Ciberseguridad para infraestructuras eléctricas

www.kaspersky.com/ics
#truecybersecurity

Índice

Ciberseguridad para infraestructuras eléctricas

Un sistema de energía eléctrica actual es una instalación técnica compleja, única en términos de tamaño e importancia para la vida humana. Dadas las características físicas de la energía eléctrica y la alta velocidad característica de los procesos eléctricos, controlar la operación de una instalación como esta resulta ser una tarea compleja desde el punto de vista organizativo y técnico. Por este motivo, los dispositivos diseñados para la protección de emergencia del equipo energético y la automatización surgieron a la vez que el sector energético. Los requisitos para estos dispositivos, así como su diseño y funcionalidad, han evolucionado a la vez que los sistemas de energía eléctrica que protegían, como respuesta a la demanda creciente de los clientes y de las operaciones.

El sistema de protección, automatización y control (PACS) actual es un conjunto complejo de sistemas de información interrelacionados que cubre todas las áreas de operación de las instalaciones de energía eléctrica. El rápido desarrollo de las tecnologías informáticas y de comunicación han cambiado los sistemas de protección y automatización de los componentes eléctricos. Además, las nuevas funciones de control integradas en los sistemas de protección y automatización actuales cambian los principios de construcción de las instalaciones de red de fuente de alimentación.

Una de las principales tareas en el desarrollo de fuentes de alimentación del futuro y en la transición hacia los sistemas de red eléctrica inteligente es la mejora del control. Por este motivo, los sistemas de control juegan un papel clave en la generación, transporte y distribución de electricidad.

Los PACS actuales están muy integrados y usan tecnologías de comunicación digital basadas en normas internacionales abiertas como IEC 60870, IEC 61850 e IEC 61970. La integración de subsistemas independientes mejoró las capacidades de los sistemas de protección y control, haciendo que fueran más inteligentes y eficientes. Además, las normas de homogeneización redujeron significativamente el coste de la integración y proporcionaron un mayor nivel de fiabilidad funcional.

Un sistema de control y protección de instalaciones eléctricas actual que incluye distintos tipos de subsistemas de información como:

- dispositivos hardware y software para control de envío automatizado
- control automático para el mantenimiento de modos de operación de sistemas de energía eléctrica
- sistemas de protección
- sistemas de protección de emergencia automáticos
- sistemas de control de procesos
- sistemas de medición de energía eléctrica automatizados
- sistemas de control de calidad eléctrica

Vulnerabilidad de los PACS de las infraestructuras eléctricas al enfrentarse a amenazas de seguridad de la información

El alto nivel de apertura e integración de los sistemas de energía eléctrica, en combinación con la incorporación de las TI y de Internet en la vida diaria, ha creado nuevos desafíos en el sector de la energía eléctrica. Los sistemas de protección y control automatizados actuales para las infraestructuras eléctricas son sistemas informáticos distribuidos e integrados que se comunican mediante protocolos abiertos. En dichos sistemas, la ciberseguridad no es una prioridad ya que los sistemas de control de energía eléctrica se han construido como soluciones aisladas. Sin embargo, para los sistemas de control actuales, integrados de forma global y conectados con servicios corporativos, hay grandes riesgos de ciberseguridad.

Según la norma IEC 62351 de "Gestión de sistemas de potencia e intercambio de información asociada. Seguridad de datos y comunicaciones", se resaltan los siguientes problemas de seguridad de la información en las instalaciones de energía eléctrica y sus causas:

Comunicaciones abiertas

Líneas de comunicación abiertas y desprotegidas entre los componentes de los sistemas de protección y control, así como entre las infraestructuras energéticas:

- **Falta de verificación de identidad**
  Autenticación débil o inexistente de los agentes de interacción, por ejemplo, un dispositivo de red aleatorio en la red tecnológica puede enviar comandos de control incorrectos o maliciosos a un sistema de máximo nivel que, a su vez, podría hacer que un operador de envío ejecute acciones no válidas

- **Normas abiertas y transmisión de datos abierta**
  Los protocolos de transmisión de datos usados se basan en normas disponibles, abiertas y bien documentadas de forma pública. Las implementaciones gratuitas de protocolos y sus códigos fuente, junto con herramientas para el análisis y la emulación están disponibles de forma pública. Los datos transmitidos en estas redes suelen estar abiertos para la captura, lectura, modificación y repetición; esto simplifica el acceso y la ejecución de amenazas por parte de los intrusos potenciales

- **Alto nivel de comunicaciones de red**
  Los altos niveles de comunicación entre los protocolos IEC 60807-5-10x e IEC 61850 MMS resultan en un aspecto normal de su operación. Pero estas comunicaciones abiertas también facilitan la denegación simple de ataques al servicio en los dispositivos de infraestructura tecnológica (por ejemplo, sistema de control de procesos del centro de envío o terminales de protección) a través del envío masivo de paquetes de datos no válidos

- **Conexiones a redes públicas**
  Las redes corporativas y tecnológicas de una instalación industrial actual pueden tener varias interconexiones en casi cada nivel jerárquico del sistema de control, esto aumenta el riesgo de acceso externo no autorizado al equipo tecnológico

Falta de concienciación sobre la ciberseguridad entre los empleados

Un número limitado del personal técnico mantiene un gran número de dispositivos que normalmente se distribuyen en un territorio y funcionan sin supervisión constante. El personal de las instalaciones no suele tener un conocimiento básico sobre ciberseguridad:

- **Acceso remoto desde una red no fiable**
  Para facilitar el mantenimiento y la comodidad, el personal técnico suele conceder privilegios totales de acceso al equipo de las instalaciones remotas. Este acceso suele organizarse de forma extraoficial y sin seguridad, por ejemplo, desde estaciones de trabajo corporativas y sin acceso a Internet

- **Falta de protección de contraseñas y políticas de control de usuarios**
  Cuando un número limitado de trabajadores mantiene un gran número de dispositivos, la organización y el mantenimiento de las políticas de acceso del dispositivo se complican, incluida la protección de contraseñas y las políticas de control de usuarios. Como resultado, los dispositivos tecnológicos suelen utilizarse con contraseñas predeterminadas que simplifican el acceso no autorizado

- **Software obsoleto**
  El software de IED casi nunca se actualiza durante su vida útil en la instalación tecnológica. Los errores de software conocidos no se eliminan a menos que afecten directamente a los procesos industriales

- **Mantenimiento desde estaciones de trabajo no seguras**
  Las estaciones de trabajo portátiles (portátiles) utilizadas en el curso de mantenimiento de infraestructura tecnológica suelen utilizarse como estaciones de trabajo corporativas regulares, al igual que como equipo de "laboratorio de pruebas" para pruebas de software o para necesidades personales

- **Falta de configuración periódica y de control de software**
  Las comprobaciones de configuración del dispositivo y de verificación de software se realizan de forma manual e irregular, no más de una vez al año

No se siguen los requisitos de seguridad

Los requisitos de seguridad de la información se tienen en cuenta en raras ocasiones en el diseño del dispositivo o de software y en los procesos de desarrollo para infraestructuras tecnológicas.

- **Poca resistencia a la piratería**
  Los desarrolladores no suelen tener en cuenta la vulnerabilidad del código ante los ataques dirigidos o ante las acciones ilegítimas en la infraestructura tecnológica y sus elementos. Esto implica que la resistencia del dispositivo ante el pirateo es, por lo general, reducida

- **Configuración de seguridad de red no válida o insuficiente**
  La configuración no válida de segmentación de la red y de control de acceso entre segmentos de red en la red tecnológica, así como la ausencia de soluciones de diseño de red específicas en proyectos de implementación PACS, es un problema típico. Por esta razón, la calidad de la configuración de la estructura de red normalmente depende de las habilidades y cualificaciones del equipo de instalación

- **Ausencia de protección de datos cuando se transmiten a través de canales abiertos**
  Existe una falta o ausencia de medios seguros para la transferencia de datos mediante líneas de comunicación abiertas

- **Ausencia de control de acceso basado en roles**
  La ausencia de controles de acceso basados en roles puede facilitar permisos de acceso incorrecto a dispositivos, permitiendo a los usuarios un acceso que no se corresponde con sus tareas oficiales

- **Ausencia de soluciones de control de inicio de las aplicaciones**
  La ausencia de soluciones compatibles para proteger los sistemas informáticos del inicio de aplicaciones no autorizado suele dejar los sistemas desprotegidos ante el inicio de software no autorizado en entornos industriales. Las herramientas generales para el control de inicio de las aplicaciones no suelen ser compatibles o eficaces con los sistemas industriales (incompatibilidad con software tecnológico, recursos insuficientes en sistemas tecnológicos específicos, etc.)

- **Ausencia o la insuficiencia de una herramienta de registro de eventos de seguridad**
  No hay herramientas de registro de eventos de ciberseguridad y de supervisión específicas en los sistemas de control de procesos o su funcionalidad no es suficiente para proporcionar la interpretación correcta de una situación

Complejidades de control de acceso del contratista

Es frecuente hacer uso de contratistas para determinados tipos de trabajo de mantenimiento. Como resultado, es muy importante proporcionar solo acceso temporal a una cantidad de equipos limitada que no tenga influencia en otros componentes del sistema. La cancelación del acceso al finalizar el trabajo es fundamental.

Vida útil prolongada de los componentes vulnerables

La vida útil de los dispositivos y sistemas de protección y control es de 20 a 30 años; los sistemas no seguros instalados actualmente solo se sustituirán en un par de décadas aproximadamente. La actualización parcial suele ser muy complicada, ya que las soluciones de seguridad (por ejemplo, las que utilizan cifrado) suelen ser incompatibles con las soluciones vulnerables estándar.

Además de los problemas técnicos indicados anteriormente, también hay problemas organizativos importantes. En primer lugar, la falta de protocolos que definan las acciones que han de llevarse a cabo cuando se detecta actividad sospechosa en los sistemas automatizados. En segundo lugar, la falta de documentos y prácticas relacionadas con la investigación de las alteraciones en entornos tecnológicos, incluida la influencia maliciosa en los sistemas de control a través de tecnologías de la información. Por ejemplo, debido a su antigüedad, algunos documentos de referencia para la investigación y clasificación de alteraciones tecnológicas ni siquiera tienen en cuenta los incidentes de ciberseguridad como posible causa del funcionamiento incorrecto. Aunque se produzca un accidente, las verdaderas causas no se revelarán. Como resultado, no se tomarán las medidas adecuadas y el incidente puede volver a producirse.

Todo lo mencionado demuestra que existen numerosos problemas sistémicos:

- Los sistemas de energía eléctrica actuales de protección y control del equipo energético no son sistemas aislados ni cerrados
- Los sistemas de protección, automatización y control no tienen suficientes funciones de ciberseguridad integradas
- Desde el punto de vista organizativo y técnico, en las condiciones actuales es muy complicado detectar influencia negativa
- No hay directrices claras sobre cómo responder cuando se detecta un ataque

Soluciones técnicas para la prevención de amenazas de ciberseguridad, la detección y la mitigación

La IEC 62351 "Gestión de sistemas de potencia e intercambio de información asociada. Seguridad de datos y comunicaciones" describe en detalle las posibles herramientas para la prestación de seguridad de la información compleja en instalaciones de energía eléctrica. Sin embargo, la mayoría de las soluciones propuestas solo se pueden implementar con una sustitución total de los dispositivos de automatización, ya que requieren modificaciones del procedimiento del protocolo de comunicación y formato.

Aunque una implementación total de IEC 62351 parece una posibilidad remota dadas las circunstancias, parte de los requisitos pueden cumplirse y aplicarse a los sistemas modernos.

Kaspersky Industrial CyberSecurity (KICS) es una solución integral para infraestructuras industriales que cumple con estos requisitos.

La solución consta de dos componentes:

- KICS for Nodes: un componente para la protección de endpoints de red industriales (como las estaciones de ingeniería, las estaciones de operadores, los servidores SCADA)
- KICS for Networks: un componente para la supervisión de red industrial con comprobación de la integridad de red y capacidades exhaustivas de inspección del protocolo de aplicación (IEC 60870-5-104, IEC 61850, etc. para infraestructuras de energía eléctrica)

KICS for Nodes

KICS for Nodes es un producto especializado para los sistemas industriales. Como aplicación de software informático, está diseñada para proteger los servidores tecnológicos, las estaciones de trabajo de ingeniería y operadores, así como la HMI que ejecuta el sistema operativo Windows.

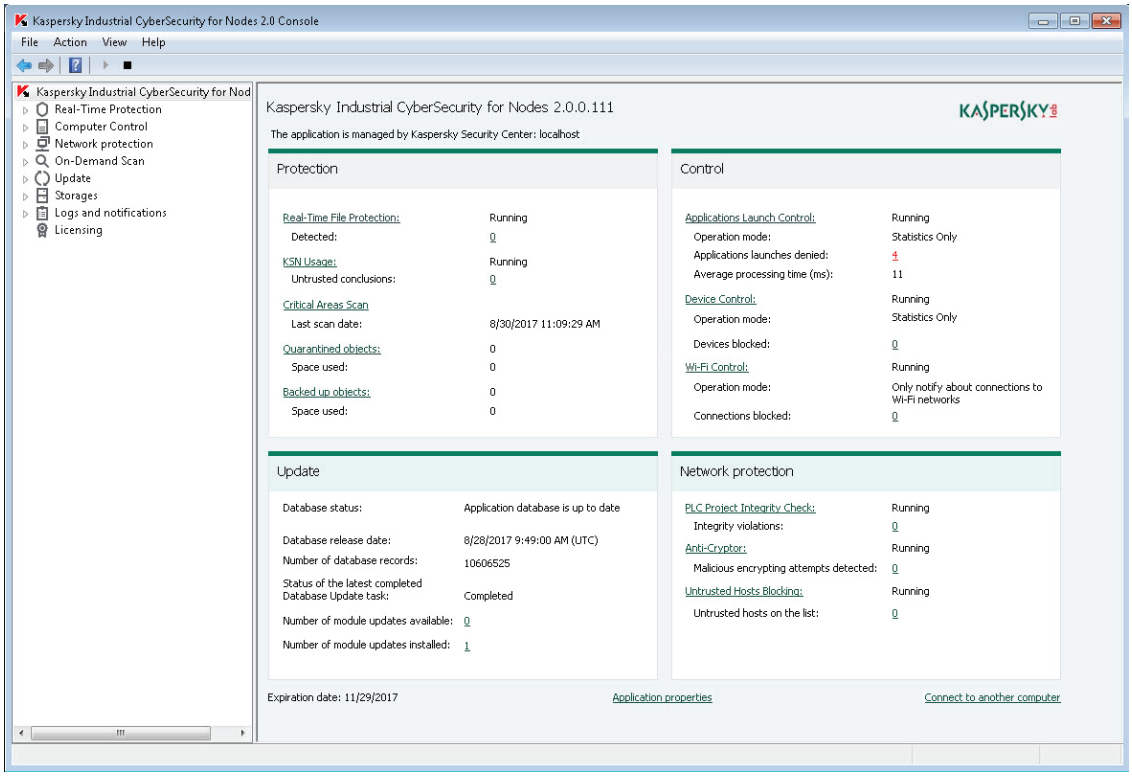

Imagen n.º 1. Interfaz de KICS for Nodes

Las funcionalidades de la solución principal:

- Lista blancas de aplicaciones (control de inicio de las aplicaciones): bloquea todas las aplicaciones para evitar que se inicien, excepto las que se permitan de forma explícita. El componente de protección proporciona el modo de prueba para admitir una configuración y depuración fáciles en la fase de implementación
- Control de dispositivos: permite a los administradores definir y especificar qué dispositivos pueden conectarse a los hosts industriales protegidos. La tecnología ofrece oportunidades para proteger los sistemas industriales de las conexiones de dispositivos no autorizados. La tecnología es compatible con máscaras para la administración fácil y el funcionamiento masivo de dispositivos
- Control de la red Wi-Fi: permite la supervisión de cualquier intento de conectarse a redes Wi-Fi no autorizadas
- Detección de software malicioso (incluido el ransomware): combina métodos de protección de autor y heurísticos para proteger las estaciones de trabajo de Windows frente a las amenazas conocidas, desconocidas y avanzadas. La tecnología anti-cryptor especial permite evitar los ataques de ransomware
- Firewall basado en host: proporciona capacidades para limitar las conexiones de red a los hosts industriales
- Comprobación de la integridad de PLC: permite un control adicional sobre la configuración del controlador a través de comprobaciones periódicas de los cambios en los proyectos

KICS for Nodes puede gestionarse de forma centralizada tras la integración en un sistema de control de infraestructuras de seguridad basado en Kaspersky Security Center, lo que hace posible realizar las siguientes funciones:

- Gestión centralizada y control de la política de seguridad: función que permite la configuración de los ajustes de seguridad para dispositivos individuales y grupos
- Actualización centralizada de bases de datos de antivirus (aunque la red tecnológica no esté conectada a Internet): ayuda en la admisión de un nivel de seguridad alto debido a la actualización de los agentes de seguridad desde un solo servidor de control en la red tecnológica. Las actualizaciones se pueden descargar en el servidor de control directamente desde Internet, desde un nodo de retransmisión (instalado en la red de TI o DMZ), o transferirse al servidor de control mediante un administrador a través de dispositivos USB
- Comprobación de nuevas actualizaciones antes de la distribución: permite que se compruebe la compatibilidad de las actualizaciones con software industrial antes de la distribución en hosts industriales
- Modelo basado en roles para la gestión de políticas y acciones independientes con el agente de seguridad: elimina la posibilidad de cambios de política de seguridad no autorizados en el servidor de control, al igual que previene la desactivación de la protección o los cambios de configuración de la solución de endpoint
- Recopilación centralizada de datos de eventos de seguridad de endpoints: permite el análisis completo de datos de seguridad de la información en función de los eventos registrados, a la vez que identifica las causas exactas de los incidentes y facilita la planificación de la mitigación

Debe tenerse en cuenta que el funcionamiento de KICS for Nodes se basa en enfoques que, de forma predeterminada, no tienen impacto en los procesos industriales.

KICS for Networks

KICS for Networks es una solución de software especializada para la supervisión de red industrial. La solución puede identificar anomalías y registrar información importante sobre los eventos de tráfico de red industrial sin interferir en el proceso industrial.

Las principales funciones de la solución son:

1. Supervisión de la integridad de la red:

- Modo de autoformación que permite la detección y el registro de todos los nodos LAN disponibles y las comunicaciones entre ellos; estos datos pueden utilizarse como punto de referencia y también para el seguimiento de cambios
- Detección basada en direcciones IP y MAC y registro de nuevos dispositivos de red conectados a los segmentos controlados de la red tecnológica
- Detección y registro de las nuevas comunicaciones de red entre nodos en función de los siguientes atributos: dirección del nodo del remitente, dirección del nodo del destinatario, protocolo de red, puerto, número de conexiones permitidas, etc.

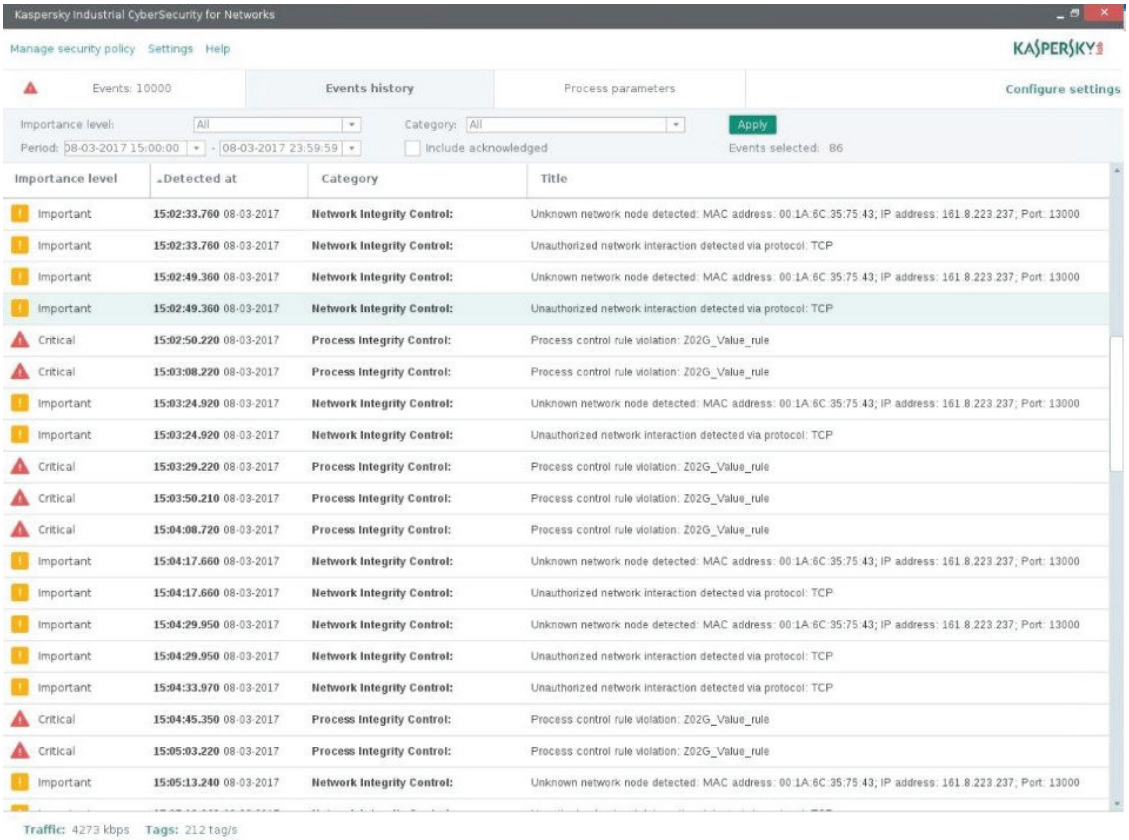

Imagen n.º 2. Interfaz KICS for Networks

2. Inspección exhaustiva de paquetes:

- Revisión, análisis y registro de mensajes importantes de protocolos tecnológicos en función de la configuración:
  - Detección de comandos de gestión del dispositivo (por ejemplo, el encendido/apagado) a través de protocolos de red industriales (IEC 61850, IEC 60870-5-104)
  - Detección de comandos para cambiar los parámetros de protección y de funcionamiento del sistema de control (por ejemplo, cambio de grupo de punto de ajuste) a través de protocolos de red industriales (IEC 61850, IEC 60870-5-104)
  - Detección de control de IED e intentos de parametrización con software de servicio a través del segmento de red controlado
- Supervisión general de mensajes telemétricos

3. Almacenamiento de eventos:

- El sistema KICS for Networks proporciona almacenamiento de eventos detectados en una base de datos interna segura
- La información está limitada por el periodo de almacenamiento y el límite de tamaño de archivo. En la imagen n.º 3 se muestra un ejemplo de la solución que ilustra un posible escenario de implementación de KICS for Networks y varios escenarios de implementación de KICS for Nodes

KICS for Nodes y KICS for Networks: Un ejemplo de implementación en una subestación de energía eléctrica moderna

Un sistema de protección y control protegido incluye dos segmentos LAN de topología de anillo. El primer segmento de subestación de energía eléctrica es el bus de estación (según la IEC 61850), que proporciona comunicaciones entre IED. Además, los bus de subestación, los controladores de subestación y las pasarelas telemétricas se utilizan para la interacción informativa con mayores niveles de control de envío. El segmento LAN proporciona acceso al equipo del sistema de protección y control mediante software de ingeniería. Puede ofrecerse acceso al servicio tanto de forma local como remota. El acceso al servicio local se proporciona utilizando un notebook conectado directamente a IED o a la LAN del bus de estación. El acceso al servicio también puede realizarse desde una estación de trabajo remota. Las comunicaciones rápidas entre nodos de red durante el funcionamiento estable se llevan a cabo de acuerdo al protocolo IEC 61850 MMS. Las comunicaciones de servicio relacionadas con la parametrización de dispositivos del sistema de protección y control se establecen bajo los protocolos de aplicación interna del fabricante del equipo.

El segmento LAN físico del bus CAN es una red de anillo formada por dos conmutadores conectados. Todos los dispositivos se conectan a los conmutadores como nodos dobles adjuntos (DAN). Por lo tanto, no existe un punto único de fallo en el segmento que proporciona un mayor nivel de fiabilidad de red. Los IED cuentan con conmutadores integrados y se combinan en cadenas. Los extremos de las cadenas se conectan a los conmutadores de red de anillo; por lo tanto, el tráfico entre dispositivos de una cadena no se transmite a través de los conmutadores de red de anillo. El control de red de topología de anillo se ejecuta mediante el RSTP. El conmutador de red está incluido para proporcionar acceso de servicio remoto a la red industrial mediante una VPN.

El segundo segmento (segmento de red del operario) también se representa mediante una topología de red de anillo designada para las estaciones de trabajo de operadores y la interacción del servidor del sistema de control de procesos.

La interacción con el centro de control de red y el operador del sistema se proporciona directamente a través de un controlador de subestación conectado al sistema de automatización (consulte la imagen n.º 3). El intercambio se realiza a través del protocolo IEC 60870-5-104.

Se requiere la instalación de KICS for Networks en cada segmento de la red seleccionada, con el fin de proporcionar una supervisión completa de la infraestructura de red tecnológica. Por tanto, deben instalarse tres servidores de KICS for Networks para el diagrama especificado: uno para el segmento del bus de estación, otro para el segmento de red del operador y otro para la línea de comunicación a niveles superiores de control. Para conectar los servidores de KICS for Networks a la infraestructura, se requiere el cambio de la reconfiguración del equipo para enviar todo el tráfico de SPAN de cada segmento de red al servidor correspondiente.

El servidor de KICS for Networks se conecta a los puertos de SPAN de los conmutadores de red. Esta configuración ofrece oportunidades de recibir solo tráfico industrial, sin afectar al proceso industrial. KICS for Networks procesa el tráfico industrial y detecta eventos sospechosos. Los datos asociados a los eventos registrados se cifran y se almacenan de forma segura. Además, los eventos se transmiten a través de un canal cifrado a Kaspersky Security Center, proporcionando así a los especialistas en seguridad una lista final de eventos detectados.

El software de KICS for Nodes deberá instalarse en cada host industrial con el fin de proteger la infraestructura de los equipos que ejecuten el SO Windows. KICS for Nodes también envía los eventos detectados al servidor de Kaspersky Security Center. Los host industriales deben contener una interfaz de red adicional para conectarse al segmento de la red de control.

Todas las comunicaciones de la red de control están cifradas. En caso de fallo en la red de control, los componentes de KICS for Networks y KICS for Nodes continuarán funcionando en el modo independiente. Los datos recopilados se transmiten a Kaspersky Security Center cuando se restablezca el funcionamiento del segmento de la red.

LICS admite la integración con sistemas SIEM. Kaspersky Security Center organiza un canal cifrado con el sistema SIEM y transfiere eventos configurados a SIEM (HP ArcSite, IBM QRadar y otros a través del formato Syslog). También pueden enviarse notificaciones mediante correo electrónico y SMS.

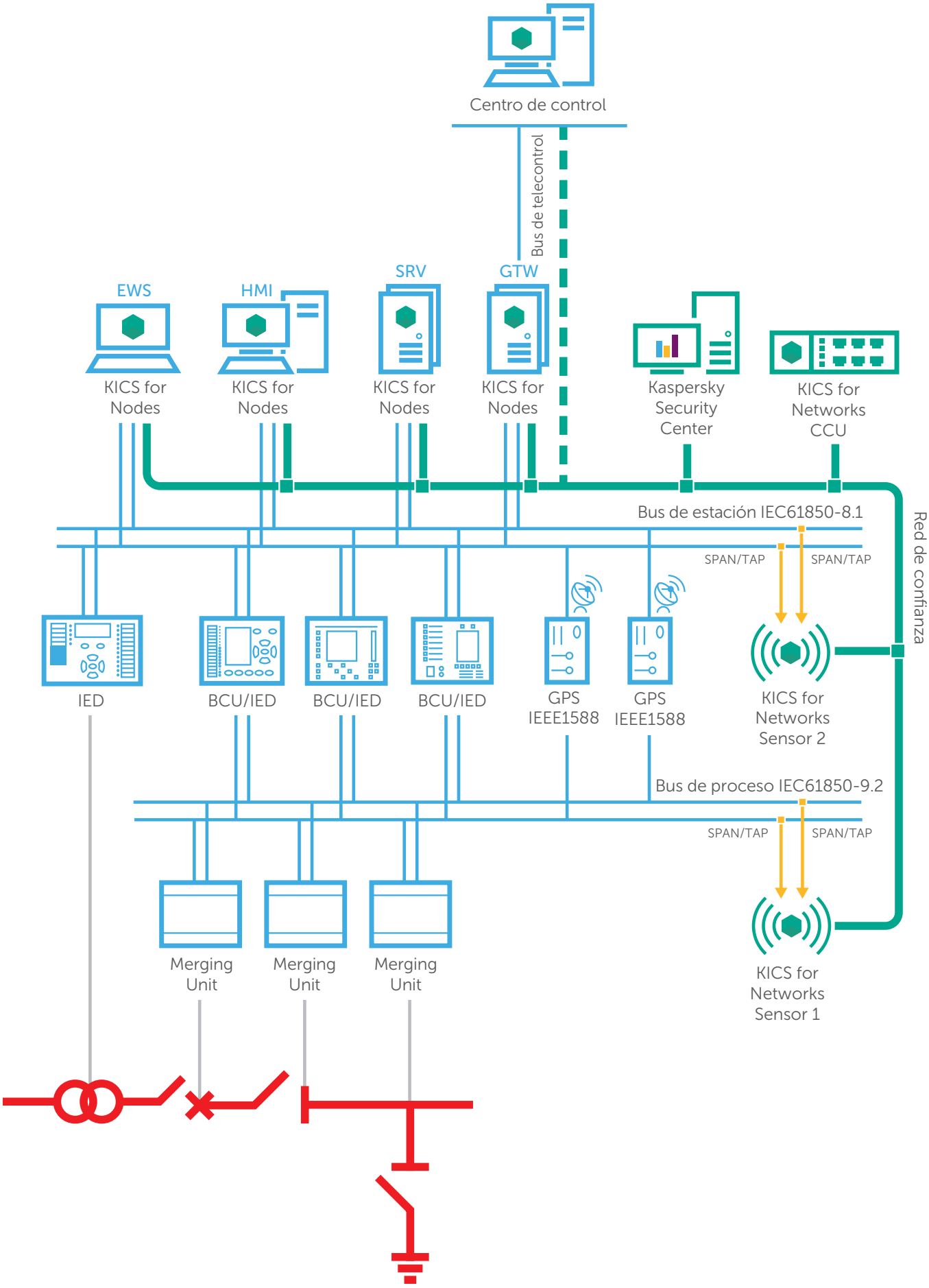

Imagen n.º 3: Implementación de los componentes de Kaspersky Industrial CyberSecurity

Términos y definiciones

CD: dispositivo informático. Instalación técnica capaz de ejecutar el procesamiento de datos según una lógica de programa predefinida.

CSPS: sistema de protección de ciberseguridad. Sistema automatizado diseñado para proporcionar ciberseguridad a la instalación protegida.

IED: dispositivo electrónico inteligente. Instalación informática multiusos basada en un microprocesador con numerosas capacidades de comunicación digital.

Ciberseguridad industrial: estado de protección que proporciona disponibilidad, integridad y confidencialidad del proceso industrial a nivel de IT/OT.

LAN: red de área local. Red informática que cubre un conjunto fijo de unidades de red conectadas a través de medios gestionados de forma local y agrupadas según el principio de ubicación de área limitada.

PACS: sistema de protección, automatización y control. Término colectivo que designa a un conjunto de sistemas de control automáticos y automatizados con diferentes propósitos integrados en la instalación.

PCS: sistema de control de procesos. Sistema hombre-máquina basado en la automatización industrial y en las instalaciones de telecomunicaciones que proporciona un control de procesos automático y automatizado in situ integral en la instalación controlada y que permite una ejecución de control desde un centro de envíos remoto.

Sistema de protección: un conjunto de IED diseñado para la detección y desconexión rápidas de segmentos dañados del sistema de energía eléctrica controlado para garantizar un rendimiento del sistema estable.

SCL: lenguaje de configuración de la subestación. Lenguaje y formato de representación especificado por IEC 61850-6 para la configuración de dispositivos de subestación eléctrica. Contiene recursos para la representación de un modelo de información del dispositivo, conjuntos de datos y servicios de comunicación. Basado en el lenguaje XML.

Red eléctrica inteligente: un sistema de energía eléctrica de nueva generación basado en el principio de agente múltiple de organización y control sobre su operación y desarrollo, para utilizar de forma eficaz todos los recursos (naturales, sociales y de producción, así como humanos). Este sistema proporciona una fuente de alimentación segura, eficiente y de calidad a los clientes debido a la interacción flexible con todos los interesados (todo tipo de generación, red y cliente de energía eléctrica). Interacción basada en tecnologías actuales y en un sistema de control jerárquico, inteligente y unificado.

SPAN: analizador de puerto conmutado. Puerto de conmutación de red utilizado para recopilar tráfico de red duplicado desde los puertos seleccionados del conmutador utilizado para el análisis.

Bus de estación: red informática rápida y muy fiable que proporciona una transmisión de datos a través de dispositivos inteligentes que implementan funciones de procesos (nivel de celda), así como conjuntos de dispositivos, hardware y software que implementan funciones generales de subestación (nivel de subestación), por ejemplo, SCADA, pasarela telemecánica, etc. En algunos casos, un bus de estación puede proporcionar comunicaciones horizontales entre dispositivos a nivel de celda. Para evitar interferencias electromagnéticas en las comunicaciones, los buses de estación suelen fabricarse con un medio de transferencia de datos de fibra óptica.

Todo sobre ciberseguridad ICS:
https://ics-cert.kaspersky.com
Noticias de ciberamenazas: **https://securelist.lat/**

#truecybersecurity

www.kaspersky.es

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* Premio al logro científico y tecnológico de Internet líder en el mundo en la III Conferencia Mundial de Internet
** Premio especial de la Feria Industrial Internacional de China (CIIF) en 2016