EATON EAS
Grid Automation System Solutions

Substation Automation - Cybersecurity

Maricelly Rivera / Alejandro Guzman

Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

Grid Automation System Solution Substation Automation / Cybersecurity

INTEROPERABILIDAD

CIBERSEGURIDAD

CONFIABILIDAD

NERC CIP

ROBUSTEZ

AMBIENTE ELÉCTRICO

CERTIFICADO

SCADA

Yukon Visual T&D

MySQL

Servidor SCADA

SMP Gateway - Automation Platform

SMP Digital Series

Concentrador /Gateway

RTU/ **Controlador**

Adquisición de Datos

Indicadores de Fallas

GridAdvisor Series II smart sensor

Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

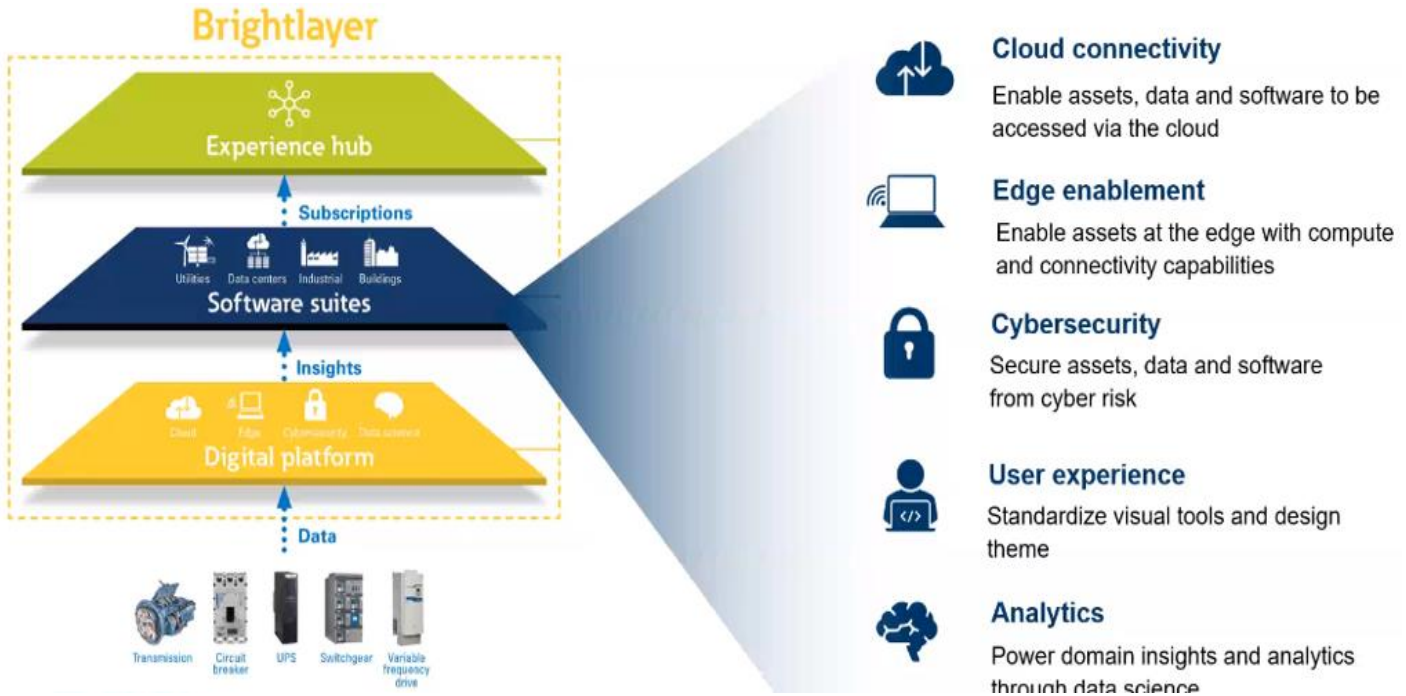
Soluciones EATON EAS

Automatización de Subestaciones Eléctricas

- **Sistema SCADA (IHM) Yukon Visual T&D**
  - IHM Local Nivel 2
  - SCADA de Operación Centralizado
- **Sistema de Automatización de Subestaciones (SAS)**
  - Concentrador de subestación / Gateway (SMP)
  - Redes de comunicación y sincronización de tiempo
- **Adquisición de señales y control (RTU)**
  - RTU SMP IO
- **Sistema de automatización para administración de redes de MT**
  - Localizadores de falla Grid Advisor
  - Concentrador de IEDs (SMP)

The Brightlayer Utilities suite

- IED manager suite (IMS)
- Yukon Feeder Automation (YFA)



Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

Ciberseguridad OT: Una Necesidad Urgente para subestaciones eléctricas en el Sector Energético

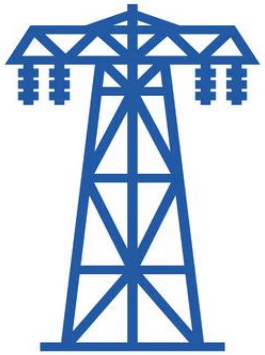
La infraestructura eléctrica es un componente crítico de la economía moderna, y su confiabilidad es esencial para el bienestar de las comunidades y el funcionamiento de las empresas en el país. Las subestaciones eléctricas desempeñan un papel fundamental en la distribución y transmisión de energía, lo que las convierte en objetivos potenciales para ataques cibernéticos. En un mundo cada vez más conectado, la ciberseguridad en operaciones de tecnología (OT) se ha convertido en una necesidad urgente en el sector energético.

La Vulnerabilidad de las Subestaciones Eléctricas

Las subestaciones eléctricas son el punto de convergencia de la infraestructura eléctrica, donde se controlan y gestionan los flujos de energía. Las amenazas cibernéticas a las subestaciones eléctricas pueden tener consecuencias devastadoras, desde interrupciones en el suministro eléctrico hasta daños físicos en la infraestructura. Los atacantes pueden aprovechar vulnerabilidades en los sistemas OT para manipular equipos, causar cortes de energía o incluso infiltrarse en la red eléctrica nacional. Para garantizar la confiabilidad y la seguridad de la infraestructura eléctrica, es esencial abordar estos riesgos de manera proactiva con **sistemas de automatización y gestión de IEDs confiables, robustos y ciberseguros.**

CIBERSEGURIDAD

NERC CIP



CERTIFICADO

Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

Ciberseguridad OT: Una Necesidad Urgente para subestaciones eléctricas en el Sector Energético

La Importancia de la Ciberseguridad en OT

La ciberseguridad en OT se refiere a las prácticas y medidas **diseñadas para proteger los sistemas de control y automatización de amenazas cibernéticas.** Estas medidas son cruciales para garantizar la operación segura y confiable de las subestaciones eléctricas. Algunas de las razones por las cuales la ciberseguridad en OT es fundamental incluyen:

1. Protección contra Amenazas Emergentes

El panorama de amenazas cibernéticas está en constante evolución, con **atacantes cada vez más sofisticados**. La implementación de medidas de ciberseguridad en OT ayuda a detectar y mitigar amenazas antes de que causen daño.

2. Minimización de Riesgos Operativos

Los ataques cibernéticos pueden tener un impacto significativo en la operación de las subestaciones eléctricas. **La ciberseguridad en OT ayuda a minimizar los riesgos operativos y garantiza que las subestaciones sigan funcionando de manera eficiente.**

3. Cumplimiento Normativo

Las regulaciones y normativas en el sector eléctrico colombiano exigen un enfoque riguroso en la ciberseguridad. Cumplir con estas regulaciones no solo es una obligación legal, sino que también protege la reputación de las empresas de energía.

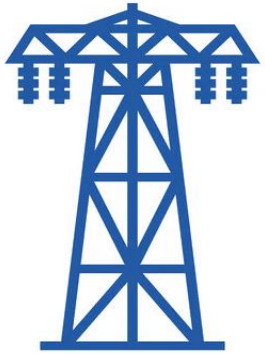
4. Protección de la Infraestructura Crítica

Las subestaciones eléctricas se consideran infraestructura crítica, y su protección es esencial para la seguridad nacional. La ciberseguridad en OT contribuye a salvaguardar esta infraestructura vital.

Concentrador
Gateway / RTU

CIBERSEGURIDAD

NERC CIP



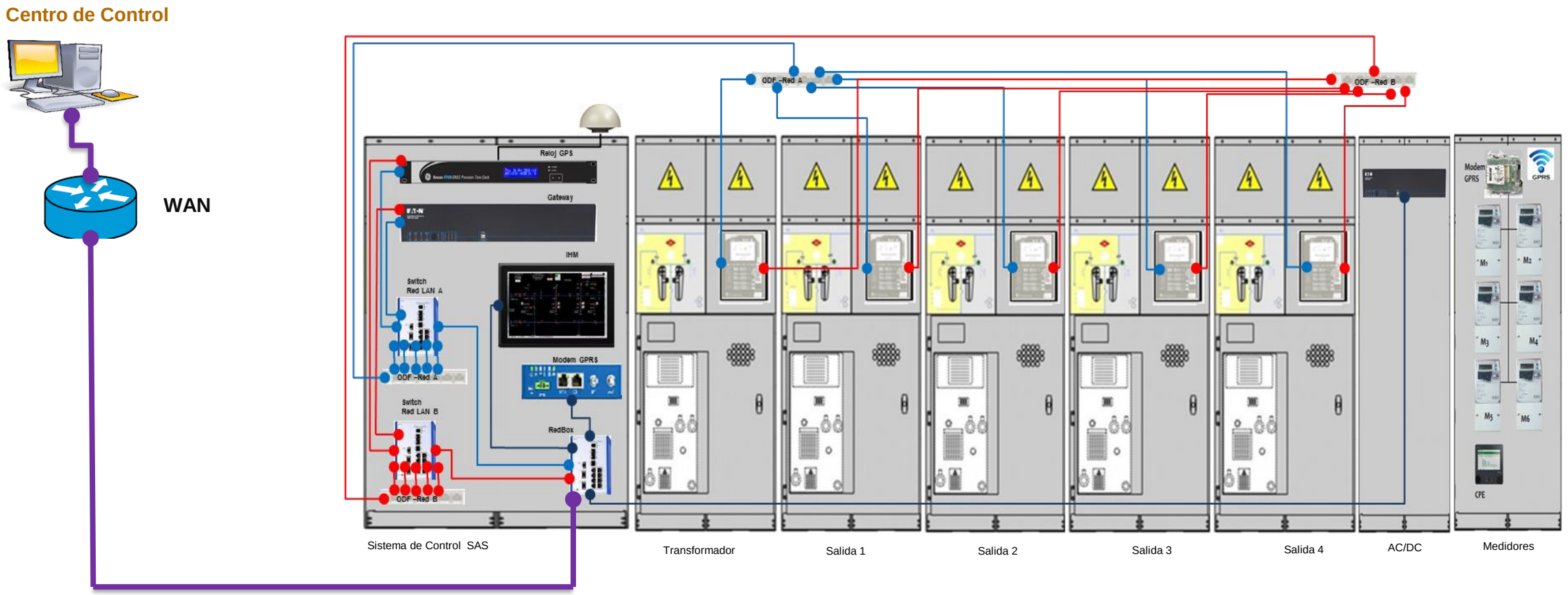
CERTIFICADO

Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

Porque Implementar Sistemas de Automatización y Gestión de IEDs ciberseguros?

Para abordar eficazmente los desafíos de la ciberseguridad en las subestaciones eléctricas, las empresas de energía en Colombia deben considerar la implementación de **sistemas de automatización y gestión de IEDs ciberseguros en un entorno OT.**



Plataformas de automatización / Gateway / Ciberseguridad

En el ámbito de los sistemas eléctricos, contar con una plataforma de automatización que sea moderna, confiable, robusta y con una sólida ciberseguridad para entornos OT, es esencial para garantizar un funcionamiento seguro y eficiente de las subestaciones eléctricas. En este sentido, la plataforma de automatización SMP SG4260 se destaca como una solución integral que combina todas estas características en una sola plataforma.

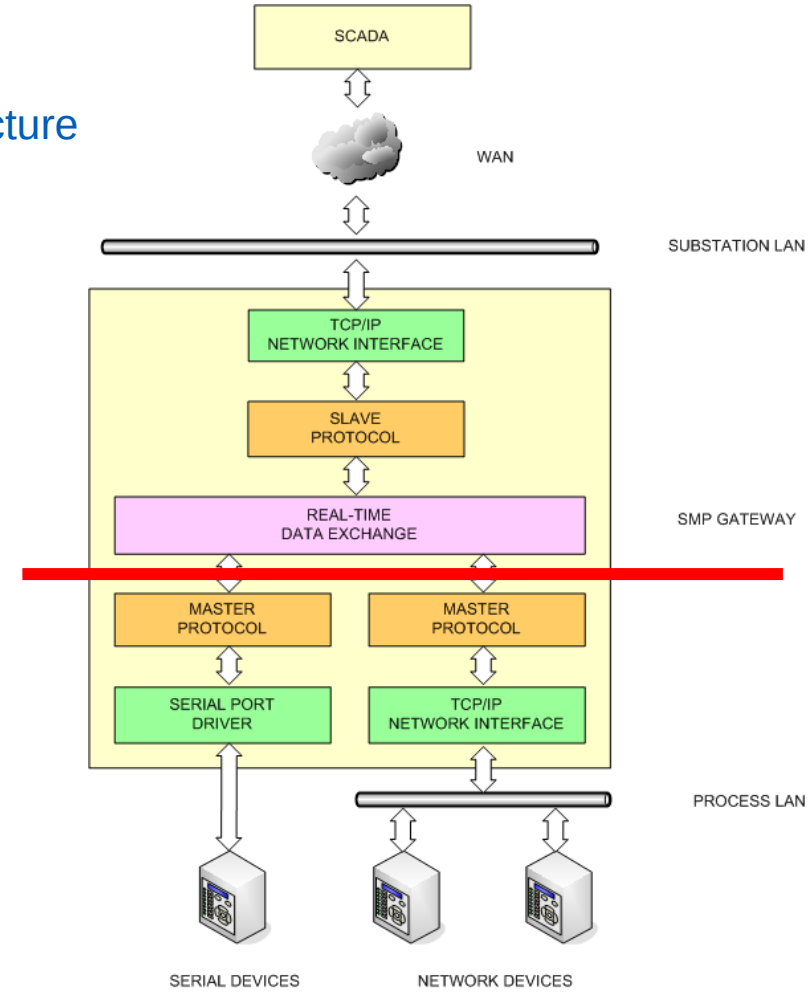
Cuenta con subestaciones eléctricas automatizadas con plataforma SMP EATON

Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

Plataformas de automatización / Gateway / Ciberseguridad

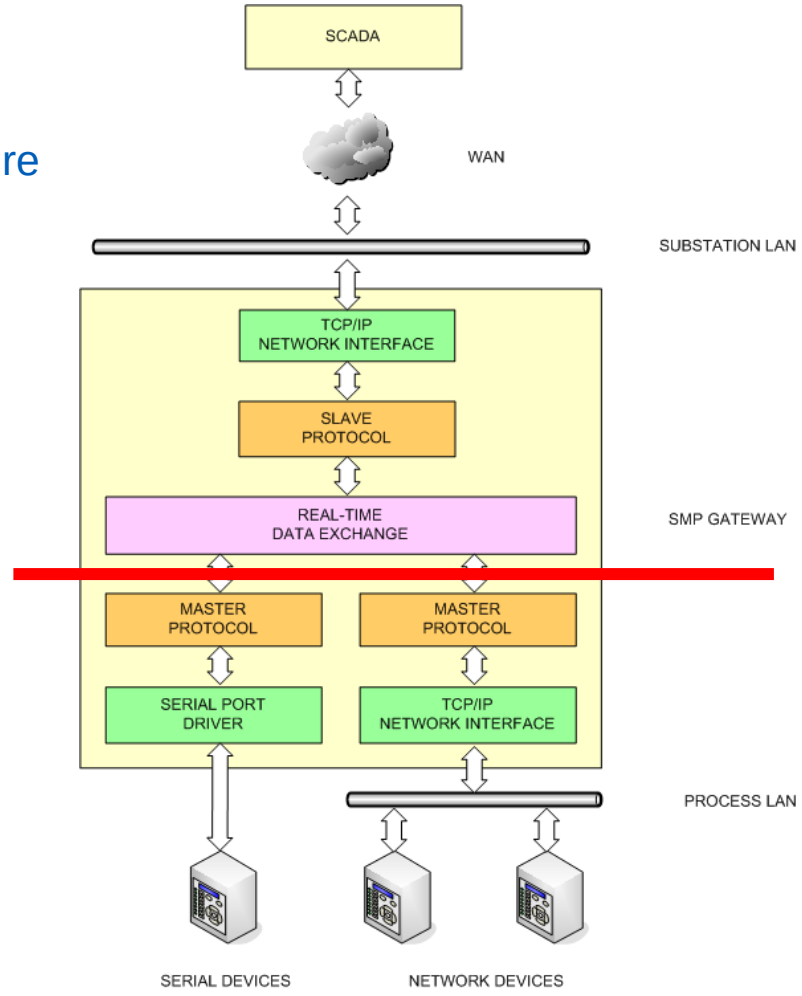
SMP Gateway
Software Architecture



- SMP Gateway procesa todos los datos intercambiados entre dispositivos y SCADA, y **aísla las redes**.
- Los múltiples adaptadores de red proporcionan **segmentación de red.**
- **No se enrutan paquetes TCP/IP entre redes**.
- **Estructura de datos en tiempo real (RTDx).**
- Se ha agregando soporte VLAN para proporcionar capacidades de segmentación adicionales.
- La cantidad de tags mínimas en una configuración estándar para Gateway es de **20.000 puntos**.

Plataformas de automatización / Gateway / Ciberseguridad

SMP Gateway
Hardware Architecture



- Equipo dedicado para aplicaciones de subestación eléctrica basados en hardware con **sistema operativo embedido** y características de seguridad Secure SCADA protocol (**SSL/TLS**). No computadores industriales/subestación.
- Equipos **grado subestación IEEE Std 1613, IEC 61850 -3** (no grado industrial).
- Para uso y operación en Colombia (Clima Tropical), manejan un limite de temperatura superior a los **80°C** para ambientes eléctricos en el país.
- Prueba Dry Heat Bd de **16 horas a 85°C**, dada la condición de temperatura en una subestación eléctrica. **IEC 60068-2-2 ed5.0 e IEC 60068-2-1 ed6.**
- **Hardware del CSE sin disipadores de calor en su diseño, puesto que son generadores de calor al interior del tablero SAS de la subestación**.

Plataformas de automatización / Gateway / Ciberseguridad

- Todos los modelos de SMP Gateway han obtenido la certificación Wurldtech Achilles Communications como dispositivo de red.
-
- La certificación de Achilles confirma que SMP Gateway puede mantener la disponibilidad incluso cuando se envía a un gran volumen de tráfico, o a un tráfico mal formado como resultado de problemas de red o intenciones maliciosas.
-
- Esta certificación es un subconjunto de la certificación ISA Secure.

CIBERSEGURIDAD

NERC CIP

CERTIFICADO

Cuenta aproximadamente con subestaciones eléctricas automatizadas con plataforma SMP EATON certificadas.

Metodología de prueba

- Las pruebas ejecutadas se dividen en dos categorías:

  - Pruebas de agotamiento de recursos. Pruebas que intentan agotar un recurso particular del DUT. Por ejemplo, tormentas que envían paquetes a velocidades rápidas en un intento de desbordar los recursos de memoria del DUT.
  - Pruebas de paquetes no válidos. Pruebas que envían paquetes formados ilegalmente al DUT. Las pruebas utilizan fuzzers y gramáticas para crear estos paquetes no válidos.

RECOMENDACIONES

Ciberseguridad

- Se recomienda equipo CSE con certificado de pruebas de robustez cibernética para dispositivos y equipos, evaluando su resistencia a amenazas cibernéticas.

- Se recomienda que el componente hardware y software del Concentrador deba permitir la prevención de ciberataques, a través de la robustez de su sistema operativo embebido, una matriz de datos en tiempo real (RTDx) y componentes de red.

- Se recomienda que el hardware y software del Concentrador de subestación sea del mismo fabricante, aplicaciones software en hardware de terceros desde el punto de vista del desempeño y ciberseguridad, la aplicación SAS se vuelve una virtualización, la cual es muy versátil pero difícil de mantener debido a su vulnerabilidad; un concentrador de subestación debe garantizar el desempeño y seguridad cibernética de una aplicación de automatización de subestaciones 100% segura, avalada por certificaciones internacionales.

RECOMENDACIONES

Temperatura de Operación Hardware

- Se recomienda que los equipos CSE para uso y operación en Colombia (Clima Tropical), manejen un limite de temperatura superior a los 80°C para ambientes eléctricos en Colombia. El equipo CSE opera en temperaturas -40 °C to 80 °C (Temperatura de funcionamiento).

- Se recomienda cumplir con los requisitos de la prueba Dry Heat Bd de 16 horas a 85°C, dada la condición de temperatura en una subestación eléctrica. IEC 60068-2-2 ed5.0 e IEC 60068-2-1 ed6.

- Se recomienda considerar que el hardware del CSE no incluya disipadores de calor en su diseño, puesto que son generadores de calor al interior del tablero SAS de la subestación.

- Evaluar derrateo de temperatura de operación de los equipos CSE (reporte de pruebas del fabricante).

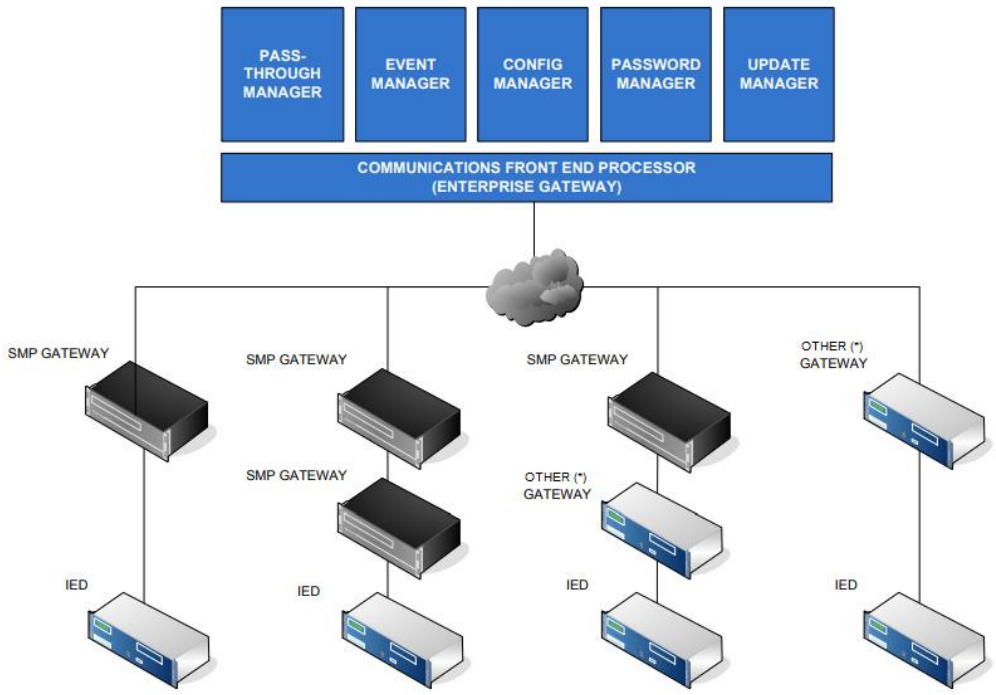
RECOMENDACIONES

Tags / Numero de puntos

Con la nueva tecnología de los concentradores de subestación y atendiendo a las caracteristicas minimas requerida de estos equipos, la cantidad de tags minimas en una configuración estándar es de 20.000 puntos, con la posibilidad de ampliar hasta 30.000 puntos.

Software de Gestión de IEDs/ Ciberseguridad

IED MANAGER SUITE (IMS)



Descripción del Administrador de IED IMS (IED Manager Suite):

Passthrough Manager: proporciona acceso de mantenimiento seguro a IED remotos, de conformidad con NERC Requisitos del PIC. Presenta automáticamente a los usuarios la lista de IED a los que están autorizados a acceder y les permite seleccionar y conectarse a un dispositivo mediante una operación de un solo clic. Mantiene registros de acceso y seguimientos completos de todas las sesiones Passthrough. Con Passthrough Manager, *AIRE* puede acceder remotamente al Puerto de mantenimiento de dispositivos remotos para mantenimiento e ingeniería. Puede gestionar el acceso de seguridad del IED política y registrar todas las operaciones.

IMS Event Manager: consolida todos los eventos SER/DFR/IED en una única base de datos homogénea a la que se puede acceder a los usuarios a través de un servidor web. Puede sondear los IED de forma programada o trabajar con SMP Gateway. Usando un SMP Gateway en la subestación, los IED pueden ser sondeados para determinar la disponibilidad de nuevos registros/archivos de eventos/perturbaciones en un de forma continua. Tan pronto como haya nueva información disponible, el SMP Gateway la recogerá en la subestación. nivel y reenviado a la base de datos central. En el proceso, se analiza para que las notificaciones por correo electrónico opcionales que contienen los archivos de eventos que se pueden enviar a usuarios seleccionados. Como resultado, los usuarios finales tienen información detallada sobre acontecimientos a los pocos minutos de su ocurrencia. Todos los archivos que contienen datos secuenciados en el tiempo generalmente se almacenan en el base de datos en formato sin formato (para mantener la información completa), pero normalmente se puede convertir al formato COMTRADE en sobre la marcha, para su uso con visores COMTRADE y paquetes de análisis de terceros. Con Event Manager, usted recupere y procese automáticamente archivos de eventos de relés de protección y otros dispositivos de subestación. ***AIRE*** puede almacenar y mostrar datos de eventos y notificar a usuarios y grupos.

IMS Configuration Manager: proporciona servicios de gestión de configuración para dispositivos compatibles. El Configuration Manager recupera y almacena archivos y/o configuraciones de configuración del dispositivo. Escanea artefactos explosivos improvisados en un de forma programada o realiza un seguimiento de los cambios de forma continua cuando se utiliza con SMP Gateway en la subestación. Él detecta cambios en la configuración del dispositivo y notifica a los usuarios cuando se detecta un cambio. Con configuración Administre, detecte y registre todos los cambios de configuración de IED admitidos. ***AIRE*** puede monitorear automáticamente artefactos explosivos improvisados configuración y generar alertas cuando se ha cambiado la configuración de un IED. Los usuarios de IED Manager Suite Podrá revisar en cualquier momento el estado de configuración del IED junto con el historial de cambios de configuración.

IMS Password Manager: proporciona un conjunto completo de herramientas e informes para administrar contraseñas de IED y ayudar cumplir con los requisitos reglamentarios. ***AIRE*** puede administrar contraseñas de IED, ver y actualizar contraseñas a pedido, imprimir Informes de cumplimiento y caducidad de contraseñas. Con Password Manager, usted tiene el control del proceso. IMS Update Manager es una extensión de IMS Configuration Manager que proporciona la capacidad de realizar cargas de firmware y ajustes de configuración para SMP Gateway. Las capacidades de IMS Security Manager están actualmente incluidas en IMS Passthrough Manager y no se ofrecen. por separado. Actualmente, IED Manager Suite (IMS) admite los dispositivos descritos en el documento: Dispositivos Compatible con IMS

Powering Business Worldwide

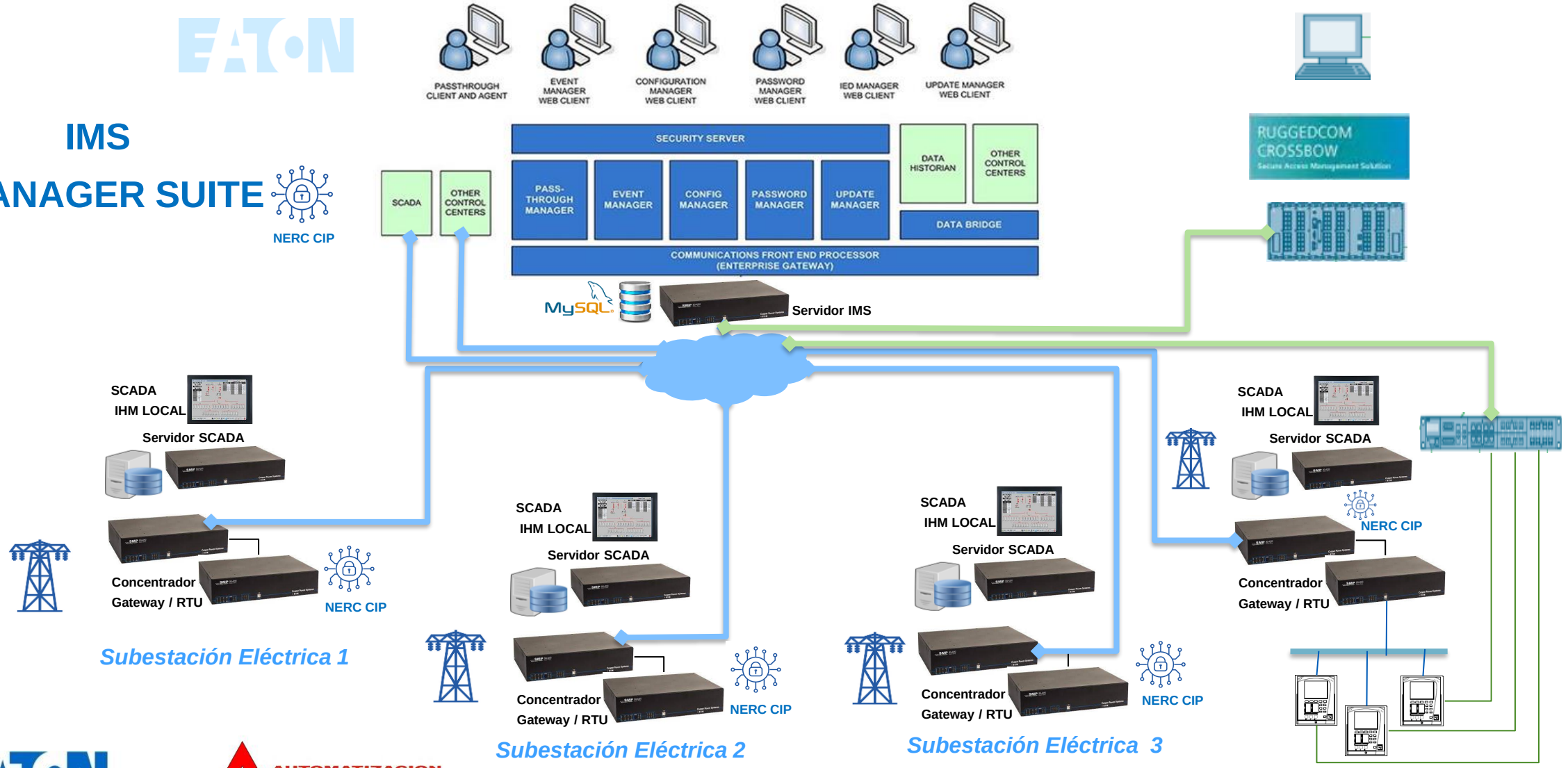
AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

ARQUITECTURA DE CONTROL, COMUNICACIONES Y CIBERSEGURIDAD

IMS

IED MANAGER SUITE

NERC CIP



Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

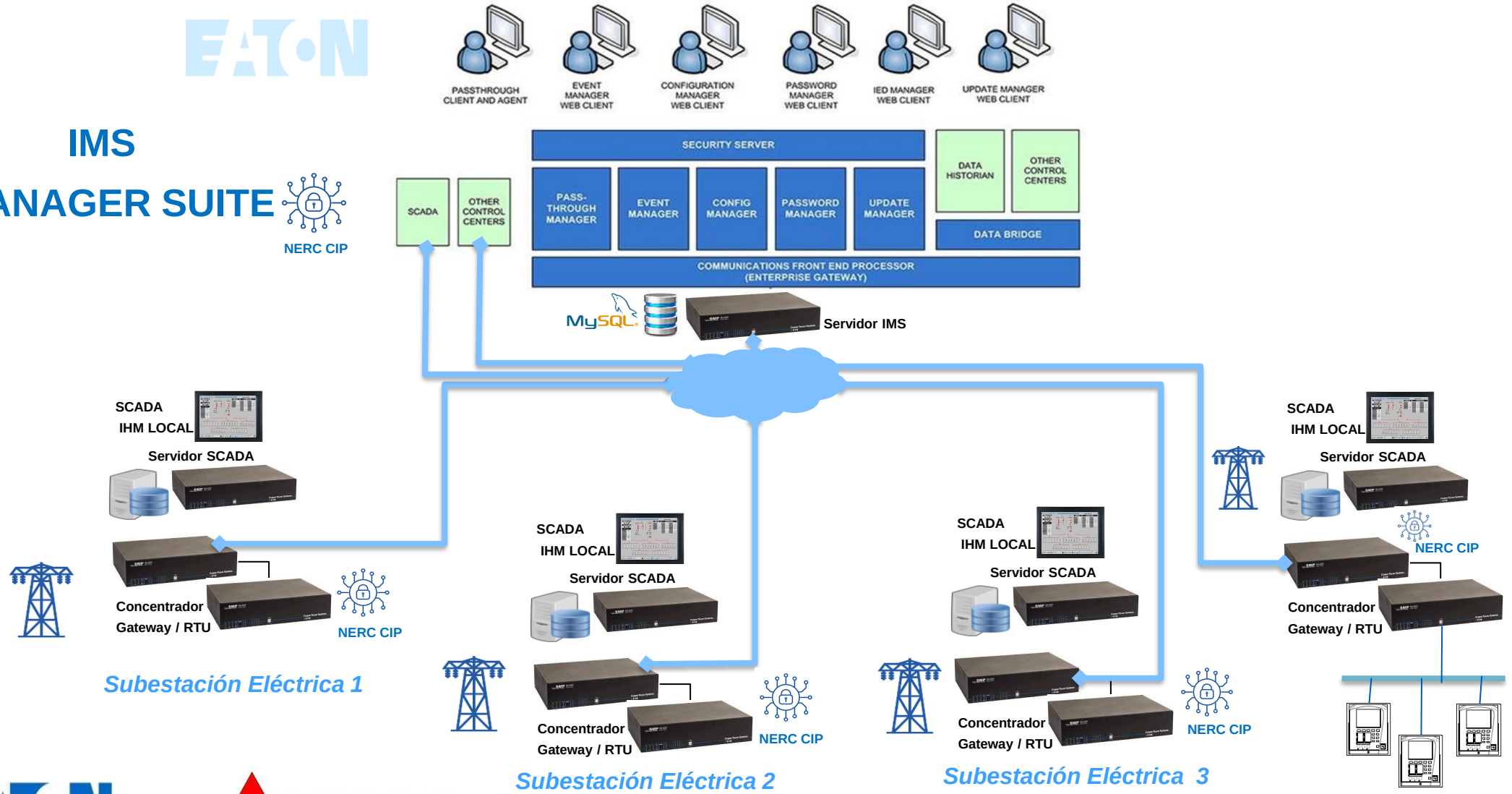
Brightlayer Utilities suite

ARQUITECTURA DE CONTROL, COMUNICACIONES Y CIBERSEGURIDAD

IMS

IED MANAGER SUITE

NERC CIP



Powering Business Worldwide

AUTOMATIZACION AVANZADA S.A.
www.automatizacionavanzada.com

Brightlayer Utilities suite
Subestación Eléctrica …n

Contáctanos

Alejandro Guzmán

Móvil: +52 33 1411 - 8061

alejandroguzman1@eaton.com

Maricelly Rivera

Móvil: +57 3168752723

mrivera@automatizacionavanzada.com