, se organiza un sistema y está configurado para reconocer las desviaciones en el comportamiento de la comunicación de una red. El sistema comprende una red, en particular una red de automatización, al menos dos células de red, un interruptor intelectual de acuerdo con el segundo aspecto de la presente invención, o un interruptor regular y un dispositivo de acuerdo con el tercer aspecto de la presente invención. Al menos dos celdas de red están conectadas de forma comunicativa, sobre la red. El dispositivo de acuerdo con el tercer

aspecto de la presente invención está conectado de forma comunicativa, o acoplado al interruptor regular. El interruptor inteligente de acuerdo con el segundo aspecto de la presente invención, o el interruptor regular, se encuentra en un punto de conexión central de al menos dos celdas de red en la red.

La presente invención es, en particular, aplicable a las redes industriales utilizadas para las unidades de automatización (redes de automatización). La red puede tener una topología de anillo, o una topología de estrella.

En el contexto de la presente invención, el término conectado de forma comunicativa significa que dos entidades de una red pueden comunicarse entre sí directamente, o sobre una o más entidades adicionales (por ejemplo, interruptores) en la red. En el contexto de la presente invención (comunicativa) acoplados significa que dos entidades de una red pueden comunicarse entre sí directamente a través de una conexión directa sin otras entidades en el medio.

En el contexto de la presente invención, una comunicación es el transporte (enviando y recibiendo) de al menos un mensaje de un remitente a un receptor. En particular, en un paquete basado en paquetes, envío y recepción (transporte) de la cantidad de al menos un mensaje, se realiza en forma de al menos un paquete que comprende al menos una parte del mensaje como los datos y, de manera opcional, un encabezado y/o un pie de página o cualquier metadato adicional.

De preferencia, el interruptor respectivo (inteligente), desde el cual se obtienen los metadatos, se encuentra en un punto de conexión central de la red. El punto de conexión central puede ser un punto en la red en donde todas las conexiones entre todas las entidades (por ejemplo, las celdas de la red u otras unidades) de la red se reúnen de manera que todas las comunicaciones en la red se ejecuten sobre ese punto de conexión y, por lo tanto, sobre el Interruptor respectivo (inteligente). En ese caso, todos los datos atraviesan el interruptor respectivo (inteligente) en su camino desde un remitente a un receptor (por ejemplo, de una de las celdas de la red a la otra).

En el contexto de la presente invención, los metadatos de comunicación comprenden datos sobre las características de una sola comunicación. Los metadatos de comunicación contienen al menos 10 valores que caracterizan la respectiva comunicación única. Los valores de los metadatos de la comunicación pueden comprender la latencia, la tasa de transferencia, la velocidad en baudios, el tamaño del paquete, la duración de la comunicación, el tiempo de retardo, el tiempo de tránsito, etc. En particular, los metadatos de la comunicación pueden comprender los siguientes valores:

- un número de paquete que da el número total de paquetes enviados en la comunicación.
- un conteo de paquetes actuales [pkts/s] [paquetes por segundo], lo que le da al conteo actual de paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de paquetes promedio [pkts/s] lo que da el conteo promedio de los paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de paquetes mínimos [pkts/s] lo que da el conteo mínimo de paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de paquetes máximos [pkts/s] lo que da el número máximo de los paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos actuales [kbps] [kilobit por segundo] lo que da el conteo actual de datos enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos promedio [kbps] lo que da el conteo promedio de datos enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos mínimos [kbps] lo que da el conteo mínimo de datos enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos máximo [kbps] lo que da el conteo máximo de datos enviados por unidad de tiempo (segundos) en la comunicación.

El interruptor (inteligente) de la red se monitorea con respecto a las comunicaciones que se ejecutan sobre ella o más avanzadas por ella. En el interruptor (inteligente), los metadatos de comunicación de cada comunicación se recopilan y almacenan. Cada comunicación sobre el interruptor (inteligente), por lo tanto, se caracteriza por valores como la latencia, la tasa de transferencia, la velocidad en baudios, el tamaño del paquete, la duración de la comunicación, el tiempo de retardo, el tiempo de tránsito, etc. que se comprometa a los metadatos de la comunicación respectiva.

Todos los metadatos de comunicación de las comunicaciones sobre el interruptor (inteligente) se proporcionan al modelo de la comunicación de la red, lo que da a la mayoría de los tres valores de seguridad basados en los metadatos de la comunicación. Los metadatos de comunicación pueden obtenerse desde el interruptor o, más bien, desde el módulo de metadatos del interruptor inteligente por el dispositivo, de acuerdo con el tercer aspecto de la presente invención, o el modelo del comportamiento de la comunicación.

El modelo del comportamiento de comunicación de la red puede seleccionar solo valores de los metadatos de la comunicación relacionados o contribuir a la evaluación de la seguridad de la red. La selección de dichos valores puede efectuarse ponderando los valores con pesos respectivos para aumentar o disminuir su influencia a la evaluación de la seguridad de la red. Sobre la base de todos o los valores seleccionados/ponderados de los metadatos de la comunicación, el modelo del comportamiento de comunicación deriva en la mayoría de los tres valores de seguridad para cada comunicación sobre el interruptor (inteligente). Estos valores de seguridad se asemejan al comportamiento de la

comunicación actual de la red. Los más de tres valores de seguridad describen una comunicación sobre el interruptor solo considerando los datos relevantes de seguridad de los metadatos de comunicación. Derivar a lo sumo tres valores de seguridad permite una indicación del estado de seguridad actual de la red basada en su comportamiento de comunicación que se deriva de las comunicaciones sobre el interruptor (inteligente).

Derivar a lo sumo tres valores de seguridad, que se comparan con los valores de umbral respectivos. Puede haber límites superiores y/o límites inferiores, o múltiples intervalos que tienen un límite superior y un límite inferior a los valores de umbral para cada valor de seguridad. Los valores de umbral pueden derivarse automáticamente durante la generación del modelo del comportamiento de la comunicación de la red.

Cada vez que una comunicación sobre el interruptor (inteligente) o más bien, sus valores de seguridad derivados no se ajustan a los valores de umbral, se puede generar una advertencia de seguridad. La advertencia de seguridad se puede emitir en una pantalla o a través de un altavoz (por ejemplo, administrador de red) o enviado como mensaje (correo electrónico, notificación, SMS, mensaje de empuje, etc.) a un usuario. El usuario puede decidir en función de la advertencia de seguridad, ya sea que se hayan iniciado las medidas contrarias como encapsular una celda de red afectada, o toda la red. Además, la advertencia de seguridad también se puede usar para la activación automática de las medidas de contador (por ejemplo, encapsular una celda de red afectada o la red completa).

Esta invención, que utiliza el análisis de metadatos de comunicación por medio de una ANN capacitada, permite la detección de cualquier desviación en las comunicaciones de la red de trabajo normal. Por lo tanto, incluso los problemas de seguridad nuevos y desconocidos, como nuevo malware o spyware, se pueden detectar en función del impacto e influencia en las comunicaciones en la red sobre el interruptor monitoreado (inteligente).

De acuerdo con un refinamiento de la presente invención, se derivan dos valores de seguridad o tres valores de seguridad para cada comunicación en la etapa de derivación. Los dos valores de seguridad o tres valores de seguridad definen un punto de seguridad de la comunicación respectiva en un dominio bidimensional (2D), o un dominio tridimensional (3D).

El modelo del comportamiento de la comunicación está dispuesto y configurado para derivar dos o tres valores de seguridad de los metadatos de la comunicación. Los valores que caracterizan cada comunicación sobre el interruptor (inteligente) se analizan mediante el modelo del comportamiento de comunicación con respecto a los aspectos relevantes de seguridad, y se combinan en los dos o tres valores de seguridad. Los dos valores de seguridad definen un punto de seguridad 2D (por ejemplo, en las coordenadas cartesianas). Los tres puntos de seguridad definen un punto de seguridad 3D (por ejemplo, en coordenadas cartesianas).

La derivación de dos o tres valores de seguridad, por un lado, afecta una reducción de la complejidad, en la que los puntos de seguridad 2D o 3D basados en dos o tres valores de seguridad, pueden ser más comprensibles para los usuarios (humanos), y luego, puntos de seguridad, mejor dimensionados. Por otro lado, los valores de los metadatos no se convierten demasiado (en un solo valor de seguridad), de manera que se preserva una cantidad suficiente de información de los metadatos de comunicación originales. Por lo tanto, se proporciona una indicación comprensible y precisa del estado de seguridad de la red.

De acuerdo con un refinamiento de la presente invención, el método comprende además la siguiente etapa.

-Abarcar un sobre 2D en el dominio 2D o un sobre 3D en el dominio 3D en función de los valores de umbral.

El sobre 2D define un área de umbral en el dominio 2D. El sobre 3D define un espacio de umbral en el dominio 3D. En el área de umbral y el espacio de umbral, respectivamente, todos los valores de umbral respectivos se cumplen con los puntos de seguridad respectivos. Se verifica para cada comunicación, ya sea que el punto de seguridad se encuentre dentro del sobre 2D o un sobre en 3D, o en el interior; y en el sobre 2D o en el sobre 3D o en el interior y dentro de una distancia predeterminada del sobre 2D o en 3D en la etapa de verificación.

La etapa para abarcar se puede ejecutar en paralelo a las etapas restantes.

El sobre 2D/3D permite una verificación geométrica simple de los puntos de seguridad 2D/3D de las comunicaciones sobre el interruptor (inteligente) en lugar de muchas comparaciones con dos o tres valores de umbral. Además, se puede determinar y utilizar una distancia de los puntos de seguridad 2D/3D para un análisis de seguridad adicional de las comunicaciones respectivas (mayor será la distancia, mayor será la desviación del comportamiento normal de la comunicación, que podría ser el resultado de un problema de seguridad más severa).

De acuerdo con un refinamiento de la presente invención, el método comprende además la siguiente etapa:

-Mostrar los puntos de seguridad y el sobre en una pantalla.

La etapa de visualización se puede ejecutar en paralelo a las etapas restantes.

Los puntos de seguridad 2D/3D de las comunicaciones y el sobre respectivo 2D/3D se muestran a un usuario. La pantalla

puede ser un monitor o una impresora (por ejemplo, desde una impresora) o, en particular, para los puntos de seguridad 3D y los sobres 3D, visores de realidad virtual/lentes 3D. Los puntos de seguridad 2D/3D de todas las comunicaciones o solo los puntos de seguridad actuales/3D de las últimas comunicaciones (por ejemplo, los últimos 100 o los últimos 1000) pueden mostrarse al usuario.

Dicha representación gráfica del estado de seguridad es fácil de comprender para los usuarios humanos, de manera que puedan decidir rápidamente sobre las medidas de contador adecuadas en caso de que un problema de seguridad sea evidente, en función de los puntos de seguridad mostrados.

De acuerdo con un refinamiento de la presente invención, la advertencia de seguridad se genera en caso de que al menos uno de los valores de seguridad no baste con el respectivo valor umbral predeterminado para un número predefinido de comunicaciones y/o por una duración predefinida en la etapa de generación.

Como la red es un sistema dinámico, que no siempre se comporta de la misma manera durante la operación normal (debido a las influencias del entorno/ruido), no todas las desviaciones del comportamiento de comunicación normal (todos los valores/puntos de seguridad dentro de los umbrales respectivos/sobre) debe ser el resultado de una emisión de seguridad. Por lo tanto, solo si una cantidad de comunicaciones iguales o más altas que el número predefinido se desvía con sus valores/punto de seguridad de la comunicación normal, se caracteriza por los valores/sobre de umbral, se emite una advertencia de seguridad. De forma alternativa o adicional, si todo o parte de las comunicaciones dentro de la duración predefinida se desvía de la comunicación normal se emite una advertencia de seguridad. De este modo, solo uno de los valores de seguridad puede no ser suficiente para varias comunicaciones o cualquiera de los valores de seguridad pueden no ser suficientes para varias comunicaciones. También solo si se cierra una comunicación (por ejemplo, de un remitente en particular a un receptor en particular) o tipo de comunicación (por ejemplo, los mensajes que ingresan desde Internet, las señales de control enviadas por un controlador, etc.) no se comportan como una advertencia de seguridad normal, se debe emitir una advertencia de seguridad.
no es suficiente para varias veces seguidas o en un intervalo de tiempo predefinido o con un lapso máximo predefinido, el intervalo de tiempo, cada uno que no sea suficiente.

El número predefinido de comunicaciones y/o la duración predefinida permite evitar la emisión de advertencias de seguridad falsas.

De acuerdo con un refinamiento de la presente invención, los metadatos de la comunicación son la función de limpieza de datos procesados previamente, que determina los datos válidos de los metadatos de comunicación en la etapa de derivación. Solo se proporcionan los datos validos determinados al modelo del comportamiento de comunicación para derivar la mayoría de las tres variables de seguridad.

Antes de que se alimente a los metadatos de la comunicación al modelo del comportamiento de la comunicación, se puede ejecutar una limpieza previa de datos. En los valores de limpieza de datos sobre las características de una comunicación única de los metadatos de comunicación que son erróneos, incompletos, ilógicos y/o inesperados se vuelven automáticamente. Por lo tanto, solo se limpian y, por lo tanto, valores válidos de los metadatos de comunicación que comprenden información válida sobre las comunicaciones sobre el interruptor (inteligente) se consideran y se utilizan para derivar los tres valores de seguridad por medio del modelo del comportamiento de la comunicación.

La función de limpieza de datos garantiza que el comportamiento actual de la comunicación de la red se evalúe en función de los valores/puntos de seguridad que se derivan exclusivamente de datos/valores válidos de los metadatos de comunicación. En consecuencia, aumenta la confiabilidad del comportamiento de comunicación actual de la red.

De acuerdo con un refinamiento de la presente invención, el modelo del comportamiento de la comunicación se deriva de los metadatos de la comunicación de la capacitación mediante un algoritmo de selección de pretensión hacia adelante y/o un algoritmo de selección de características hacia atrás, para derivar en la mayoría de los tres valores de seguridad. Más de tres valores de seguridad describen una comunicación sobre el interruptor solo considerando los datos relevantes de seguridad de los metadatos de comunicación.

Los metadatos de comunicación de capacitación son los metadatos de la comunicación de una red, provistos para derivar un modelo del comportamiento de la comunicación de la red respectiva. El algoritmo de selección de características hacia adelante y/o un algoritmo de selección de características hacia atrás, se utiliza para determinar los datos relevantes de seguridad de los metadatos de comunicación.

Los algoritmos usados (hacia adelante/hacia atrás) pueden ser algoritmos de fuerza bruta en algoritmos basados en la prueba y error, o basados en Gauss, basados en funciones de optimización. El algoritmo de selección de características hacia adelante/hacia atrás, puede ser compatible mediante un enfoque de “cuaderno”, como las aplicaciones web de Jupiter Notebook o Apache Zeppelin.

El algoritmo de selección hacia adelante/hacia atrás proporciona un modelo robusto que se puede usar para derivar más de tres valores de seguridad con poco esfuerzo computacional.

De acuerdo con un refinamiento de la presente invención, el algoritmo de selección de características hacia adelante y/o el algoritmo de selección de características hacia atrás son una máquina de vector de soporte (SVM), una covarianza robusta, o un algoritmo de aislamiento.

La SVM, la covarianza robusta y el aislamiento de los algoritmos de Forrest son algoritmos robustos para derivar el modelo del comportamiento de la comunicación.

De acuerdo con un nuevo refinamiento de la presente invención, el modelo del comportamiento de la comunicación se basa en una Red Neuronal Artificial (ANN). La ANN está capacitada con los metadatos de comunicación para resolver en la mayoría de los tres valores de seguridad. Los tres valores de seguridad describen una comunicación sobre el interruptor, solo considerando los datos relevantes de seguridad de los metadatos de la comunicación.

La ANN está capacitada para que solo se consideren los valores de los metadatos de comunicación relacionados con o contribuciones a la evaluación de la seguridad de la red. Esto puede efectuarse adaptando los pesos de la ANN, tal que solo dichos datos/valores relevantes de los metadatos de la comunicación se consideran para derivar los tres valores de seguridad. Incluso las dependencias complejas de múltiples valores de los metadatos de comunicación relacionados o que contribuyen a la seguridad de la red se consideran para la ANN capacitada.

La ANN proporciona valores/puntos de seguridad confiables, incluso en redes con arquitectura compleja y muchas dependencias.

De acuerdo con un refinamiento adicional de la presente invención, el modelo del comportamiento de la comunicación se deriva de los metadatos de comunicación de capacitación por un algoritmo analítico para derivar en la mayoría de los tres valores de seguridad. Los tres valores de seguridad describen una comunicación sobre el interruptor, solo considerando los datos relevantes de seguridad de los metadatos de la comunicación.

Un modelo analíticamente derivado del comportamiento de la comunicación es particularmente preciso y, de manera adicional, no computacionalmente intensivo en derivación de los tres valores de seguridad.

De acuerdo con un refinamiento de la presente invención, los metadatos de comunicación de capacitación están procesados previamente con una función de limpieza de datos que determinan los datos de capacitación válidos de los metadatos de la comunicación de capacitación. Solo se utilizan los datos de capacitación válidos determinados para resolver el modelo del comportamiento de la comunicación.

Antes de que se procesen los metadatos de la comunicación de capacitación para generar el modelo del comportamiento de la comunicación (algoritmo de selección de características o algoritmo ANN o analítico), se puede ejecutar una limpieza de datos anteriores. En los valores de capacitación de limpieza de datos sobre las características de una comunicación única de los metadatos de comunicación de capacitación que son erróneos, incompletos, ilógicos y/o inesperados se retiran automáticamente. Por lo tanto, solo los valores de capacitación limpios y, por lo tanto, válidos de los metadatos de comunicación de capacitación que comprenden información válida sobre las comunicaciones a través del interruptor (inteligente), se consideran y usan para derivar el modelo del comportamiento de comunicación.

La función de limpieza de datos garantiza que el modelo del comportamiento de comunicación de la red se base en datos de capacitación válidos/valores de los metadatos de la comunicación de capacitación. En consecuencia, se incrementa la confiabilidad del modelo del comportamiento de la comunicación. Además, en caso de que el modelo de comportamiento de comunicación se base en una ANN, la capacitación con datos/valores de capacitación válidos permite una ANN menos compleja ya que se consideran menos valores/datos de capacitación.

Según un refinamiento de la presente invención, el modelo del comportamiento de la comunicación se deriva de los metadatos de la comunicación de capacitación de las comunicaciones en una red de trabajo regular.

La comunicación en la red mientras la red se encuentra en un estado de funcionamiento regular proporciona información sobre el comportamiento de comunicación regular de la red cuando no hay problemas de seguridad. Estos metadatos de comunicación de capacitación de las comunicaciones regulares de la red para las que se va a derivar el modelo del comportamiento de la comunicación permiten derivar un modelo del comportamiento de la comunicación (algoritmo de selección de características/ANN/algoritmo analítico) que es capaz de discernir entre un estado de funcionamiento regular con un comportamiento de comunicación regular de la red respectiva y un estado de funcionamiento irregular que puede ser causado por un problema de seguridad (spyware, malware, etc.). En particular, cuando el modelo se deriva con base a metadatos de comunicación de capacitación de comunicaciones en una red que funciona regularmente. Por lo tanto, los valores de umbral predeterminados para los valores de seguridad pueden derivarse automáticamente basándose en los metadatos de comunicación de capacitación de las comunicaciones en la red de trabajo regular respectiva.

Con los metadatos de comunicación de capacitación de las comunicaciones en una red de trabajo regular, se puede derivar un modelo robusto del comportamiento de la comunicación de la red respectiva. Además, los valores de umbral pueden derivarse automáticamente.

Según un refinamiento de la presente invención, el modelo del comportamiento de la comunicación se deriva de los metadatos de la comunicación de capacitación de las comunicaciones en una red relacionada con los ataques conocidos en la red.

La comunicación en la red, mientras que la red está bajo ataque de un ataque conocido o un problema de seguridad conocido (malware, spyware, etc.) y, por lo tanto, en un estado de trabajo irregular, proporciona información sobre el comportamiento de comunicación irregular de la red cuando se conoce un problema de seguridad conocido está presente. Estos metadatos de comunicación de capacitación de las comunicaciones irregulares de la red para la cual se debe derivar el modelo del comportamiento de la comunicación (algoritmo de selección de características/ANN/algoritmo analítico) que puede identificar el problema de seguridad o la clase de problema de seguridad que está causando el estado de trabajo irregular. Además, cuando el ANN está capacitado con los metadatos de comunicación de las comunicaciones en una red, que las comunicaciones están relacionadas con ataques conocidos en la red (por ejemplo, la comunicación causada por el malware o el spyware, etc.), los valores de umbral para los valores de seguridad se pueden refinar de forma adicional, (limitado/restringido) basado en el comportamiento de la red bajo un ataque de un problema de seguridad conocido.

Por lo tanto, el modelo derivado del comportamiento de la comunicación es capaz de identificar directamente cualquier problema de seguridad conocido que causa un comportamiento de comunicación irregular de la red respectiva (si se utilizaron metadatos de comunicación de la red respectiva que está bajo ataque por el problema de seguridad actual para derivar el modelo utilizado del comportamiento de comunicación). Además, los valores del umbral pueden ser refinados de forma automática.

De acuerdo con un refinamiento de la presente invención, el modelo del comportamiento de la comunicación se deriva de los metadatos de la comunicación de capacitación de las comunicaciones en una red de operación realmente existente y/o actual.

Una red existente (por ejemplo, una planta de fabricación existente que tiene varias unidades de automatización conectadas a través de una red industrial) se puede ampliar con un interruptor inteligente, de acuerdo con el segundo aspecto de la presente invención, o con un interruptor regular y un dispositivo, de acuerdo con el tercer aspecto de la invención, en donde dicho interruptor/dispositivo inteligente comprende un modelo del comportamiento de comunicación de la red existente simplemente leyendo los metadatos de comunicación de las comunicaciones en la red existente mientras está funcionando.

En consecuencia, las redes existentes pueden ser expulsadas de manera tal que pueden reconocer las desviaciones en el comportamiento de la comunicación y, por lo tanto, descubrir los problemas de seguridad sin o con un mínimo de tiempo de inactividad de la red existente. Además, el modelo así derivado del comportamiento de la comunicación se ajusta exactamente a la red existente.

De acuerdo con un refinamiento de la presente invención, el modelo del comportamiento de la comunicación se deriva de los metadatos de la comunicación de capacitación de las comunicaciones en un gemelo digital de la red.

El modelo del comportamiento de la comunicación de la red se puede derivar en función de las comunicaciones simuladas en un gemelo digital (modelo digital) de la red. En el gemelo digital, que solo los modelos (pero todas) las entidades relevantes de la red, los metadatos de comunicación de la comunicación simulada (regular y/o irregular) se utilizan para derivar el modelo del comportamiento de la comunicación de la red real.

Por ejemplo, directamente después de colocar una unidad de automatización o una planta de fabricación y antes de configurar la unidad de automatización/planta de fabricación (incluso antes de que la unidad de automatización/planta de fabricación real esté construida en el mundo real) y se conecte a Internet, el modelo respectivo del comportamiento de la comunicación de la red real (aún no existente) se puede generar. Por lo tanto, tan pronto como se usa la red real respectiva de la unidad de automatización/planta de fabricación, la seguridad se puede observar por medio de cualquiera de los aspectos de acuerdo con la presente invención. Por lo tanto, no existe una brecha de seguridad entre la configuración de la unidad de automatización/planta de fabricación y su inicio.

De acuerdo con un refinamiento de la presente invención, el dispositivo de acuerdo con el tercer aspecto de la presente invención, es un dispositivo vanguardista acoplable al interruptor.

Un dispositivo de borde (por ejemplo, computadora separada) se puede reequipar y conectar a un interruptor existente de una red existente, incluso durante el tiempo de ejecución. Por lo tanto, el interruptor existente no debe ser reemplazado con un interruptor inteligente, de conformidad con el segundo aspecto de la presente invención. Además, el dispositivo de borde separado tiene suficiente energía de cómputo para ejecutar la ANN, de tal manera que el interruptor existente no esté sobrecargado debido a tareas computacionales adicionales.

La presente invención y su campo técnico se explican posteriormente con más detalle por un alcance, a modo de ejemplo, mostrado en las Figuras. El ejercicio a modo de ejemplo solo conduce mejor la comprensión de la presente invención y, en ningún caso, se debe interpretar como limitante para el alcance de ésta. En particular, es posible extraer aspectos del

sujeto descrito en la Figura y combinarlo con otros componentes y hallazgos de la presente descripción o las Figuras, si no se describe explícitamente de manera diferente. Los signos de referencia iguales se refieren a los mismos objetos, de modo que las explicaciones de otras cifras pueden utilizarse de forma complementaria.

La Figura 1 muestra un diagrama de flujo esquemático del método, de acuerdo con el primer aspecto de la presente invención.

La Figura 2 muestra una vista esquemática de un sistema que comprende una red, de acuerdo con el cuarto aspecto de la presente invención, con un interruptor inteligente, de acuerdo con el segundo aspecto de la presente invención.

La Figura 3 muestra una vista esquemática de un sistema que comprende una red, de acuerdo con el cuarto aspecto de la presente invención, con un interruptor regular y un alcance del dispositivo de acuerdo con un segundo aspecto de la presente invención.

La Figura 4 muestra una vista esquemática de un sistema que comprende una red, de acuerdo con el cuarto aspecto de la presente invención, con un interruptor regular y un alcance adicional del dispositivo, de acuerdo con el tercer aspecto de la presente invención.

La Figura 5 muestra una vista esquemática de un sistema que comprende una red, de acuerdo con el cuarto aspecto de la presente invención, con un interruptor regular y otro alcance adicional de acuerdo con el dispositivo, ingresando al tercer aspecto de la presente invención.

La Figura 6 muestra una vista esquemática de un interruptor inteligente, de acuerdo con el segundo aspecto de la presente invención.

La Figura 7 muestra una vista esquemática de un dispositivo, de acuerdo con el tercer aspecto de la presente invención.

En la Figura 1, se muestra un diagrama de flujo de un método de reconocimiento de las desviaciones en el comportamiento de la comunicación de una red, de acuerdo con el primer aspecto de la presente invención. En una etapa de recolección 1 de la comunicación, se recogen metadatos. En la etapa de derivación se derivan 2 tres valores de seguridad. En la etapa de la verificación 3 se verifican los valores de seguridad. En la etapa de generación 4 se genera una advertencia de seguridad. Además, en una etapa opcional para abarcar 5a un sobre tridimensional (3D) se extiende en función de los valores de umbral y en una etapa opcional para mostrar 6 puntos de seguridad 3D y el sobre 3D.

La recolección 1 puede ser una recolección de los metadatos de la comunicación en o una recuperación de los metadatos de la comunicación desde un interruptor de la red. Cada comunicación comprende enviar al menos un mensaje de un remitente a un receptor en donde se recibe el mensaje para su procesamiento adicional. El mensaje se puede enviar a través de al menos un paquete, en donde el paquete comprende datos de al menos una parte del mensaje y, de manera opcional, un encabezado y/o un pie de página y/o metadatos adicionales. Cuando se envía al menos un mensaje o paquete sobre el interruptor, se generan metadatos de comunicación. Los metadatos de comunicación comprenden datos sobre las características de cada comunicación sobre el interruptor:

- un número de paquete que da el número total de paquetes enviados en la comunicación.
- un conteo de paquetes actuales [pkts/s] [paquetes por segundo], lo que le da al conteo actual de paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de paquetes promedio [pkts/s] lo que da el conteo promedio de los paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de paquetes mínimos [pkts/s] lo que da el conteo mínimo de paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de paquetes máximos [pkts/s] lo que da el número máximo de los paquetes enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos actuales [kbps] [kilobit por segundo] lo que da el conteo actual de datos enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos promedio [kbps] lo que da el conteo promedio de datos enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos mínimos [kbps] lo que da el conteo mínimo de datos enviados por unidad de tiempo (segundos) en la comunicación.
- un conteo de datos máximo [kbps] lo que da el conteo máximo de datos enviados por unidad de tiempo (segundos) en la comunicación.

En la derivación 2 para cada comunicación sobre el interruptor, tres valores de seguridad se derivan de los metadatos de la comunicación respectiva. Cada conjunto de tres valores de seguridad de una comunicación respectiva define un punto de seguridad de la comunicación respectiva en las coordenadas cartesianas en 3D. La derivación 2 se efectúa por medio de un modelo del comportamiento de la comunicación de la red. El modelo del comportamiento de la comunicación se puede derivar de los metadatos de la comunicación de capacitación de las comunicaciones sobre el interruptor en la red. Los metadatos de la comunicación de capacitación se recolectan en la red o en un gemelo digital simulado de la red,

mientras que funcionan regularmente y /o mientras están en ataque de un problema de seguridad conocido y, por lo tanto, funciona de manera irregular. El modelo se puede derivar por medio de un algoritmo de selección de características hacia adelante y/o un algoritmo de selección de características hacia atrás, como una máquina de vector de soporte, covarianza robusta, o algoritmo de aislamiento Forrest para derivar en la mayoría de los tres valores de seguridad que describen una comunicación sobre el interruptor solo tiene en cuenta los datos relevantes de seguridad de los metadatos de comunicación. De forma alternativa, el modelo se puede resolver mediante un algoritmo analítico para derivar en la mayoría de los tres valores de seguridad que describen una comunicación sobre el interruptor, solo considerando datos relevantes de seguridad de metadatos de comunicación. Además, el modelo se puede basar en una red neuronal artificial (ANN) que se formó con los metadatos de la comunicación de capacitación para derivar en la mayoría de los tres valores de seguridad que describen una comunicación sobre el interruptor.

En la expansión opcional 5, el sobre 3D se expande en el dominio 3D. El sobre 3D define un espacio en coordenadas cartesianas 3D en donde los respectivos puntos de seguridad cumplen todos los valores de umbral respectivos. Los valores de umbral predeterminados se determinan automáticamente durante la derivación del modelo o en la capacitación de la ANN. El comportamiento de comunicación regular de la red está descrito por el sobre 3D (o más bien por los valores del umbral).

Durante la verificación 3 para cada comunicación es comprobado si el punto de seguridad respectivo se encuentra dentro o en el sobre 3D (o más bien si los tres valores de la seguridad cumplen con los valores de umbral predeterminados respectivos). Si un punto de seguridad se encuentra fuera del sobre 3D, la comunicación respectiva en la red es una comunicación irregular que podría ser causada por un problema de seguridad como el malware o el spyware, la red se ha infectado.

En caso de que al menos un punto de seguridad se encuentra fuera, el sobre 3D (o más bien al menos uno de los valores de seguridad no cumple con los valores de umbral predeterminados respectivos) se genera la advertencia de seguridad. Para evitar falsas alarmas debido a las perturbaciones de la red desde el exterior no relacionadas con un problema de seguridad, la generación 4 puede restringirse a los casos en los que el número definido de comunicaciones en una fila y/o dentro de una duración predefinida, no cumple con los criterios para una comunicación regular definida por el sobre 3D (valores de umbral predeterminados). La advertencia de seguridad puede mostrarse en un monitor, o puede reproducirse a través de un altavoz o puede ser reenviada como un mensaje a un usuario, como un administrador de red.

Los puntos de seguridad 3D de todos, o un número predefinido de comunicaciones recientes sobre el interruptor y el sobre 3D, se pueden mostrar al usuario en un monitor o por medio de visores de realidad virtual/lentes 3D.

En caso de que se genere una advertencia de seguridad, se pueden iniciar automáticamente medidas. Dichas medidas contadoras como la encapsulación de la celda de la red respectiva o la red completa son bien conocidas y, por lo tanto, no se discuten más.

En la Figura 2 se representa en un esquema, un sistema 20 que comprende una red 21, de acuerdo con el cuarto aspecto de la presente invención, con un interruptor inteligente 11 para reconocer las desviaciones en el comportamiento de la comunicación de la red 21, de acuerdo con el segundo aspecto de la presente invención. El sistema 20 es una unidad de automatización. La red 21 comprende tres celdas de red 22.1, 22.2, en donde una celda de red es una celda de control 22.1 y las dos celdas de red restantes 22.2 son celdas de red regulares 22.2. Las celdas de red 22.2 pertenecen cada una a una célula de automatización respectiva de la unidad de automatización 20. La celda de control 22.1 y las dos celdas de red 22.2 están conectadas de forma comunicativa a través del interruptor inteligente 11. Cada una de las celdas de red 22.2 comprende un interruptor 23 de entidades de red como controladores 24, y dispositivos de automatización (sensores, actores, etc.) 25 de las celdas de la red 22.2 se conectan de forma comunicativa, a través del interruptor respectivo 23, que conecta de forma comunicativa a la celda de red respectiva 22.2 con la red 21. La celda de control 22.1 también comprende un interruptor 23 que conecta la celda de control 22.1 a la red 21. Además, la celda de control 22.1 comprende al menos una computadora 26 (por ejemplo, un terminal de control o PC, y similares). Una computadora 26 puede tener una conexión 27 a la Internet, a través de la cual, el malware, spyware y otros problemas de seguridad, pueden infectar y atacar la red 21.

El interruptor inteligente 11 está dispuesto y concluido para implementar y ejecutar el método de la Figura 1. Al mismo tiempo, el interruptor inteligente 11 comprende un módulo de metadatos, un modelo del comportamiento de la comunicación de la red 21 y un módulo de seguridad. El módulo de metadatos está conectado de forma comunicativa, al modelo del comportamiento de comunicación que está conectado de forma comunicativa, al módulo de seguridad. El módulo de metadatos está dispuesto y configurado para implementar y ejecutar la recolección 1, de acuerdo con el método de la Figura 1. El modelo del comportamiento de la comunicación se encuentra y está configurado para implementar y ejecutar el derivado 2 del método de la Figura 1. El módulo de seguridad está dispuesto y configurado para implementar y ejecutar la generación 4 y de forma opcional, la expansión 5 del método de la Figura 1. La visualización puede ser ejecutada por una de las computadoras 26 que tienen un monitor correspondiente o visores de realidad virtual/lentes 3D.

En caso de que la red 21 sea atacada desde el interior con un malware como un gusano, el comportamiento regular de la comunicación de la Red 21 cambia a un comportamiento irregular de la comunicación. Este comportamiento irregular de la comunicación se parece a los metadatos respectivos de la comunicación que se traduce en respectivos puntos de

seguridad irregulares por el modelo del comportamiento de comunicación del interruptor inteligente 11. Los puntos de seguridad irregulares se encuentran fuera del sobre 3D y, por lo tanto, una advertencia de seguridad es generada por el módulo de seguridad del interruptor inteligente 11. De manera opcional, el interruptor inteligente 11 puede iniciar automáticamente las medidas del contador en respuesta al problema de seguridad detectado, en función de la comunicación irregular sobre el interruptor inteligente 11.

En las Figuras de la 3 a la 5 se presenta en un esquema, el sistema 20 que comprende la red 21 de acuerdo con el cuarto aspecto de la presente invención, con un interruptor regular 28 y un dispositivo 12 para reconocer las desviaciones en el comportamiento de la comunicación de la red 21, de acuerdo con el segundo aspecto de la presente invención. Los alcances representados en las Figuras de la 3 a la 5 tienen diferentes organizaciones del dispositivo 12, en relación con el interruptor regular 28. En las siguientes diferencias solo al sistema 20 y se discuten la red 21 de la Figura 2. En las Figuras de la 3 a la 5, el interruptor normal 28 conecta las dos celdas de red 22.2 y la celda de control 22.1 entre sí. En la Figura 3, el dispositivo 12 se acopla de forma comunicativa, al interruptor regular 12. En la Figura 4, el dispositivo 12 se encuentra en el control celular 22.1 y conectado de forma comunicativa al interruptor regular 28, a través del interruptor 23 de la celda de control 22.1. En la Figura 5, el dispositivo 12 se encuentra en una de las celdas de la red 22.2, y conectado de forma comunicativa al interruptor regular 28, a través del interruptor 23 de la celda de red respectiva 22.2.

El dispositivo 12 está dispuesto y configurado para implementar y ejecutar el método de la Figura 1. Al mismo tiempo, el dispositivo 12 comprende un modelo del comportamiento de comunicación de la red 21 y un módulo de seguridad. El modelo del comportamiento de la comunicación está comunicado con el módulo de seguridad. Los metadatos de la comunicación se obtienen desde el interruptor 28 por el dispositivo 12 para el modelo del comportamiento de la comunicación. El modelo del comportamiento de la comunicación está dispuesto y configurado para implementar y ejecutar el desarrollo 2 del método de la Figura 1. El módulo de seguridad está dispuesto y configurado para implementar y ejecutar la generación 4 y, de manera opcional, el del método de la Figura 1.

En la Figura 6 se presenta en un esquema, un interruptor inteligente 11, de acuerdo con el segundo aspecto de la presente invención. El interruptor inteligente 11 está conectado a la celda de control y las celdas de la red en los interruptores correspondientes 23 de las respectivas celdas de control/red. El interruptor inteligente 11 comprende un módulo de metadatos 13, un modelo 14 del comportamiento de la comunicación de la red 21, y un módulo de seguridad 15. El módulo de metadatos 13 está conectado de forma comunicativa al modelo 14 del comportamiento de la comunicación que se conecta de forma comunicativa al módulo de seguridad 15.

Los mensajes que atraviesan el interruptor inteligente 11 del interruptor 23 de una celda de control/red al interruptor 23 de otra célula de control/red se evalúa mediante el módulo de metadatos 13 con respecto a las características mencionadas anteriormente de las comunicaciones. Los metadatos de comunicación sobre el interruptor inteligente 11 se generan y (temporalmente) almacenan. Los metadatos de comunicación sobre el interruptor inteligente 11 se reenvían desde el módulo de metadatos 13 al modelo 14 del comportamiento de la comunicación o se obtiene por el modelo 14 del comportamiento de la comunicación del módulo de metadatos 13. El modelo 14 del comportamiento de la comunicación deriva los tres valores de seguridad y genera un punto de seguridad en 3D correspondiente para cada comunicación sobre el interruptor inteligente 11. Cada punto de seguridad en 3D se reenvía o se reduce por el módulo de seguridad 15. El módulo de seguridad 15 comprueba si los puntos de seguridad se encuentran dentro o sobre (en el espacio) en las coordenadas cartesianas en 3D. En caso de que uno o varios puntos de seguridad no cumplan con los valores de umbral que abarca el sobre, ya que se encuentran fuera del sobre, el módulo de seguridad 15 genera una advertencia de seguridad, tal como se describe anteriormente.

En la Figura 7, se representa en un esquema, un dispositivo 12 según el tercer aspecto de la presente invención. A continuación, solo se describirán las diferencias con el interruptor inteligente. El interruptor normal 28 está conectado a la celda de control y a las celdas de red en los correspondientes interruptores de las respectivas celdas de control/red. El dispositivo 12 comprende un modelo 14 del comportamiento de comunicación de la red 21 y un módulo de seguridad 14. El interruptor regular 28 está conectado de forma comunicativa al modelo 14 del comportamiento de comunicación del dispositivo 12 que está conectado de forma comunicativa al módulo de seguridad 15.

Los mensajes que atraviesan el interruptor regular 28 desde el interruptor de una celda de control/red al interruptor de otra celda de control/red son evaluados por el interruptor regular 28 con respecto a las características de comunicaciones antes mencionadas, por ejemplo, en un módulo de metadatos del interruptor regular 28. Los metadatos de comunicación de cada comunicación a través del interruptor normal 28 se generan y (temporalmente) se almacenan. Los metadatos de comunicación de cada comunicación a través del interruptor normal 28 se envían al modelo 14 del comportamiento de comunicación del dispositivo 12, o son obtenidos por el modelo 14 del comportamiento de comunicación del dispositivo 12 desde el interruptor normal 28 (desde el módulo de metadatos de el interruptor normal 28).

Aunque los alcances específicos han sido ilustrados y descritos en el presente documento, se apreciará por las habilidades ordinarias en la técnica, que existen una variedad de implementaciones alternativas y/o equivalentes. Cabe apreciar que el alcance o los alcances son solo ejemplos, y no se pretende que limiten el alcance, la aplicabilidad o la configuración de ninguna manera. Más bien, el resumen anterior y la descripción detallada proporcionará a los expertos en la técnica con un mapa de ruta más grande para implementar al menos un alcance, a modo de ejemplo, comprendiendo que se pueden hacer varios cambios en la función y la disposición de los elementos descritos en un alcance, a modo de ejemplo, sin

salida del alcance tal como se establece en los mensajes adjuntos que atraviesan el interruptor regular 28 de las reivindicaciones.

En la descripción detallada anterior, varias características se agrupan en uno o más ejemplos con el fin de racionalizar la divulgación. Se entiende que la descripción anterior está destinada a ser ilustrativa, y no restrictiva.

La nomenclatura específica utilizada en la descripción anterior se utiliza para proporcionar una comprensión profunda de la invención. Sin embargo, será evidente para un experto en la técnica a la luz de la especificación proporcionada en este documento, que los detalles específicos no son necesarios para practicar la invención. Por lo tanto, las descripciones anteriores de alcances específicos de la presente invención se presentan con fines de ilustración y descripción. A lo largo de la especificación, los términos “incluyendo” y “en los que se incluyen”, se utilizan como los equivalentes de inglés simple de los términos respectivos “que comprenden” y “en donde”, respectivamente. Más aún, los términos “primero”, “segundo”, y “tercero”, etc., se usan simplemente como etiquetas, y no están destinados a imponer requisitos numéricos para establecer cierta calificación en la importancia de los objetos. En el contexto de la presente descripción, la conjunción “o” debe entenderse para incluir (“y / o”) y no para excluir (“este o esto”).

REIVINDICACIONES

1.Método de reconocimiento de las desviaciones en el comportamiento de la comunicación de una red (21) que comprende las siguientes etapas:

- recopilación (1) de metadatos de comunicación en un interruptor (11, 28) de la red (21), en el que los metadatos de comunicación comprenden datos sobre las características de cada comunicación sobre el interruptor (11, 28).
- derivación (2) para cada comunicación sobre el interruptor (11, 28) dos valores de seguridad o tres valores de seguridad de los metadatos de comunicación, y un umbral respectivo de valores derivados durante la generación de un modelo (14) del comportamiento de la comunicación derivado de los metadatos de la comunicación de capacitación de la red (21).
- expansión (5) de un sobre 2D en el dominio 2D, o un sobre 3D en el dominio 3D basado en los valores de umbral, el sobre que define un área en el dominio 2D o un espacio en el estado 3D, en donde todos los valores de umbral respectivos cumplen los puntos de seguridad respectivos.
- comprobación (3) para cada comunicación, ya sea los respectivos en la mayoría de los tres valores de seguridad cumplen con los respectivos valores de umbral predeterminados, en los que se revisa para cada comunicación, ya sea que el punto de seguridad, que se define por los valores de seguridad derivados, se encuentra dentro o en el sobre.
- generación (4) de una advertencia de seguridad en caso de que al menos uno de los puntos de seguridad de la comunicación se encuentre fuera del sobre.

2. Método de conformidad con la reivindicación 1,

en donde en la etapa de derivación (2) se derivan dos valores de seguridad o tres valores de seguridad para cada comunicación, y
en donde los dos valores de seguridad o tres valores de seguridad definen un punto de seguridad de la comunicación respectiva en un dominio bidimensional, 2D, o tridimensional, 3D.

3. Método de conformidad con la reivindicación 1, que comprende además la etapa de:

- visualización (6) de los puntos de seguridad y el empleo en una pantalla.

4. Método de conformidad con cualquiera de las reivindicaciones precedentes,
en donde la etapa de generación (4), la advertencia de seguridad se genera, en caso de que al menos uno de los valores de seguridad no satisfaga el valor de umbral predefinido respectivo para un número predefinido de comunicaciones y/o por una duración predefinida.

5. Método de conformidad con cualquiera de las reivindicaciones precedentes,

en donde en la etapa de derivación (2) de los valores de seguridad, los metadatos
de comunicación están previamente procesados con una función de limpieza de datos que determina datos válidos de los metadatos de comunicación, y en los que solo se proporcionan los datos validos determinados al modelo (14) del comportamiento de la comunicación para derivar la mayoría de las variables de seguridad.

6. Método de conformidad con cualquiera de las reivindicaciones precedentes,
en donde modelo (14) del comportamiento de la comunicación se deriva de metadatos de comunicación de capacitación, mediante un algoritmo de selección de características hacia adelante y/o un algoritmo de selección de características hacia atrás, para derivar en la mayoría de los tres valores de seguridad que describen un comunicación sobre el interruptor (11, 28), solo considerando los datos relevantes de la seguridad de los metadatos de la comunicación.

7. Método de conformidad con la reivindicación 6,
en donde el algoritmo de selección de características hacia adelante y/o el algoritmo de selección de características hacia atrás, es una máquina de vector de soporte, una covarianza robusta o un algoritmo de aislamiento.

8. Método de conformidad con cualquiera de las reivindicaciones de la 1 a la 5,
en donde el modelo (14) del comportamiento de la comunicación se basa en una red neuronal artificial (ANN) capacitada con metadatos de comunicación de capacitación para determinar en la mayoría de los tres valores de seguridad que describen una comunicación sobre el interruptor (11, 28) solo considerando los datos relevantes de la seguridad de los metadatos de la comunicación.

9. Método de conformidad con cualquiera de las reivindicaciones de la 1 a la 5,
en donde el modelo (14) del comportamiento de la comunicación se deriva de metadatos de comunicación de capacitación por medio de un algoritmo analítico para derivar a lo sumo tres valores de seguridad que describen una comunicación sobre el interruptor (11, 28) teniendo en cuenta solo los datos relevantes para la seguridad de los metadatos de comunicación.

10. Método de conformidad con cualquiera de las reivindicaciones de la 6 a la 9,

en donde los metadatos de la comunicación de capacitación están previamente procesados con una función de limpieza de datos que determinan los datos de capacitación válidos de los metadatos de comunicación de capacitación, y
en donde solo se utilizan los datos de capacitación válidos determinados para derivar el modelo (14) del comportamiento de la comunicación.

11. Método de conformidad con cualquiera de las reivindicaciones de la 6 a la 10,

en donde el modelo (14) del comportamiento de la comunicación es un modelo robusto
derivado de metadatos de comunicación de capacitación en una red de trabajo regular (21).

12. Método de conformidad con cualquiera de las reivindicaciones de la 6 a la 11,
en donde el modelo (14) del comportamiento de la comunicación se deriva de metadatos de comunicación de capacitación en una red (21) relacionada con ataques conocidos en la red (21).

13. Método de conformidad con cualquiera de las reivindicaciones de la 6 a la 12,
en donde el modelo (14) del comportamiento de la comunicación se deriva de los metadatos de la comunicación de capacitación de las comunicaciones en una red que en realidad existente y/o actualmente se encuentra en operación (21).

14. Método de conformidad con cualquiera de las reivindicaciones de la 6 a la 13,
en donde el modelo (14) del comportamiento de la comunicación se deriva de los metadatos de comunicación de capacitación de las comunicaciones en un gemelo digital de la red (21).

15. Interruptor inteligente (11) para reconocer las desviaciones en el comportamiento de la comunicación de una red (21) arreglada y configurada para implementar y ejecutar el método de acuerdo con la reivindicación 1, que comprende:

- un módulo de metadatos (13) dispuesto y configurado para recopilar (1) metadatos de comunicación en el interruptor inteligente (11), en el que los metadatos de comunicación comprenden datos sobre las características de cada comunicación sobre el interruptor inteligente (11).
- un modelo (14) del comportamiento de comunicación de la red (21) acoplado de forma comunicativa, al módulo de metadatos (13) y está dispuesto y configurado para derivar (2) para cada comunicación sobre el interruptor inteligente (11) dos valores de seguridad o tres valores de seguridad de los metadatos de la comunicación de la comunicación respectiva, y los valores de umbral derivados durante la generación del modelo del comportamiento de la comunicación derivados de los metadatos de la comunicación de capacitación de la red.
- un módulo de seguridad (15) acoplado de forma comunicativa, al modelo (14) de la comunicación y dispuesta y está dispuesta y configurada para la ampliación (5) un sobre 2D en el dominio 2D o en un sobre 3D en el dominio 3D basado en el Los valores de umbral, el sobre que define un área en el dominio 2D o un espacio en el dominio 3D donde se cumplen todos los valores de umbral respectivos por los puntos de seguridad respectivos, para verificar (3) para cada comunicación, ya sea respectiva a la mayoría de las tres seguros de seguridad. Los valores cumplen con los respectivos valores de umbral predeterminados, en los que se verifica para cada comunicación, ya sea que el punto de seguridad, que se define por los valores de seguridad derivados, se encuentra dentro o en el sobre, y para generar (4) una advertencia de seguridad en caso de que al menos uno de los puntos de seguridad de la comunicación se encuentra fuera del sobre.

16. Interruptor inteligente (11) según la reivindicación 15, en el que el interruptor inteligente (11) está dispuesto y configurado para implementar y ejecutar el método de acuerdo con cualquiera de las reivindicaciones de la 2 a la 13.

17. Dispositivo (12) para reconocer las desviaciones en el comportamiento de la comunicación de una red (21) dispuesta y concluido para implementar y ejecutar el método de acuerdo con la reivindicación 1 y con conexión comunismo a un interruptor (28) de la red (21), que comprende:

- un modelo (14) del comportamiento de la comunicación de la red (21) dispuestos y configurados para derivar (2) para cada comunicación sobre el interruptor (28) dos valores de seguridad o tres valores de seguridad de los metadatos de comunicación de la comunicación respectiva recuperada Desde el interruptor (28), en el que los metadatos de comunicación comprenden datos sobre las características de cada comunicación sobre el interruptor (28) y para resolver los valores de umbral de la generación del modelo del comportamiento de la comunicación derivados de los metadatos de la comunicación de capacitación de la red.
-un módulo de seguridad (15) acumulado de forma comunicativa, al modelo (14) de la comunicación, hablado y dispuesto y configurado para abarcar (5) un sobre 2D en el dominio 2D o un sobre 3D en el dominio 3D basado en el Los valores de umbral, el sobre que define un área en el dominio 2D o un espacio en el dominio 3D donde se cumplen todos los valores de umbral respectivos por los puntos de seguridad respectivos, para verificar (3) para cada comunicación, ya sea máximo tres valores de seguridad cumplen con los valores de umbral predeterminados informativos, en los que se verifica para cada comunicación, ya sea que el punto de seguridad está definido por los valores de seguridad derivados, se encuentra dentro o en el sobre, y para generar (4) una seguridad advirtiendo en Caso al menos uno de los puntos de seguridad de la comunicación se encuentra fuera del sobre.

18. Dispositivo (12) de conformidad con la reivindicación 17, en el que el dispositivo (12) está dispuesto y configurado para implementar y ejecutar el método de acuerdo con cualquiera de las reivindicaciones de la 2 a la 14.

19. Dispositivo (12) de conformidad con la reivindicación 17 o 18, en el que el dispositivo (12) es un dispositivo de borde acoplable al interruptor (28).

20. Sistema (20) dispuesto y configurado para reconocer desviaciones en el comportamiento de la comunicación de una red (21), que comprende:

- una red (21).
- al menos dos células de red (22.1, 22.2) comunicativas conectadas sobre la red (21).
- un interruptor inteligente (11) según la reivindicación 15 o 16.
- un interruptor regular (28) y un dispositivo (12) de acuerdo con cualquiera de las reivindicaciones de la 17 a la 19 conectadas de forma comunicativa o acoplada en el interruptor regular (28), en el que se encuentra el interruptor inteligente (11) o el interruptor regular (28) en un punto de conexión central de las al menos dos celdas de red (22.1, 22.2) en la red (21).

FIG 1

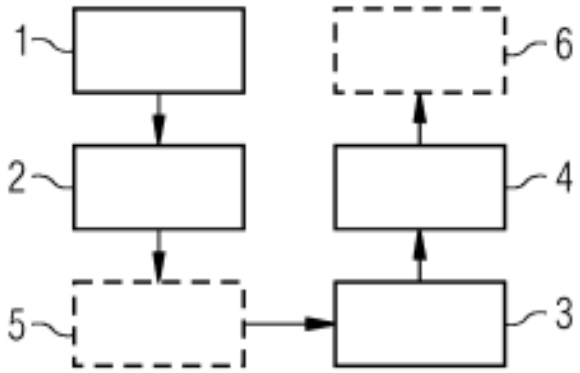

FIG 2

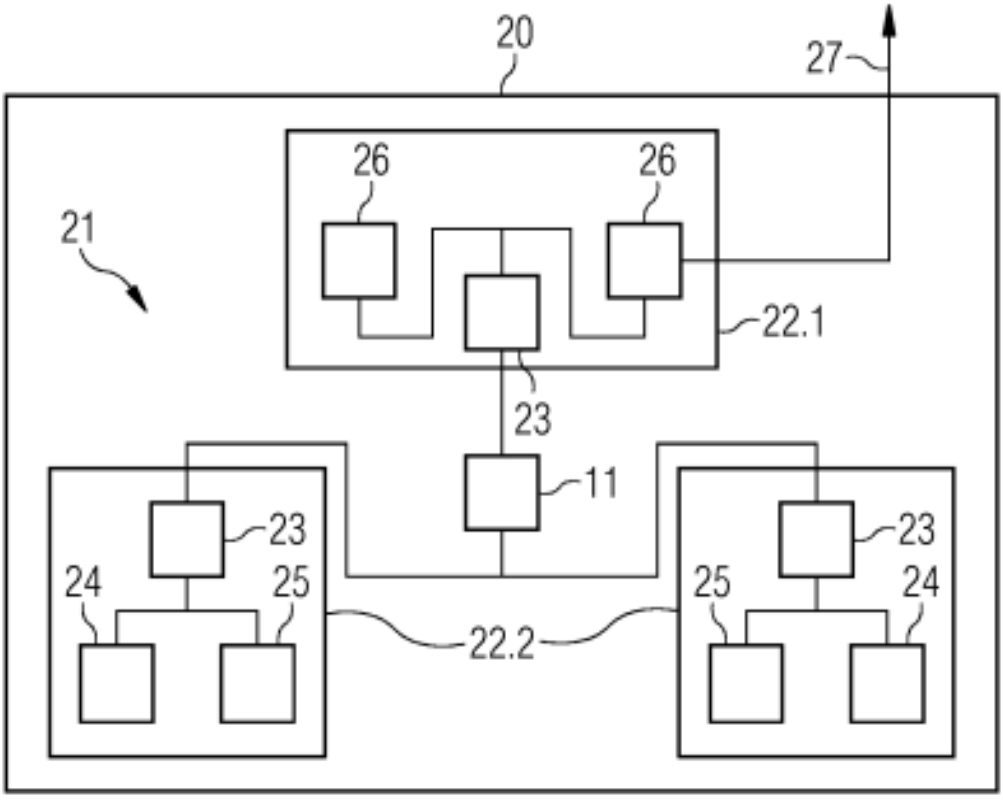

FIG 3

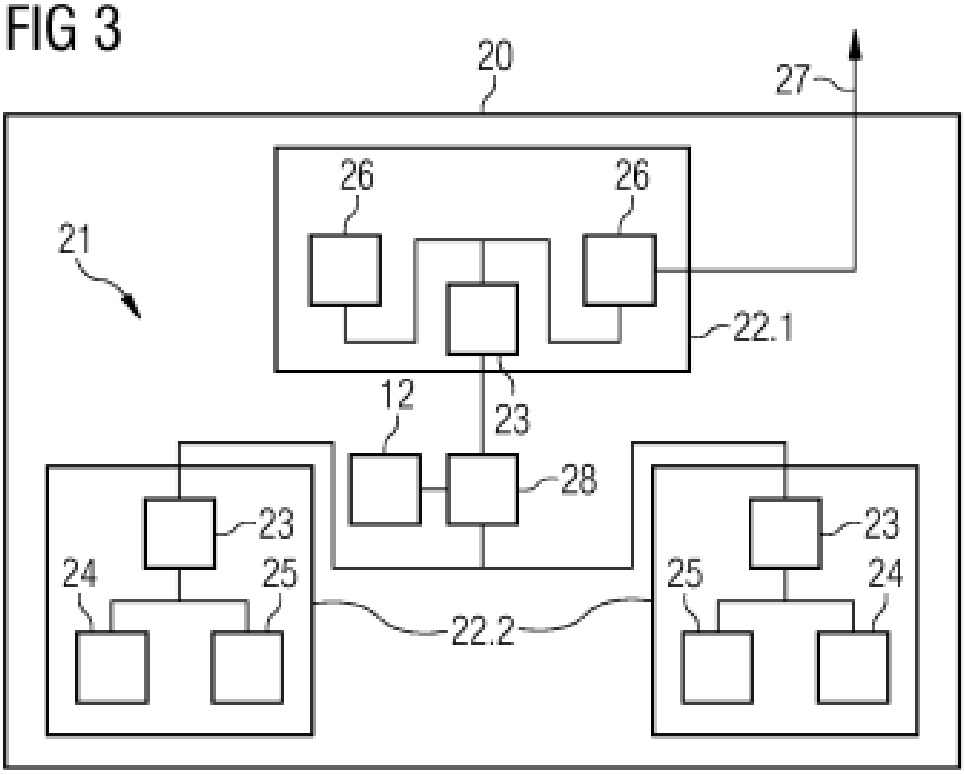
20
27
26
26
21
22.1
12
23
28
23
23
24
25
25
24
22.2

FIG 4

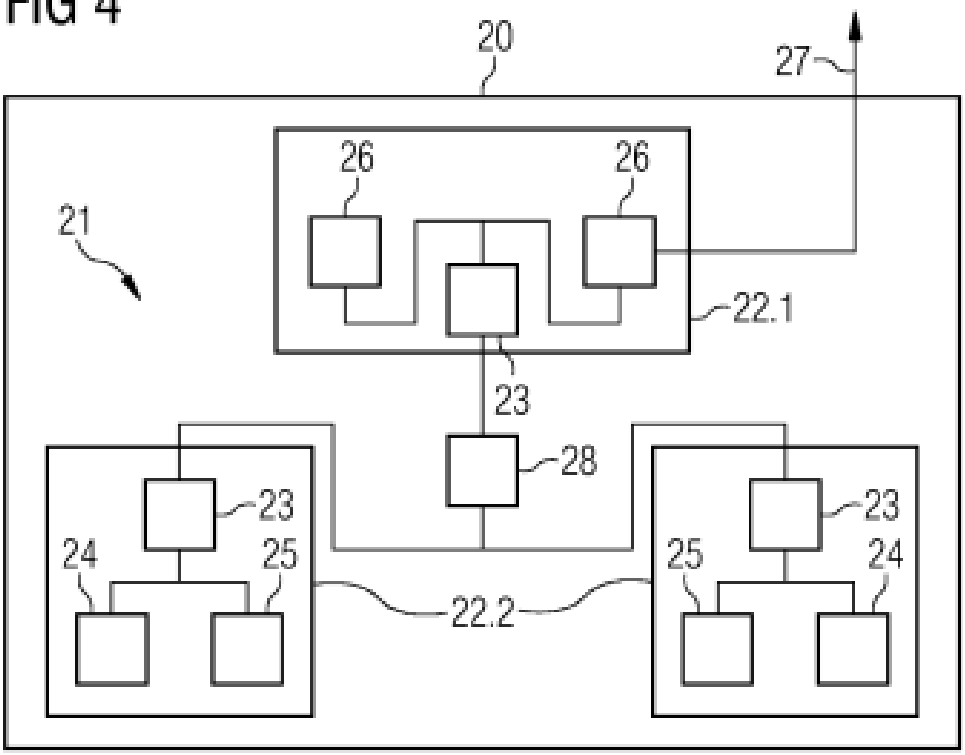
20
27
26
26
21
22.1
23
28
23
23
24
25
25
24
22.2

FIG 5

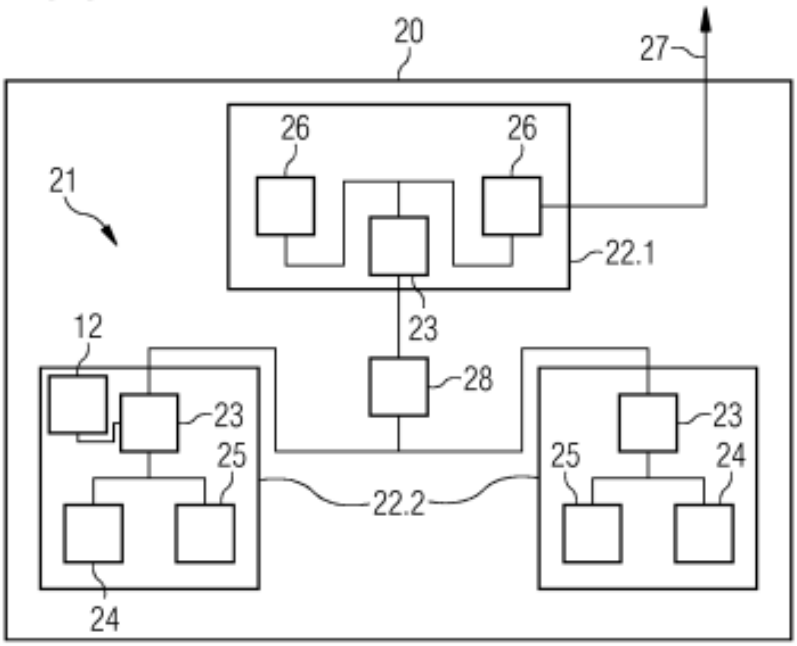

FIG 6

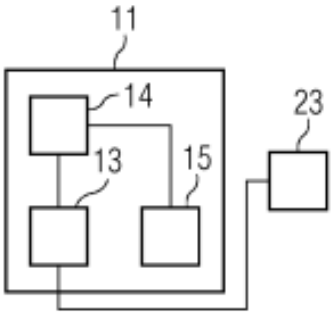

FIG 7