DISEÑO Y PUESTA EN SERVICIO DE UNA ARQUITECTURA DE RED DE SUBESTACIÓN SEGURA

Andreas Klien[1], Yann Gosteli[2], Stefan Mattmann[3]

[1]OMICRON electronics GmbH, Klaus, Austria (andreas.klien@omicronenergy.com)
[2]Centralschweizer Kraftwerke (CKW) AG, Luzern, Suiza (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Luzern, Switzerland (stefan.mattmann@ckw.ch)

Palabras clave: SEGURIDAD CIBERNÉTICA, IEC 61850, DETECCIÓN DE INTRUSIÓN, AUTOMATIZACIÓN DE SUBESTACIONES

Resumen

Los auditores de las compañías eléctricas y de seguridad cibernética consideran cada vez más como vector de ataque crítico, no sólo el centro de control, sino también las subestaciones, como posibles puntos de entrada de los ataques cibernéticos. Son factores de riesgo importantes los procesos, la manera de realizar la puesta en servicio de los sistemas de protección y control, así como la manera de implementar el acceso de mantenimiento a distancia. Por lo tanto, debe revisarse la arquitectura del sistema de protección y control por seguridad. Para lograrlo, la compañía suiza de generación y distribución eléctrica, Centralschweizer Kraftwerke AG (CKW), inició en 2016/2017 un proyecto para desarrollar una nueva arquitectura de referencia para sus sistemas secundarios. Su diseño aborda estos vectores de ataque con contramedidas, al tiempo que ofrece un equilibrio sensato entre sostenibilidad y seguridad. El diseño incluye múltiples niveles de seguridad, incluyendo múltiples capas de cortafuegos. Además, se aplica un sistema de detección de intrusión (IDS, Intrusion Detection System). La selección de un IDS adecuado para las subestaciones resultó ser todo un reto, ya que muchos IDS no soportan los requisitos de las redes de subestaciones. Este documento comienza con una enumeración de los vectores más importantes de ataque a las subestaciones, seguida de una descripción de la arquitectura de seguridad sin precedentes implementada por primera vez por CKW en un proyecto de subestación de 110kV. El documento concluye con las experiencias en la selección de un IDS adecuado para las subestaciones y las lecciones aprendidas en la prueba de aceptación en fábrica de este proyecto.

1. Introducción

1.1. Vectores de ataque a las subestaciones

Asumiremos para el resto de este artículo que un ciberataque a una subestación es 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. Para lograr esto, un atacante puede usar una de las rutas de ataque mostradas en la Figura 1 [1].

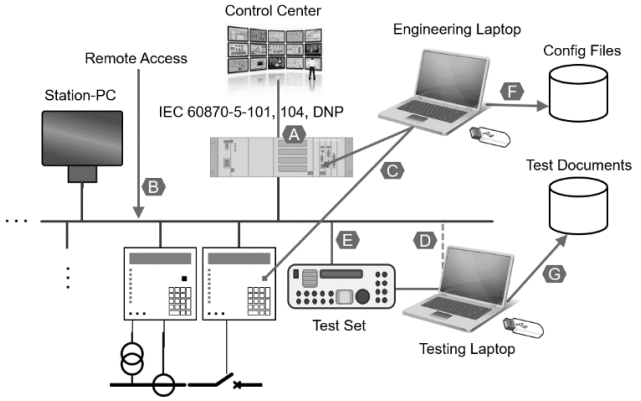

Figura 1 Vectores de ataque a las subestaciones [1]

Un atacante podría entrar por la conexión al centro de control (**A**), como ocurrió en el primer ciberataque a la red eléctrica de Ucrania, donde se modificó el firmware de los dispositivos de la puerta de enlace (gateway), causando su destrucción [2], o a través de una conexión de acceso remoto (**B**), como ocurrió en el segundo ciberataque a Ucrania en 2016 [3] y en el ciberataque "TRITON" a los PLC críticos de infraestructura [4].

Constituyen otro punto de entrada los PC de ingeniería (**C**), tanto directamente conectados a los equipos de la subestación como a la red de la subestación. Cuando un ingeniero de protección conecta su PC a un relé para modificar los ajustes (de protección), un malware en el PC podría a su vez instalar malware en el relé como ocurrió con los PLC en el famoso ciberataque "Stuxnet" 2010 [5].

Las computadoras portátiles utilizadas para probar el sistema IEC 61850 (**D**) suelen estar conectadas directamente al bus de la estación, lo que también es una manera potencial de infectar los Dispositivos

Electrónicos Inteligentes (IED, Intelligent Electronic Devices). 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. Queda entonces el propio dispositivo de prueba (**E**) como una posible vía de entrada. Por eso es importante que los proveedores de equipos de prueba inviertan en proteger sus dispositivos para que un atacante no pueda aprovecharse de ellos como vía de entrada.

El lugar de almacenamiento de los ajustes (**F**) y los documentos de prueba (**G**) también podrían constituir una fuente de infección. Por lo tanto, el emplazamiento del servidor o de almacenamiento también pertenece al perímetro crítico y no debe estar en la zona informática de la oficina. Por lo tanto, tiene sentido introducir una solución de gestión de datos independiente, aislada y protegida para esos datos.

2. Nueva propuesta de arquitectura de subestación

2.1. La vanguardia en seguridad cibernética de OT

La asociación suiza del sector eléctrico VSE creó un grupo de trabajo sobre la seguridad de la tecnología operativa (OT, Operational Technology), que posteriormente publicó un documento de recomendaciones para el sector: "Handbook on Basic Protection of Operational Technology in Power Systems" (Manual de protección básica de la tecnología operativa de los sistemas eléctricos). Este manual hace referencia al "Cyber Security Framework for Critical Infrastructure" (Marco de seguridad cibernética para infraestructuras críticas) del National Institute of Standards (NIST) [7] que se adapta y mejora continuamente, con la última versión actualizada en 2018. El marco del NIST se basa en la suposición de que nunca hay una protección al 100% contra los ataques cibernéticos. Con suficientes conocimientos y esfuerzo, pueden vulnerarse todas las medidas de seguridad. Partiendo de esta base, el marco del NIST recomienda un proceso que consta de los siguientes cinco pasos: "Identificar", "Proteger", "Detectar", "Responder", "Recuperar". Por consiguiente, el primer paso es la identificación de los vectores de ataque (Identificar), como se ha explicado en el apartado anterior de este documento. Luego pueden aplicarse las contramedidas en el siguiente paso (Proteger). Si un atacante sigue siendo capaz de superar estas barreras, tiene que detectarse el ataque (Detectar) y, en el mejor de los casos, actuar inmediatamente (Responder) para restablecer el estado normal lo más rápidamente posible (Restaurar). Con las lecciones aprendidas en Detectar y Responder pueden identificarse nuevos vectores de ataque, aplicarse nuevas contramedidas y así repetirse el proceso.

La recomendación del sector suizo hace mucho hincapié en la interacción de las personas, la tecnología y los procesos dentro de la organización. Por ejemplo, la vigilancia continua o la detección de intrusión (Detectar) sólo tiene sentido si se responde adecuadamente a los mensajes de alarma. Por lo tanto, los mensajes de alarma deben ser comprensibles para todos los que participan en el proceso de respuesta: los ingenieros de OT y especialistas en seguridad informática. De lo contrario, el proceso de respuesta se vuelve ineficiente. Además, si el IDS da demasiadas falsas alarmas, acabarán ignorándose todas las alarmas.

2.2. Iniciativas de seguridad cibernética de la OT en CKW [6]

El tema de la seguridad de la OT, especialmente de los sistemas de control y protección, ha cobrado cada vez más importancia en CKW en los últimos años. Esto se debió a las recomendaciones mencionadas del sector suizo, pero sobre todo a las evaluaciones de seguridad de OT realizadas por CKW en los últimos años. Estas evaluaciones indicaron puntos débiles tanto en las redes como en la tecnología de control utilizadas en las subestaciones. Por ejemplo, se encontraron transiciones de zonas inseguras y algunos métodos de acceso remoto críticos en las computadoras de control de estación. Además, no fue posible evaluar si se está produciendo actualmente un ataque en la red de la subestación o si hay actividades sospechosas en la red que puedan indicar un ataque inminente.

Basándose en estos hallazgos, CKW se ha fijado el objetivo de eliminar los puntos débiles esenciales y endurecer los requisitos para su futura arquitectura de subestaciones, por lo que estos hallazgos se

integraron en la nueva norma de diseño de subestaciones de CKW.
Además de trabajar en esta norma de diseño, CKW pudo participar en el grupo de trabajo suizo para el mencionado manual de seguridad de OT. Basándose en este intercambio de información, CKW integró sistemáticamente las conclusiones del grupo de trabajo en sus propias normas de diseño.

En 2016/2017, un equipo de proyecto de CKW comenzó a planificar la nueva subestación "US Rothenburg", que entrará en funcionamiento en 2020. En este proyecto se aplicó la nueva norma de seguridad de arquitectura de CKW y se siguieron las últimas recomendaciones del manual de seguridad de OT suizo. Para poder implementar estas sofisticadas medidas de seguridad, CKW decidió implementar por su cuenta la arquitectura de la red y la configuración de conmutación.

2.3. Diseño de la red

En el diseño de la red de US Rothenburg, se implantaron obstáculos en cada zona para hacer un ataque lo más difícil posible. La Figura 2 representa la red de la subestación US Rothenburg.

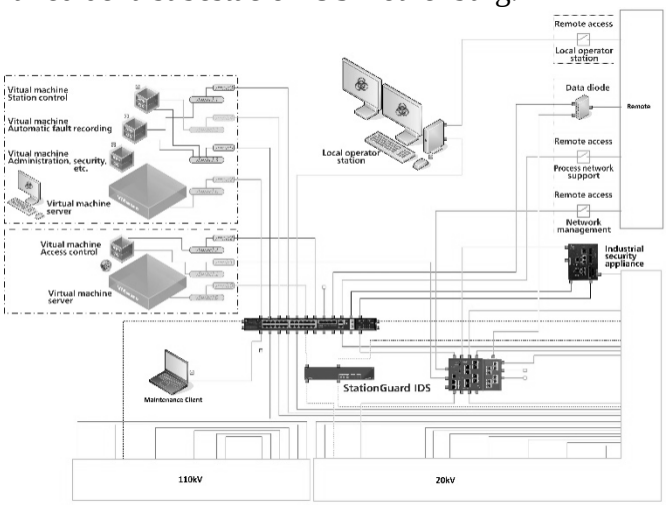

Figura 2 Arquitectura de la red de US Rothenburg [6]

En esta arquitectura, todos los vectores de ataque descritos en el apartado 1.1 de este documento se abordan utilizando una amplia gama de medidas de seguridad. Las conexiones remotas de la planta se abordaron con la máxima prioridad. Estas conexiones remotas no sólo se protegen mediante cortafuegos y soluciones de túnel, sino que se desactivan por defecto. Las conexiones para el acceso remoto sólo se activan cuando es necesario. Esto significa que intervienen varias personas para permitir el acceso remoto, de manera similar al proceso de autenticación de dos factores.
La comunicación de control de supervisión y adquisición de datos (SCADA, Supervisory Control and Data Acquisition) con el centro de control se realiza mediante el protocolo de serie IEC 60870-5-101. Todo el acceso a los dispositivos de la subestación a efectos de mantenimiento se realiza exclusivamente a través de estaciones de trabajo especiales, que están debidamente protegidas. Estas estaciones de trabajo están virtualizadas y en un emplazamiento central. Este acceso remoto de mantenimiento también debe ser habilitado a distancia.
El sistema SCADA, el sistema de recopilación del registrador de fallas y los servidores del sistema de seguridad están virtualizados y operados en una máquina anfitriona local en la subestación. Incluso la estación local de HMI sólo accede a estos sistemas usando un escritorio remoto a través de un cortafuegos local adicional. Se utiliza el control de acceso basado en roles (RBAC, Role-Based Access Control). Esto significa que no hay una contraseña por dispositivo, sino una contraseña por usuario. Esto tiene la ventaja de que un ingeniero puede usar su propia contraseña en todas las subestaciones. Si un empleado deja la empresa, su usuario puede eliminarse fácilmente y no es necesario cambiar las contraseñas. Esta gestión de usuarios se lleva a cabo mediante un servidor central de Active Directory (AD) y un servidor RADIUS local en la subestación. Los usuarios deben conectarse usando AD, que les asigna los permisos necesarios. Si es necesario, el acceso al AD central puede habilitarse desde una ubicación central. Además, los usuarios deben acceder a cada IED con un nombre de usuario y una contraseña. De esta manera, los IED utilizan el servidor local de RADIUS para comprobar la autentificación del usuario y la contraseña, así como para recuperar los permisos asignados a este usuario. Esto se aplica tanto al acceso a los dispositivos con herramientas de ingeniería como al uso de la pantalla del IED. No se utilizan contraseñas estándar.
Todos los PC conectados a la red de la subestación están bastionados. Esto se consigue, entre otras cosas, configurando el firewall de Windows de acuerdo con la matriz de comunicación de la subestación y, dependiendo de la función de ese

cliente, bloqueando las funciones de los sistemas operativos que no sean necesarias.
Como medida de seguridad adicional, el control de acceso a la red se lleva a cabo mediante autenticación por filtrado MAC, lo que significa que sólo los dispositivos registrados pueden conectarse al switch de la red.
En caso de alguna anomalía, el switch también debe reconocer y aceptar los dispositivos de reserva existentes. En los switches de la red de la subestación y en el cortafuegos, se configuran las listas de control de acceso para determinar qué dispositivo está autorizado a comunicarse con qué otro participante de la red, incluidos el protocolo y el puerto de switch utilizados.
La red del bus de la estación y la red para la configuración y el mantenimiento están separadas tanto lógica (VLAN) como físicamente. Esto significa que, en cada IED, la comunicación IEC 61850 MMS y GOOSE funciona en una interfaz de red diferente al acceso de mantenimiento. Además, toda la red del bus de la estación está segmentada, en la que, entre otras cosas, están separados los siguientes segmentos mediante un cortafuegos:

- 110kV (GOOSE y MMS)
- 20kV (GOOSE y MMS)
- HMI local
- Puerta de enlace del protocolo
- Sistemas auxiliares
- Redes de mantenimiento para IED y clientes
- Red de gestión, VM, RADIUS

La comunicación de la subestación a las zonas de la red de nivel superior se asegura adicionalmente mediante un diodo de datos. Este diodo de datos asegura que sólo se puedan iniciar sesiones de comunicación saliente y proporciona otra capa de seguridad.
Un sistema de detección de intrusión (IDS, Intrusion Detection System) monitoriza todo el tráfico de la red en el sistema mediante un método de lista blanca, es decir, todo el tráfico desconocido que no está en la lista blanca dispara, por defecto, una alarma. El IDS informa de la alarma al centro de control a través de la RTU y a un centro de operaciones de seguridad mediante protocolos especializados para el registro de alarmas.

3. Detección de intrusiones

La arquitectura de seguridad de CKW se basa en el establecimiento de segmentos de red, cada uno separado por cortafuegos. La configuración del cortafuegos especifica exactamente qué protocolos pueden utilizarse para la comunicación entre los segmentos. Sin embargo, los protocolos permitidos por el cortafuegos, tal como MMS/GOOSE, utilizados en la norma IEC 61850, y los protocolos de ingeniería específicos de los proveedores, también pueden utilizarse para atacar los dispositivos e infectarlos. En tales escenarios, CKW quería ser capaz de detectar actividades no autorizadas pronto. Para este fin, se decidió que se usaría un IDS en la arquitectura de referencia de CKW.
Para poder analizar el tráfico más crítico, es decir, la comunicación entre la puerta de enlace y los IED, al menos todo el tráfico de la puerta de enlace debería copiarse al IDS. Por lo general, no es necesario configurar los switches a nivel de bahía ya que normalmente sólo se origina desde allí el tráfico de multidifusión, tal como GOOSE y Sampled Values. Para asegurar que también todo el tráfico de unidifusión en todas las ramas de la red sea analizado, se recomienda que todos los switches se reflejen al IDS.
En la arquitectura de CKW, el IDS está conectado a puertos espejo en todos los switches de la red. Esto significa que el IDS analiza el tráfico en el bus de la estación, así como el tráfico que viene a distancia antes y después de que pase por los cortafuegos.

3.1. Requisitos para el IDS de subestación

Seleccionar un IDS adecuado para las subestaciones presentó dificultades. Un requisito importante era que el IDS pudiera ser fácilmente operado por los ingenieros de protección, control y redes que son responsables de todos los IED y equipos de red. Para apoyar el proceso de respuesta ante alarmas, debería ser fácilmente posible asociar las alarmas del IDS a los eventos de la subestación y los registros de eventos en la HMI. Por lo tanto, el IDS debería permitir visualizaciones específicas para las subestaciones, en lugar de sólo la terminología de seguridad informática.
Hasta hace poco, sólo había dos metodologías principales para los IDS: Las basadas en firmas y las "basadas en el aprendizaje".

La basada en firmas funciona con una lista negra, tal como suelen funcionar los sistemas antivirus de PC. Explora en busca de patrones de virus y malware conocidos. El problema es que sólo se conoce hasta ahora un pequeño número de ciberataques a las subestaciones, pero incluso la primera aparición de un nuevo ataque podría tener graves consecuencias. El IDS de una subestación debe ser capaz de detectar ataques sin ningún conocimiento previo sobre cómo podría ser el ataque.

Por lo tanto, más sistemas de IDS siguen un método "basado en el aprendizaje". El IDS examina los parámetros genéricos de los distintos protocolos para conocer los valores medios y la frecuencia de cada parámetro.

Después de eso, durante el funcionamiento normal, se activa una alarma cuando la comunicación de la red se desvía significativamente del promedio aprendido. El resultado es que se activan falsas alarmas para todos los eventos que no ocurrieron durante la fase de aprendizaje. Esto incluye, por ejemplo, los disparos y las operaciones de conmutación, o las pruebas de rutina de las protecciones. Como el sistema no conoce el significado de los paquetes de la red, los mensajes de alarma se refieren a parámetros de protocolo genéricos, como "MMS confirmado-escritura-respuesta fallida". Esto da lugar a un alto número de falsas alarmas, cada una de las cuales requiere de especialistas en informática y especialistas en IEC 61850 para su comprobación. Tal esfuerzo en el proceso de respuesta no era aceptable para CKW.

3.2. El método utilizado por el IDS

Para las subestaciones IEC 61850, todo el sistema de automatización, incluyendo todos los IED, sus modelos de datos y sus patrones de comunicación, se describe en un formato estandarizado: el SCL. Esta información permite utilizar un método diferente para detectar intrusiones: El sistema de supervisión puede crear un modelo del sistema de automatización de la subestación y puede comparar cada paquete de la red con este modelo. Incluso las variables contenidas en los mensajes (GOOSE, MMS, SV) comunicados se pueden evaluar frente a las previsiones derivadas del modelo del sistema. Este modelo del sistema implica, por lo tanto, una lista blanca, porque todos los paquetes que no coincidan con el modelo del sistema activarán una alarma. CKW seleccionó un IDS que se basa en este método (OMICRON StationGuard).

La ventaja de este método es que no sólo se detectan las amenazas de ciberseguridad, tal como los paquetes mal formados y las acciones de control de MMS prohibidas, sino también las fallas de comunicación, los problemas de sincronización de tiempos y, en consecuencia, también se detectan determinadas fallas de los equipos y se emiten las alarmas correspondientes.

Utilizando la sección de la subestación en el archivo SCL, se puede crear automáticamente un diagrama general de la subestación y las alarmas se pueden representar en este diagrama. Esta vista puede ayudar a identificar si una acción que ha activado una alarma se ha realizado intencionadamente: Por ejemplo, el evento podría haber sido causado por un ingeniero en una situación de prueba, o podría corresponder a una actividad maliciosa de una computadora portátil de pruebas infectada.

En el momento de escribir este artículo, la prueba de aceptación en fábrica (FAT, Factory Acceptance Test) de US Rothenburg ya se había realizado y la puesta en servicio estaba en curso. Tan sólo para la FAT, tuvo que terminarse casi toda la configuración de la red para poder probar si el diseño funcionaba. También aprendimos que el IDS requiere soporte y configuración adicionales para integrarse en los enrutamientos realizados por los múltiples niveles de cortafuegos. Hay múltiples duplicaciones del tráfico antes y después de los cortafuegos que podrían confundir la visión del IDS. Sin embargo, el IDS seleccionado se integró en este escenario correctamente. Además, es un esfuerzo considerable crear la matriz de comunicación para la configuración del cortafuegos, ya que esto debe hacerse manualmente. Como el IDS ya tiene una lista blanca SCL, también este proceso podría automatizarse en el futuro.

4. Conclusión y perspectivas

Si un atacante puede influir en una o más subestaciones, esto puede tener graves consecuencias para la red. Las subestaciones proporcionan varios vectores de ataque donde puede burlarse el cortafuegos. La arquitectura de red de subestación segura de CKW proporciona numerosas contramedidas a los vectores de ataque identificados en este documento. Las medidas de seguridad

proporcionan un alto nivel de seguridad, al tiempo que permiten procedimientos eficientes de mantenimiento e ingeniería mediante el acceso remoto. Esta arquitectura se basa en la detección de intrusión en el núcleo de la red. Para las subestaciones IEC 61850, se dispone de un método IDS que utiliza SCL para construir automáticamente una lista blanca de todo el tráfico de red permitido. Esto también permite mostrar los eventos detectados en el lenguaje de los ingenieros de protección, automatización y control para que puedan colaborar con los ingenieros de seguridad para determinar la causa de los eventos de manera eficiente.

Algo innato a la seguridad cibernética es que todo diseño puede mejorarse. Entre las mejoras está, por ejemplo, el control de acceso a la red basado en certificado según 802.1X [8] en lugar del método basado en MAC que se utiliza actualmente. Pero para ello, más IED tienen que admitir la norma 802.1X, lo cual no es el caso actualmente. Los documentos de seguimiento deben recoger las conclusiones de la puesta en servicio de este proyecto y documentar los resultados de futuras evaluaciones de seguridad y pruebas de penetración realizadas en esta subestación.

5. Referencias

[1] Klien, A.: "New approach for detecting cyber intrusions in IEC 61850 substations" (Nuevo método para la detección de intrusiones cibernéticas en subestaciones IEC 61850), PAC World Conference Europe, Glasgow, 2019

[2] "Analysis of the Cyber Attack on the Ukrainian Power Grid" (Análisis del ciberataque a la red eléctrica ucraniana), SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, acceso en noviembre de 2019

[3] "WIN32/INDUSTROYER - A new threat for industrial control systems", (WIN32/INDUSTROYER: una nueva amenaza para los sistemas de control industrial) https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, acceso en noviembre de 2019

[4] 'Threat Research - Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure' (Investigación de amenazas: atacantes despliegan el nuevo marco de ataque ICS "TRITON" y causan una interrupción operativa de la infraestructura crítica), https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, acceso en noviembre de 2019

[5] D. Kushner: "The Real Story of Stuxnet

How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program" (La verdadera historia de Stuxnet: cómo Kaspersky Lab localizó el malware que obstaculizó el programa de enriquecimiento de combustible nuclear de Irán), IEEE Spectrum, febrero de 2013

[6] Gosteli, Y., Klien A.: "Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg" (Tecnología de seguridad de control de estaciones: nueva arquitectura de seguridad cibernética con detección de intrusión en la subestación US Rothenburg), bulletin.ch, 2019, 6, pp 50-52

[7] NIST: "Framework for improving critical infrastructure cybersecurity" (Marco para mejorar la ciberseguridad de las infraestructuras críticas), versión 1.1, National Institute of Standards and Technology, abril de 2018

[8] IEEE: "802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control" (802.1X-2010: norma IEEE para redes de área local y metropolitana--control de acceso a la red basado en puertos), Norma internacional, febrero de 2010

OMICRON es una compañía internacional que presta servicio a la industria de la energía eléctrica con innovadoras soluciones de prueba y diagnóstico. La aplicación de los productos de OMICRON brinda a los usuarios el más alto nivel de confianza en la evaluación de las condiciones de los equipos primarios y secundarios de sus sistemas. Los servicios ofrecidos en el área de asesoramiento, puesta en servicio, prueba, diagnóstico y formación hacen que la nuestra sea una gama de productos completa.

Nuestros clientes de más de 160 países confían en la capacidad de la compañía para brindar tecnología de punta de excelente calidad. Los Service Centers en todos los continentes proporcionan una amplia base de conocimientos y un extraordinario servicio al cliente. Todo esto, unido a nuestra sólida red de distribuidores y representantes, es lo que ha hecho de nuestra empresa un líder del mercado en la industria eléctrica.

Para obtener más información, documentación adicional e información de contacto detallada de nuestras oficinas en todo el mundo visite nuestro sitio web.

www.omicronenergy.com