Protección cibernética sistema WAMPAC - ECCANDE

Chrystian Ruiz Diaz, Enrique Davalos

ANDE - Facultad Politécnica/UNA

Paraguay

1.1 Resumen

La creciente necesidad de gestionar de forma eficiente la demanda de energía eléctrica está impulsando a los sistemas de transmisión de energía eléctrica atravesar por varios desafíos exigentes como la complejidad en la operación, mejorar los niveles de confiabilidad y la constante evolución de las redes eléctricas interconectadas.

En este sentido, los sistemas de Monitoreo, Protección y Control de Área Amplia (*WAMPAC- Wide Area Monitoring Protection and Control*) han sido desarrollados como una solución para optimizar la operación de las redes eléctricas interconectadas, la cual está sustentada fuertemente en los avances de las Tecnologías de la Información y Comunicación – TIC.

Este documento presenta una revisión de las vulnerabilidades y las protecciones contra ataques cibernéticos implementada en el sistema WAMPAC, proyecto denominado ECCANDE – Esquema de Control de Contingencia de ANDE que tiene como objetivo interconectar de manera segura los sistemas eléctricos de Brasil, Paraguay, Argentina y Uruguay a través de las Centrales Hidroeléctricas de Generación los Subsistemas SS1 con Acaray - Itaipu y SS2 con Yacyreta.

El ECCANDE requiere de información precisa y sincronizada obtenida desde las PMU- *Phasor Measurement Units* instaladas en subestaciones estratégicas, distantes entre sí y geográficamente distribuidas y sincronizadas con sistema GPS - *Global Positioning System*, a su vez, estas PMU intercambian información con el Concentrador de Datos Fasoriales PDC- *Phasor Data Concentrator* que procesan un conjunto de algoritmos para las lógicas de protecciones, se comunican a través de una de red exclusiva y dedicada *MPLS-TP - Multiprotocol Label Switching - Transport Profile*, así mismo, están integradas a los sistemas SCADAs de ANDE, ITAIPU y YACYRETA a través de RTU- *Remote Terminal Unit* para el intercambio de información.

Cada uno de estos dispositivos, la sincronización, las lógicas de protección, el intercambio de información con sus diversos protocolos y la integración con otros sistemas representan un riesgo para la seguridad cibernética. Tal como en los sistemas IT - *Information Technology*, donde uno de los ataques comunes es la Denegación de Servicio DoS - *Denial of Service* que causa la indisponibilidad de un servicio o sistema, en el sistema ECCANDE, en una operación interconectada, en caso exitoso de un ataque de este tipo, podría causar la separación inmediata a dos SubSistemas SS1 y SS2. Mas aún, en un escenario más crítico, la pérdida de disponibilidad de las PDCs dejando sin lógicas de protecciones a todo el sistema interconectado acompañado de un evento eléctrico,

podría ocasionar daños severos de gran magnitud a nivel regional, razón por la cual es sumamente importante la protección cibernética adecuada.

1.2 Palabras clave

ANDE, ECCANDE, ITAIPU, PDC, PMU, Protección Cibernética , RTU, WAMPAC, YACYRETA

1.3 Cuerpo del trabajo

1. INTRODUCCION

El sistema de Monitoreo, Protección y Control de Área Amplia (*WAMPAC- Wide Area Monitoring Protection and Control*) está conformada por dispositivos denominados PMU - *Phasor Measurement Unit* los cuales son uno de los dispositivos importantes que proporciona datos sincronizados para el monitoreo, control y protección de la red eléctrica. En esencia, se encargan de colectar las mediciones analógicas con una tasa de muestreo de 30 a 120 muestras por segundo, estas muestras se colectan desde varios lugares geográficos de las subestaciones y sincronizadas a través de GPS, posteriormente pasa por un conversor Análogo-Digital, se procesa y transmite al PDC a través de una red comunicación, la estructura de la PMU se muestra en el diagrama en bloque de la Figura 1 **Diagrama en Bloque de una PMU**, los bloques "*Analog Input*" y "*Anti-aliasing*" se puede excluir de las consideraciones de seguridad cibernética. Todos los demás bloques y sistemas en adelante deben ser consideradas y protegidas, incluyendo la señal externa el bloque "*GPS Satellite Signal*".

Estas comunicaciones entre las PMUs y los PDCs tienen elevados y estrictos requerimientos como; alto grado de disponibilidad, tolerante a fallas, ancho de banda suficiente para enviar constantemente una avalancha de informaciones de manera simultánea como: las mediciones de tensión, corriente, potencias, ángulos y estados de los interruptores de las líneas de transmisión. El envío de estas mediciones debe ser lo suficientemente rápida, el tiempo de retardo debe ser mínimo entre 50ms a 200ms según las lógicas protecciones implementadas [1].

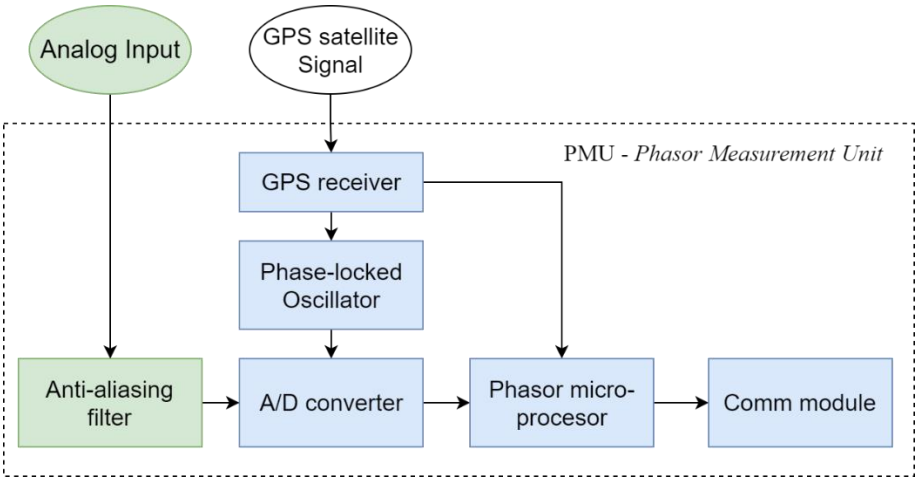

Figura 1 Diagrama en Bloque de una PMU

En el presenta trabajo se presenta la arquitectura del sistema ECCANDE, se describe las vulnerabilidades y las protecciones cibernéticas implementadas. Este documento se organiza de la siguiente manera: en la Sección 2 se describe la infraestructura tecnológica que conforma el ECCANDE, en la sección 3 se aborda brevemente sobre algunos ataques a estos sistemas, en la sección 4 se describe algunas de las protecciones cibernéticas que han sido implementadas, seguido de la conclusión en la sección 5.

2. INFRAESTRUCTURA

El ECCANDE está conformado por dieciséis PMUs instalados en subestaciones estratégicamente seleccionadas que permiten la completa observabilidad del sistema de potencia del Sistema interconectado incluyendo las Centrales de Generación Acaray, Itaipu y Yacyreta.

PMUs: en confirmación redundante están conectadas a una red exclusiva MPLS/TP - *Multiprotocol Label Switching - Transport Profile* de veintitrés multiplexores interconectados a través de fibras Ópticas del tipo OPGW - *Optical Ground Wire* y ADSS – *All Dielectric Self Supporting* como se indica en la *Figura 2* **Arquitectura de red MPLS/TP referencial ECCANDE**. La sincronización horaria lo realiza a través del GPS con el protocolo IRIG-B - *Inter-Range Instrumentation Group* conectado directamente a la PMU, conforme se indica en la **Figura *3* Arquitectura Red Local ECCANDE**.

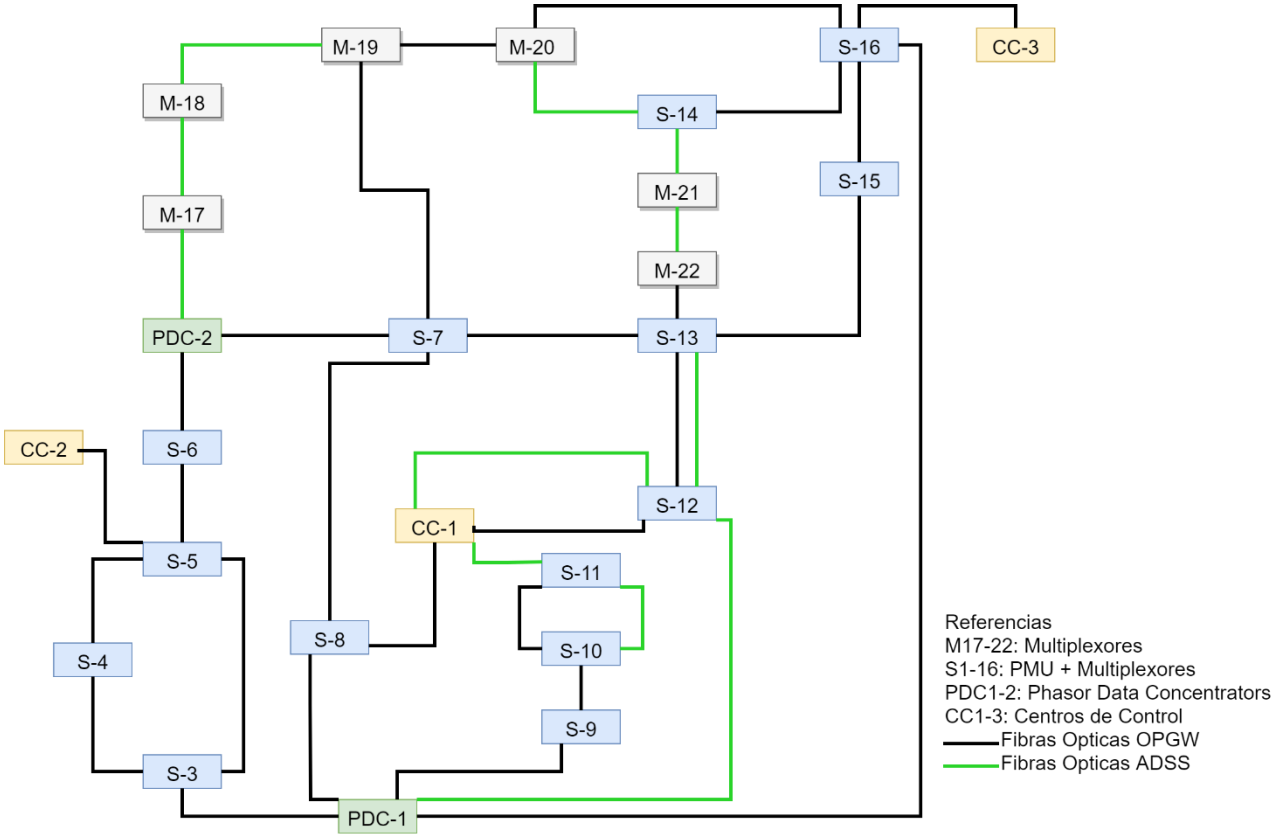

Figura 2 Arquitectura de red MPLS/TP referencial ECCANDE.

PDCs: en configuración redundantes adquieren los datos muestreados de las diversas PMUs a través del protocolo de comunicación estándar C37.118 para las mediciones y transferencia de datos de sincrofasores. Estas PDCs realizan las verificaciones y validaciones en tiempo real del estado actual de la red eléctrica, en caso de presentarse algún evento anómalo, este genera una contingencia y envía una orden de disparo por IEC60870-5-104 (IEC - *International Electrotechnical Commission*), en adelante IEC-104 a la RTU [2].

RTUs: las RTU redundantes colectan las mediciones y estados de los interruptores de las subestaciones del ECCANDE a través de la integración con el PDC con el protocolo IEC-104. En los casos de contingencias detectadas por los PDCs, esta le envía la orden de disparo a la RTU y éste genera la orden de disparo por IEC- 61850 que lo envía directamente a la PMU de la subestación para abrir el interruptor.

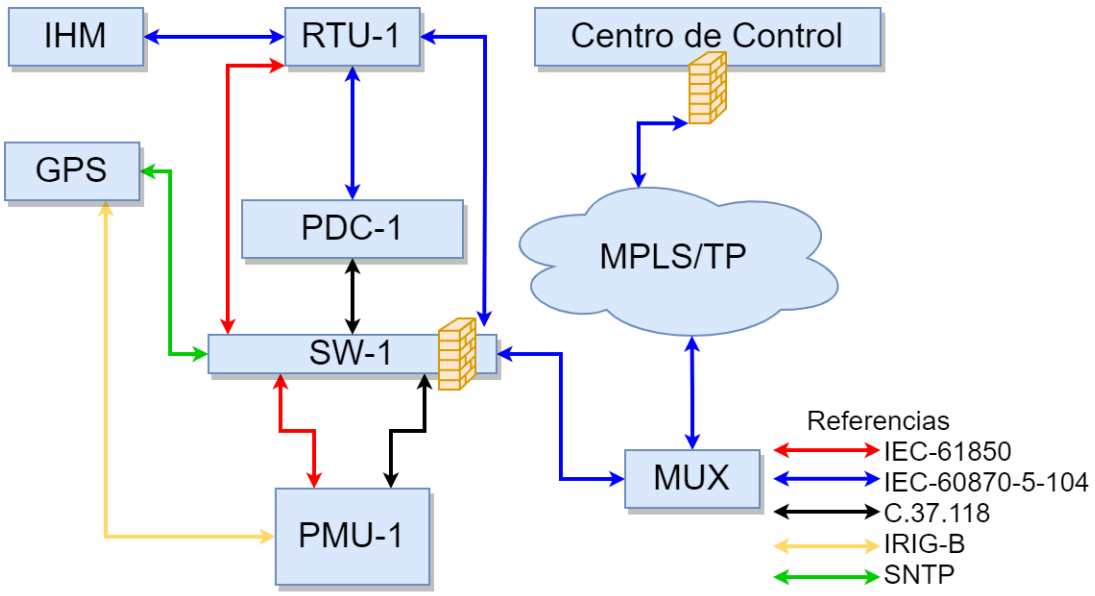

Figura 3 Arquitectura Red Local ECCANDE

Las Interfaces Hombre-Maquina - IHM están instaladas en cinco ubicaciones distintas, redundantes para los clientes IHM y el servidor es centralizado, sin redundancia.

Los dispositivos de red la conforman una solución de Switch, router y firewall embebidos donde se interconectan las redes externas al ECCANDE; interconexión con los SCADAs de ANDE, ITAIPU y YACYRETA a través del protocolo IEC-104 [3].

3. ATAQUES

De acuerdo con la arquitectura descrita en la sección 3, de las tecnologías implementadas y los protocolos utilizados IEC-104, IEC-61850 y C.37.118, estos protocolos intercambian la información

en texto claro, legible y sin encriptar, en esta sección se describen algunos ataques que podrían aprovechar algunas de estas vulnerabilidades del sistema.

3.1. **Denegación de Servicio (DoS):** los ataques DoS en general ocasiona la indisponibilidad de un sistema o servicio realizando saturación y agotamiento de ancho de banda en la red, en una operación interconectada eléctrica ANDE-ITAIIPU-YACYRETA, la indisponibilidad de las señales criticas podría causar la automática desconexión y separación en los dos subsistemas SS1 y SS2, otro evento como la indisponibilidad de algunas de las señales utilizadas por el AGC - *Automatic Generation Control* puede cambiar el control automático a manual, u otro evento más crítico como la pérdida de las PDCs dejando sin lógicas de protección al sistema interconectado y acompañado de un evento eléctrico podría ocasionar daños severos de gran magnitud.

3.2. Man In The Middle (MiTM): el atacante se interpone en el medio de la comunicación legitima entre el cliente(PMUs) y el servidor (PDCs) sin que estos se enteren, entonces el atacante podría modificar los las mediciones reportadas a los PDCs y con ello este podría actuar o dejar de actuar las lógicas de protecciones.

3.3. **Delay:** en una red SCADA el retraso o retardo de los paquetes en la comunicación entre las RTUs y el SCADA es tolerante, en cambio en la red del ECCANDE el tiempo de retraso de estos paquetes es admisible hasta 200ms, tiempos mayores podrían causar problemas a los PDCs para el monitoreo, protección y control en tiempo real de la red eléctrica.

3.4. **Sniffing:** dados que los protocolos utilizados IEC-104, IEC-61850 y C.37.118 transmiten la información en texto claro, legible y sin encriptar, son susceptibles a ser analizados previamente para posteriormente realizar ataques del tipo MiTM [4].

4. MEDIDAS DE PROTECCION

Dada la complejidad de la infraestructura tecnológica que conforman el sistema ECCANDE, en esta sección se presentan algunas medidas generales para la protección cibernética.

Protección con firewalls de nueva generación NGFW - *Next Generación Firewall:* en configuración de alta disponibilidad en las interconexiones del ECCANDE con las redes externa, los SCADAs de ANDE, ITAIPU y YACYRETA, a más de las protecciones típicas de permitir únicamente las IP, puertos origen/destino, y protecciones contra ataques nativos de los sistemas de IT, se implementó una política restrictiva hasta la capa de aplicación del modelo de referencia OSI - *Open Systems Interconnection*, incluyendo características de antimalware, a nivel de aplicaciones solo se permiten el tráfico IEC-104 denegando todos los demás tipos de tráfico innecesarios que no aplica para el ECCANDE como el tráfico de voz-video, P2P - *Peer to Peer*, redes sociales, correo electrónico entre otros.

Sistema de Detección y Prevención de intrusos IPS/IDS *Intrusion Prevention and Detection System* implementado en todas las conexiones entrantes y salientes al ECCANDE, actualizados permanente con las bases de datos de firmas del fabricante a través del Sistema Gestión Centralizada y Actualizaciones - SGCA de los firewalls.

Control de aplicaciones implementadas para permitir únicamente los tipos de ASDU - *Application Service Data Unit* del protocolo IEC-104 implementado en el ECCANDE, como referencia se indica en la **¡Error! No se encuentra el origen de la referencia.** y el nivel de granularidad de bloqueo en la capa de aplicaciones del modelo OSI [5].

Tabla I Referencia Tipo de ASDU permitido

Tipo de ASDU - *Application Service Data Unit*	
IEC.60870.5.104_Information.Transfer.M.ME.NB.1	IEC.60870.5.104_Information.Transfer.M.ST.NA.1
IEC.60870.5.104_Information.Transfer.M.ME.NC.1	IEC.60870.5.104_Information.Transfer.M.ST.TA.1
IEC.60870.5.104_Information.Transfer.M.ME.ND.1	IEC.60870.5.104_Information.Transfer.M.ST.TB.1
IEC.60870.5.104_Information.Transfer.M.ME.TA.1	IEC.60870.5.104_Information.Transfer.P.AC.NA.1
IEC.60870.5.104_Information.Transfer.M.ME.TB.1	IEC.60870.5.104_Information.Transfer.P.ME.NA.1
IEC.60870.5.104_Information.Transfer.M.ME.TC.1	IEC.60870.5.104_Information.Transfer.P.ME.NB.1
IEC.60870.5.104_Information.Transfer.M.ME.TD.1	IEC.60870.5.104_Information.Transfer.P.ME.NC.1
IEC.60870.5.104_Information.Transfer.M.ME.TE.1	IEC.60870.5.104_Information.Transfer.Parameter.Transfer
IEC.60870.5.104_Information.Transfer.M.ME.TF.1	IEC.60870.5.104_Information.Transfer.Process.Control
IEC.60870.5.104_Information.Transfer.M.PS.NA.1	IEC.60870.5.104_Information.Transfer.Process.Monitor
IEC.60870.5.104_Information.Transfer.M.SP.NA.1	IEC.60870.5.104_Information.Transfer.System.Information
IEC.60870.5.104_Information.Transfer.M.SP.TA.1	IEC.60870.5.104_Supervisory.Functions
IEC.60870.5.104_Information.Transfer.M.SP.TB.1	IEC.60870.5.104_Information.Transfer.Out.Validation

Integración con el sistema de monitoreo de red OT de ANDE

A través de la integración con el sistema de monitoreo OT, se tiene la visualización del estado de los dispositivos de red del ECCANDE que permite la trazabilidad de los eventos, pérdida y/o mantenimiento de los enlaces. Con este sistema se tiene la posibilidad de generar y notificar alarmas por correo electrónico para una detección temprana de algún inconveniente en la red, además de la extracción de varios reportes como se indica en la **Figura *4* Sistema Monitoreo OT**.

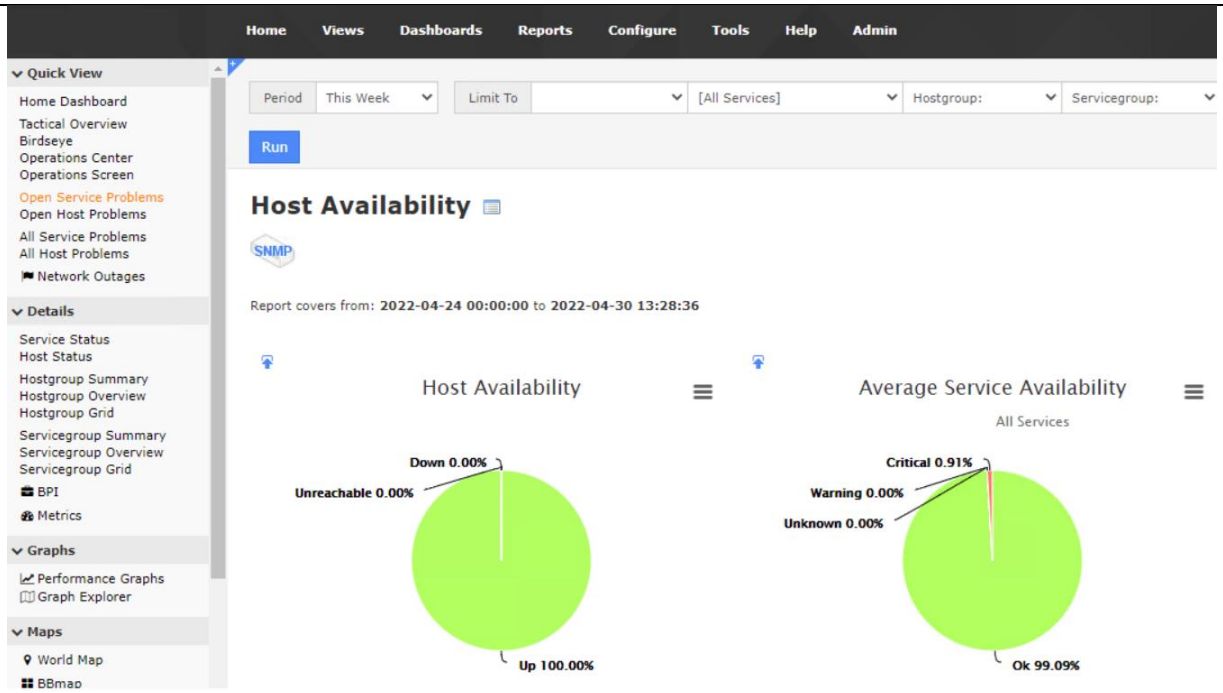

Figura 4 Sistema Monitoreo OT - SMOT

El sistema de Gestión de Eventos e Información de Seguridad – SIEM en general, sirve como herramienta para prevenir, y reaccionar contra los ataques de origen cibernéticos, los firewall se encuentran integradas a esta herramienta como referencia se muestra en la Figura 5 **SIEM - Security Information and Event Management**, en caso ocurrencia de algún evento de seguridad se reportará al SIEM automáticamente con la posibilidad de enviar las notificaciones por correo electrónico.

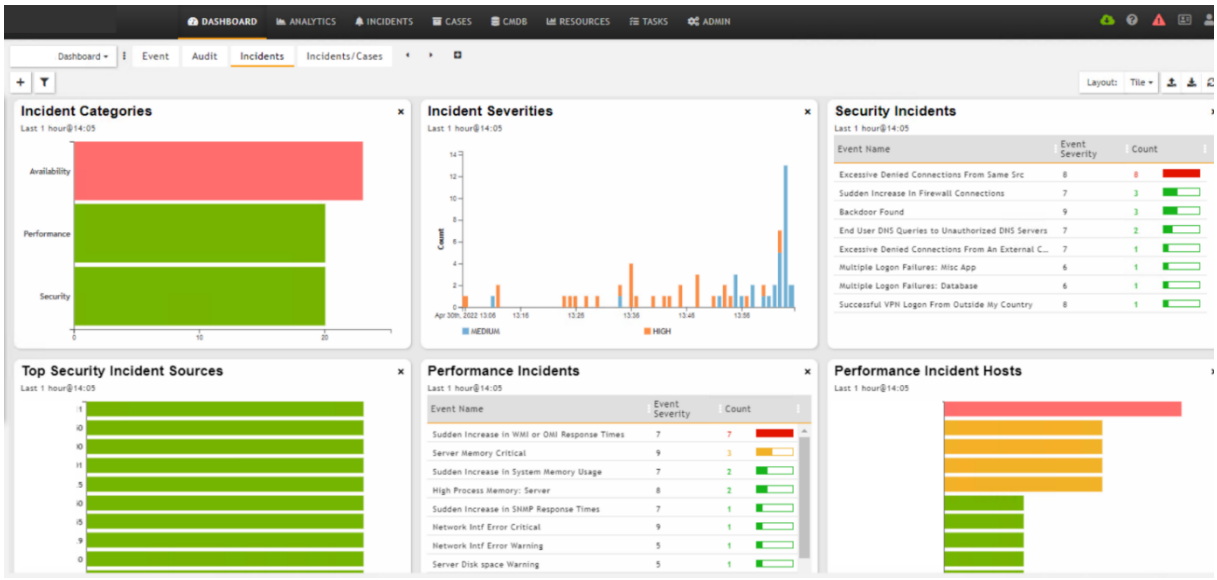

Figura 5 SIEM - Security Information and Event Management

Ningún dispositivo dentro de la red del ECCANDE tiene conexión directa a internet, por lo que todas las actualizaciones de la base de datos de firmas de los sistemas de prevención y detección de intrusos, de los antimalware, control de aplicaciones, actualizaciones generales y las definiciones de las firmas de patrones de ataques para entornos industriales se realiza con la ayuda del Sistema Gestión Centralizada y Actualizaciones – SGCA como se muestra en la **Figura *6* Sistema Gestión Centralizada y Actualizaciones – SGCA**.

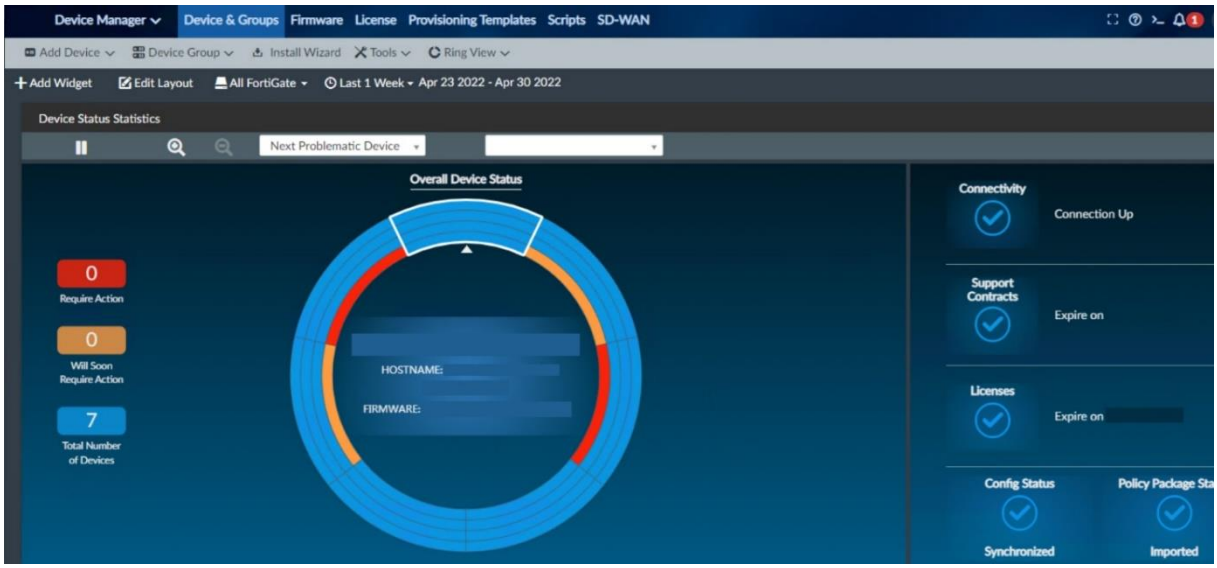

Figura 6 Sistema Gestión Centralizada y Actualizaciones – SGCA

5. CONCLUSION

En este documento se han descrito en general algunas protecciones cibernéticas implementadas para el Sistema ECCANDE, es de notar que muchas informaciones son de carácter sensible y en algunos casos confidencial, por esta razón se realizó riguroso trabajo de cuidar y no exponer información sensible que pueda comprometer la seguridad del sistema. Así mismo, se presentó la arquitectura general del sistema ECCANDE.

El ECCANDE opera en una red exclusiva y dedicada, en principio, podría parecer suficiente la protección con bloqueos simples de IP/Puertos origen-destino, sin embargo, tal protección no es suficiente, para obtener un entorno seguro de operación es necesario la implementación de varias capas de protección con las características adecuadas al tipo de arquitectura, criticidad y flujo de información.

Estas protecciones están basadas en patrones de ataques conocidos y catalogados, brevemente se ha descrito algunos ataques como; DoS, MiTM y Delay que, en caso de ser exitoso, en una operación interconectada podría tener consecuencias severas sobre el sistema eléctrico. Es necesario además considerar que existen muchos ataques del tipo "*Zero Day*" que aún no han sido reconocidas ni catalogadas, lo cual resulta sumamente importante realizar monitoreo activo en los Sistemas SMOT, SIEM y SGCA para minimizar el riesgo que un ataque de día cero pudiera ser exitoso.

Finalmente, se sugiere implementar un plan de acción para las actualizaciones de los firmwares de todos los dispositivos que conforman el sistema ECCANDE, priorizando aquellas vulnerabilidades catalogadas como severas o que pudieran tener un alto impacto negativo sobre el sistema, así mismo, es importante realizar el *hardening* o endurecimiento de todos los servidores PDCs e IHMs, dejando operativos los servicios estrictamente necesarios.

BIBLIOGRAFIA

[1] Alhelou, H. H. Wide area power systems stability, protection, and security. *Springer Nature. 2020.*

[2] CMO-PY-BR, I. A. Implatação Do Esquema De Controle De Contingências Da Ande. 2021.

[3] Barragan, A. Arquitectura Del Esquema De Control Ante Contigencias En Ande (Ecca). 2021.

[4] Diaz, C. R. *CIER*. Obtenido de https://www.cier.org/es-uy/Lists/RevistasLD/Revista%20CIER%20N%C2%B090%20v2.pdf . 2021. Pag 39-45.

[5] Matoušek, P. Description and analysis of IEC 104 Protocol. *Faculty of Information Technology, Brno University o Technology, 2017.*