Detección de intrusiones cibernéticas en las redes de subestaciones

Cómo mejorar la seguridad de las subestaciones IEC 61850

Introducción

Se necesitan varias capas para garantizar la ciberseguridad de las subestaciones. La criptografía permite la autenticación de los dispositivos, pero no pueden evitarse todos los ataques con estas medidas. Los servidores de seguridad y "gaps" pueden sortearse mediante los túneles de acceso remoto existentes o mediante computadoras de mantenimiento directamente conectadas a los IED o al bus de la estación. Por lo tanto, se necesitan medidas para detectar amenazas en la subestación con el fin de activar una respuesta rápida y minimizar las consecuencias.

Este artículo describe los requisitos de seguridad de las subestaciones IEC 61850 y los diferentes métodos para detectar amenazas en estas redes. Posteriormente, se describe un método desarrollado específicamente para el bus de estación y proceso IEC 61850.

Vectores de ataque de una subestación

Definamos un ataque cibernético en una subestación como un evento en el que un adversario modifica, degrada o desactiva un servicio de al menos un dispositivo de protección, automatización o control dentro de la subestación. Como se muestra en la figura 1, una subestación típica puede ser atacada mediante todas las vías marcadas con un número. Un atacante podría entrar por la conexión del centro de control (1), tal como sucedió en uno de los ataques cibernéticos en Ucrania, donde se modificó el firmware de los dispositivos de gateway (causando su destrucción).

Otro punto de entrada lo constituyen los PC de ingeniería (2) conectados a los equipos de la subestación. Cuando un técnico de protección conecta su PC a un relé para modificar la configuración, malware en el PC podría instalar a su vez malware en el relé de forma comparable a lo que sucedió con los PLC en el ciberataque de Stuxnet. Las computadoras portátiles utilizadas para probar el sistema IEC 61850 a menudo están conectadas directamente al bus de la estación, por lo que también constituyen una posible vía para infectar los IED (3).

Por este motivo, hay disponibles nuevas herramientas de prueba IEC 61850 que proporcionan una separación cibersegura entre el PC de prueba y la red de la subestación. Esto deja al propio dispositivo de prueba (4) como una posible vía de entrada. Debido a esto, es importante que los proveedores de los equipos de prueba inviertan en proteger sus dispositivos para asegurarse de que no sea factible para un atacante aprovecharlos como vía de entrada.

El almacenamiento de los ajustes (2a) y los documentos de prueba (3a) también pueden constituir una fuente de ataque. Este servidor de almacenamiento, por lo tanto, también pertenece al perímetro crítico. Por ello, también tiene sentido introducir una solución de gestión de datos independiente, aislada y protegida ante este tipo de datos.

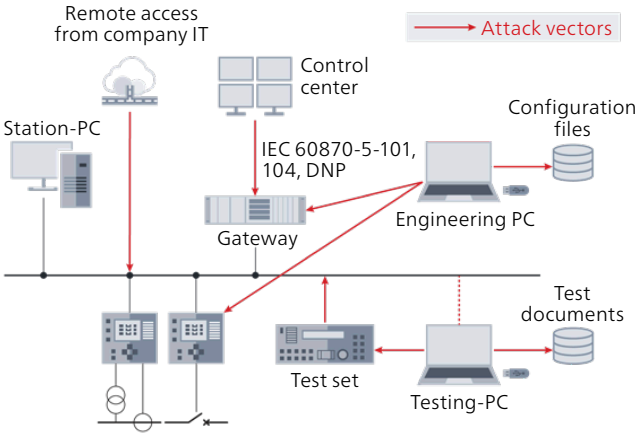

Figura 1: Vectores de ataque de una subestación

La seguridad y la norma IEC 61850

Una pregunta frecuente sobre la ciberseguridad en las subestaciones IEC 61850 es: "¿Qué sucede si un atacante inyecta un GOOSE de disparo en el bus de estación? ¿Cómo puedo evitarlo?" Para ello, no debemos suponer que el atacante necesita tener acceso físico a la red de la subestación. Esta situación también es posible mediante otras vías: un PC de ingeniería o pruebas conectado al bus de estación que se haya infectado, o incluso un IED infectado, podría empezar a inyectar mensajes GOOSE. En este contexto, los números de estado y secuencia en el mensaje GOOSE a menudo se presentan como "mecanismos de seguridad" GOOSE.

Sin embargo, estas medidas sólo se deben denominar "mecanismos disuasorios", porque cualquier adversario puede escuchar el número de estado y secuencia actual e inyectar los valores adecuados. El atacante también puede burlar fácilmente la dirección MAC fuente del paquete GOOSE. El IED que recibe los GOOSE no tiene otra opción que reaccionar ante el primer mensaje GOOSE recibido con la MAC fuente correcta y el número de estado/secuencia correcto. Por supuesto, lo mismo sucede con el contador de muestras en Sampled Values. La única

medida real para evitar tales ataques de inyección es asegurar la autenticidad e integridad del mensaje por medio de códigos de autenticación al final del mensaje GOOSE, tal como establece la norma IEC 62351-6. Con esta medida, el IED remitente se identifica claramente y resulta imposible manipular el contenido de los mensajes GOOSE. Tenga en cuenta que no es necesario codificar el mensaje para obtener estas funciones. Para proporcionar y mantener estas claves de autenticación para cada IED, se necesita una infraestructura de administración de claves en la subestación. Por eso, estos mecanismos de seguridad GOOSE no han alcanzado un uso generalizado, pero lo harán. Lo mismo puede decirse de MMS y el control de acceso basado en la función.

Cifrado

No se ha mencionado el cifrado, aunque a menudo se considera la bala de plata de la seguridad. La norma IEC 62351 también proporciona cifrado para GOOSE y MMS. Sin embargo, en el entorno de la subestación sólo hay unas pocas aplicaciones imaginables en las que es importante la confidencialidad de los mensajes. Si los mensajes no pueden alterarse (integridad) y el originador puede verificarse (autenticación), lo que se consigue mediante la autenticación en GOOSE y MMS, no es necesario cifrar los mensajes. Un ejemplo en el que el cifrado podría ser necesario es si los GOOSE enrutables (R-GOOSE) se transmitieran a través de una ruta de comunicación no cifrada. El cifrado supone una carga adicional de las CPU de los IED, aumenta el tiempo de transmisión de GOOSE e impide algunos escenarios de prueba, pero en la mayoría de los casos no proporciona medidas de seguridad adicionales a las que ya proporcionan los códigos de autenticación. El cifrado también dificulta un análisis posterior de los registros de tráfico e impide monitorear métodos como los que se describen a continuación.

La defensa en profundidad

La mayoría de las subestaciones IEC 61850 construidas hasta ahora no han implementado la norma IEC 62351. Incluso en las subestaciones en las que se aplican GOOSE y MMS con códigos de autenticación, los dispositivos infectados de la red aún podrían infectar otros dispositivos o afectar la disponibilidad mediante la perturbación del sistema de comunicación. Por lo tanto, la mayoría de los entornos de seguridad recomienda el uso de "sistemas de detección de intrusión" (IDS), un término conocido en los sistemas informáticos clásicos para detectar las amenazas y actividades maliciosas en la red. Estos IDS, tales como StationGuard de OMICRON, ahora son cada vez más comunes en el dominio de los sistemas eléctricos.

Requisitos de los IDS en las subestaciones

En una subestación IEC 61850, un IDS se conectaría como se muestra en la figura 2. Puertos espejo en todos los switches correspondientes reenvían una copia de todo el tráfico de red al IDS. El IDS inspecciona todo el tráfico de la red comunicado con estos switches. Para poder analizar el tráfico más importante entre la puerta de enlace y los IED, el IDS debe conectarse, como mínimo, con el switch adyacente al gateway y a todos los demás puntos críticos de entrada en la red. Por lo general, no es necesario abordar los switches a nivel de bahía ya que normalmente sólo se origina desde allí el tráfico de multidifusión (GOOSE, Sampled Values). Para garantizar que se analice todo el tráfico punto a punto en todas las ramas de la red, es esencial reflejar todos los switches en el IDS, lo que no siempre es posible si los IED disponen de la funcionalidad de switch.

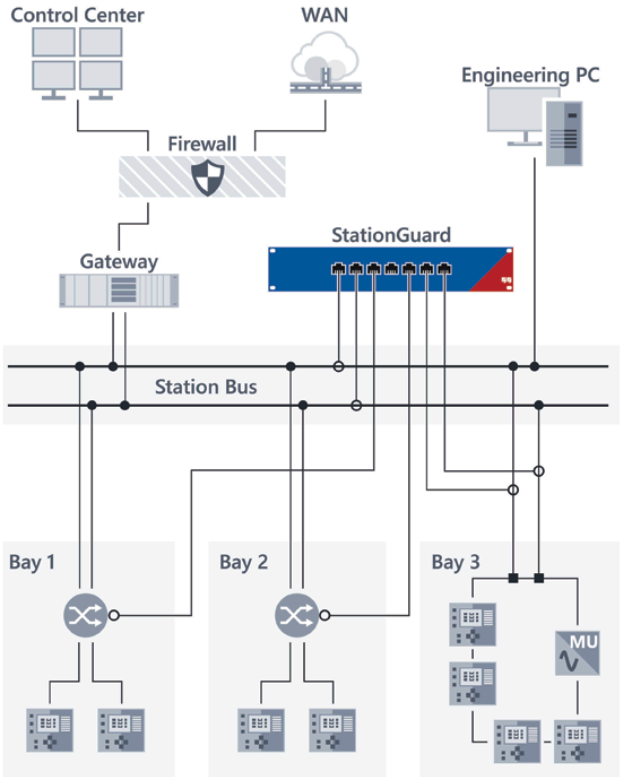

Figura 2: Estructura de una subestación con IDS conectado

Sin embargo, los IDS de la informática clásica no son adecuados para el entorno de las subestaciones. Mientras que la seguridad informática clásica se aplica a servidores de alto desempeño con millones de conexiones

simultáneas, la seguridad informática de las subestaciones se aplica a dispositivos con recursos limitados, sistemas operativos personalizados, demandas en tiempo real y protocolos de redundancia especializados. Por ejemplo, un ataque de "negación de servicio" sobre un servicio de comunicación de un IED a menudo solo requiere 10 conexiones; tal como 10 paquetes Ethernet, para tener éxito. Esto se debe simplemente a que los escenarios de "denegación de servicio" no se tuvieron en cuenta en aquellos viejos y buenos tiempos en los que se desarrollaron estos dispositivos y protocolos. Además, sólo se conoce un reducido número de ciberataques en las subestaciones, pero incluso el primer caso de un nuevo ataque podría tener consecuencias graves. Por lo tanto, un IDS de subestaciones debe poder detectar ataques sin ningún conocimiento previo sobre cómo podrían ser esos ataques y eso es exactamente lo que hace StationGuard de OMICRON. Este es un planteamiento muy diferente al de un software antivirus, que busca las firmas de virus que tiene en una lista.

Sistemas basados en el aprendizaje

Para poder detectar ataques desconocidos, muchos proveedores utilizan un método de "fase de aprendizaje". Estos sistemas estudian la frecuencia y la temporización de ciertos marcadores del protocolo para intentar aprender el comportamiento habitual del sistema. Una vez finalizada la fase de aprendizaje, se activará una alarma si uno de los marcadores se encuentra significativamente fuera del rango previsto. Esto tiene el efecto de que se activan falsas alarmas para todo lo que no ocurrió durante la fase de aprendizaje, tales como eventos de protección, acciones poco comunes de conmutación o automatización, o el mantenimiento y las pruebas de rutina. Debido a que estos sistemas no comprenden la semántica de los protocolos, los mensajes de las alarmas se expresan en términos de datos técnicos del protocolo. Por lo tanto, las alarmas sólo pueden ser examinadas por un técnico experto en datos del protocolo IEC 61850 y familiarizado con la seguridad informática de redes. El técnico que examina la alarma también debe conocer la situación operativa para juzgar si ciertos eventos del protocolo IEC 61850 corresponden a un comportamiento válido. Por lo tanto, se produce un gran número de falsas alarmas en cada subestación que tienen que ser examinadas por personal muy cualificado. Esto a menudo da lugar a que se ignoren o descarten las alarmas sin investigarlas y se desconecte el IDS en última instancia.

Figura 3: StationGuard importa el archivo SCL (System Configuration Language - lenguaje de configuración de subestaciones) de la subestación para crear un modelo completo del sistema

El método

En las subestaciones IEC 61850, todo el sistema de automatización, incluidos todos los dispositivos, sus modelos de datos y sus patrones de comunicación, se describe en un formato estandarizado: el SCL. Los archivos de descripción de configuración del sistema (SCD) normalmente contienen también información acerca de los activos primarios y un número creciente de subestaciones tiene incluso el diagrama unifilar. Esta información permite utilizar un método diferente para detectar intrusiones: El sistema de monitoreo puede crear un modelo completo del sistema de automatización y eléctrico, así como comparar todos y cada uno de los paquetes de la red con el modelo del sistema en directo. Incluso las variables contenidas en los mensajes (GOOSE, MMS, SV) comunicados se pueden evaluar frente a las previsiones derivadas del modelo del sistema. Este proceso es posible sin necesidad de una fase de aprendizaje, sólo con la configuración del SCL. Este método se implementa en el nuevo sistema de monitoreo de seguridad funcional de OMICRON, StationGuard.

Monitoreo funcional de seguridad

En esencia, se produce un monitoreo funcional muy detallado para detectar ciberamenazas en la red. Debido al nivel de detalle de la verificación, no sólo se detectan amenazas a la seguridad cibernética, tal como paquetes incorrectos y acciones de control no permitidas, sino también fallas de comunicación, problemas de sincronización y por lo tanto, también (alguno) errores de los equipos. Si el sistema conoce el diagrama de una línea y pueden observarse los valores de medición en la comunicación MMS (o incluso mediante Sampled Values), las posibilidades de lo que se puede verificar son infinitas.

Por ejemplo, solo para GOOSE hay 35 códigos de alarma disponibles para todo lo que podría fallar. Esto incluye desde simples fallos de stNum/sqNum (como se ha explicado anteriormente) a problemas más complejos, tales como los tiempos de transmisión demasiado largos. Esto último se detecta midiendo con precisión la diferencia entre la marca de tiempo el mensaje y el momento de llegada a StationGuard. Que este tiempo de transmisión en la red sea significativamente mayor que 3 ms en un GOOSE de tipo "protección" (según la norma IEC 61850-5), indica un problema en la red o en la sincronización de tiempos.

¿Qué se hace para la comunicación MMS? Según el modelo del sistema (según el SCL) se sabe qué nodos lógicos controlan qué activos primarios. De esta manera, se puede distinguir entre las acciones correctas/incorrectas y las críticas/no críticas. Para la conmutación de un interruptor de potencia y la conmutación del modo de prueba IEC 61850 se usa la misma secuencia de prueba en el protocolo MMS (seleccionar antes de operar), pero el efecto en la subestación es bastante diferente. Por lo tanto, que el PC de prueba en la figura 1 cambie el modo de prueba en un relé puede ser una acción legítima durante el mantenimiento, pero probablemente no sea legítimo que el PC de prueba opere un interruptor de potencia. En los siguientes párrafos se profundizará en este ejemplo.

Desarrollado con los técnicos de PAC

La investigación sobre este método comenzó en 2011. Derivada de este concepto, la supervisión funcional 24/7 de la sincronización horaria SV, GOOSE y PTP ha estado disponible en un dispositivo de análisis distribuido e híbrido (OMICRON DANEO 400) desde 2015. Además, tuvimos en cuenta en nuestro desarrollo las observaciones de muchas otras compañías eléctricas de todo el mundo, así como algunas instalaciones de prueba de concepto.

Figura 4: StationGuard instalado en una nueva subestación de 110kV, 2019.

En 2018, se realizó una de las primeras instalaciones de prueba de concepto en una subestación de 110 kV de la empresa suiza de generación y distribución CKW y ha estado en servicio desde entonces. La figura 4 muestra la instalación en una nueva subestación en 2019. En esta configuración, todo el tráfico del switch "núcleo" se reflejaba en StationGuard. Esto garantiza que estén visibles todas las comunicaciones desde la puerta de enlace hasta y desde todos los IED. Debido a que las conexiones de mantenimiento remotas entran también a través de ese switch, StationGuard también puede examinar todo este tráfico. Puesto que la comunicación GOOSE es de multidifusión, y debido a que la configuración de la red lo permite, todos los GOOSE de los IED en las bahías de subestación también son visibles para StationGuard.

Pantalla de alertas

Además de evitar falsas alarmas, también es de vital importancia que los mensajes de alarma sean comprensibles para los técnicos responsables de las funciones de protección, automatización y red en la subestación. Esto permite tiempos de reacción más rápidos debido a que a menudo estas alarmas son activadas por técnicos que trabajan en la subestación (o actividades remotas). Además, esto permite colaborar a los técnicos de seguridad y de PAC a la hora de rastrear eventos en una subestación.

La figura 5 muestra una captura de la pantalla gráfica de alarmas: La alarma se muestra como una flecha del participante activo (Laptop 1) realizando la acción prohibida y la "víctima" de la acción, un controlador de bahía en la bahía Q01.

La figura 6 revela detalles acerca de esa alarma: se accionó un interruptor de potencia (mediante una secuencia de control MMS), lo que no está permitido para un PC desconocido. Además, este portátil también se conectó a través del protocolo de un fabricante y descargó archivos a través de MMS. Los detalles del mensaje revelaron información adicional, como el nombre del archivo descargado.

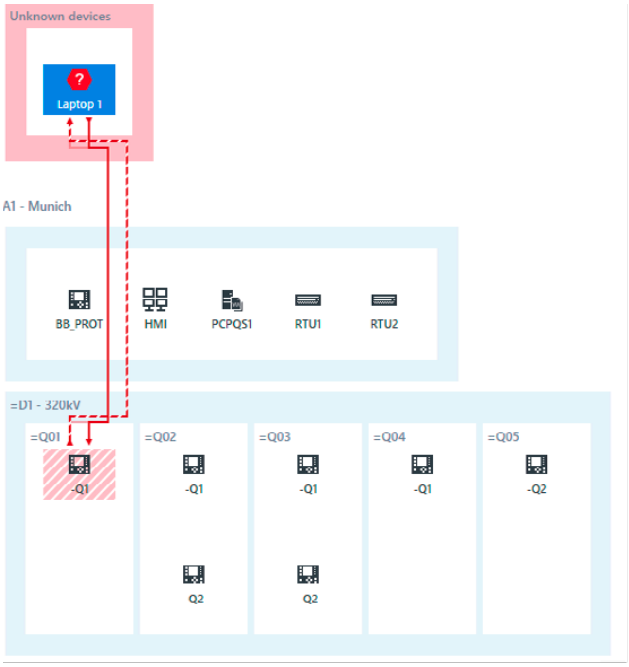

Figura 5: Visualización de alertas gráficas de IDS en lugar de listas de eventos simples

Figura 6: Datos de la figura 5: Portátil desconocido intentando un control no autorizado de un interruptor de potencia

Inventario de activos

Todos los dispositivos que se comunican en la red son detectados y visualizados. Para cada dispositivo detectado, la información del tráfico de red capturado se agrega a la información del SCL. Esto permite mostrar el proveedor, el modelo y la versión del firmware cuando esté disponible. La figura 7 muestra la información agregada para un activo cibernético, incluyendo la descripción y el nombre del dispositivo del archivo SCD del proyecto.

Configuración

Como se ha mencionado anteriormente, no es necesaria una fase de aprendizaje. La detección se inicia desde el momento en que se enciende el dispositivo y no puede desactivarse, por razones de seguridad. Hasta que se cargue el archivo SCD de la subestación, todos los IED se detectarán y presentarán como dispositivos desconocidos. Una vez que el archivo SCD se haya cargado, los IED se indicarán como dispositivos conocidos y la estructura de la subestación se ensambla en un diagrama de "línea cero", tal como se introdujo con StationScout. La configuración también puede prepararse en la oficina y luego instalarse en campo, una tras otra con una rápida puesta en servicio. Si no se incluyen todos los IED en un solo archivo (puede ocurrir), entonces también se pueden importar uno a uno los IED adicionales. Una vez realizada

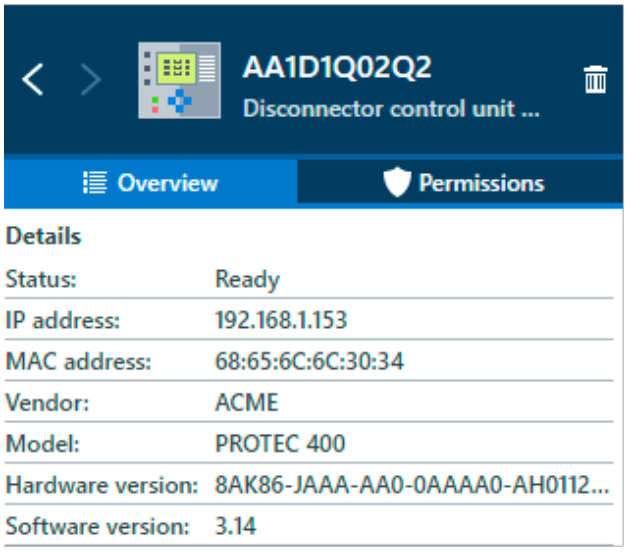

Figura 7: La información de activos combinada del tráfico de la red y el SCL

la importación, el usuario puede añadir funciones como "PC de prueba", "PC de ingeniería", etc. a los dispositivos desconocidos restantes.

¿Qué ocurre en el caso de una alarma?

Es importante tener en cuenta que StationGuard es puramente pasivo y si una acción "no está permitida" disparará una alarma. Esta alarma puede comunicarse con el gateway/RTU y el centro de control o con un sistema independiente que recopile alertas de seguridad, conocido como sistema de gestión de información y eventos de seguridad (SIEM) usando el protocolo Syslog. StationGuard no reacciona activamente ni interfiere con la subestación. Pero permite una reacción rápida, por ejemplo, el aislamiento del dispositivo en cuestión de la red antes de que pueda ocurrir cualquier daño. Dependiendo de la variante del hardware elegido, hay salidas binarias definidas por el usuario que se cablean directamente a la RTU. En este caso la señalización de alarmas se

Figura 8: Vista frontal del RBX1 variante de 19" de StationGuard

produce sin comunicación de la red y las alarmas pueden integrarse en la lista de señales SCADA normales como cualquier otra señal cableada de la estación.

Seguridad cibernética del propio IDS

Como sabemos por las películas de serie B, los ladrones siempre atacan primero el sistema de alarma antirrobo. Por lo tanto, ¿qué pasa con la seguridad de este sistema de alarma? Un aspecto importante es que se utiliza un hardware autónomo seguro y no una máquina virtual. Ambas variantes del hardware de StationGuard, el móvil (MBX1) y la variante de 19" para la instalación permanente (RBX1), tienen la misma seguridad de plataforma.

Ambos tienen un chip criptoprocesador seguro según ISO/IEC 11889. Esto garantiza que no se guarden claves cifradas en la memoria flash, sino en un chip independiente protegido contra la manipulación. Mediante la instalación de los certificados de OMICRON en el chip durante la producción se crea una cadena verificada de arranque seguro. Esto significa que cada paso en el proceso de arranque del firmware verifica las firmas del siguiente módulo o controlador que se carga. Esto garantiza que solo se puede ejecutar software firmado por OMICRON. El almacenamiento de los dispositivos se cifra con una clave exclusiva para ese hardware y se protege dentro del criptochip. Como nadie (incluyendo OMICRON) conoce esta clave, se perderán todos los datos en el dispositivo cuando se reemplace el hardware en una reparación. Muchos otros mecanismos aseguran que los procesos del dispositivo no puedan ser atacados o ser objeto de un mal uso, de manera que el planteamiento de "defensa en profundidad" se aplique también al software que se ejecuta en el dispositivo.

Resumen

Las subestaciones presentan vectores potencialmente propensos a ciberataques. Si un atacante puede influir en una o varias subestaciones, esto puede tener graves consecuencias para la red eléctrica. Por lo tanto, deben implementarse medidas de seguridad cibernética no sólo en los centros de control, sino también en las subestaciones. Para las subestaciones IEC 61850, está disponible un método para la detección de intrusión que conlleva un pequeño número de falsas alarmas sin requerir un elevado esfuerzo de configuración gracias a la potencia del SCL. StationGuard no sólo detecta amenazas a la seguridad, sino que también detecta problemas funcionales de las comunicaciones IEC 61850 y de los IED, lo que también es útil en las fases FAT y SAT. StationGuard muestra los eventos detectados en el idioma de los técnicos de protección, automatización y control, ofreciendo así la ventaja de que los técnicos de seguridad y PAC pueden trabajar juntos para averiguar la causa de los eventos.

Figura 9: Vista posterior del RBX1 variante de 19" de StationGuard

Más información en:
www.omicronenergy.com/stationguard