Cibrelec. Red Eléctrica Cibersegura

Consorcio: S2 Grupo; Ibermatica; Electrotécnica Arteche Smart Grid, Fanox Electronic, Ingeteam Power Technology, Isotrol, Sac Maker, Ziv Grid Automation; Universidad de Sevilla, Tecnalia.

Tecnología: Industria & Consumo; Ciberseguridad

Descripción general:

Investigación en tecnologías de ciberseguridad para el despliegue de una red eléctrica más segura dotando a la red de distribución eléctrica de un mayor de seguridad lógica, ciberseguridad, para lo que es necesario:

- Incrementar el nivel de seguridad de los componentes y sistemas de información (SCADA).
- Definir una arquitectura de referencia y metodología de despliegue de seguridad en laSG
- Detectar ciberataques y evitar que tengan consecuencias, y
- Evaluar el nivel de seguridad de la propia red eléctrica.

Los objetivos tecnológicos del proyecto son:

- Definición de una arquitectura de referencia y de una metodología de despliegue de la ciberseguridad en el sector eléctrico
- Evaluación del nivel de seguridad de la red en tiempo real
- Diseño de algoritmos de detección de ciberataques
- Diseño de algoritmos de defensa ante ataques de los componentes y sistemas
- Nuevas soluciones que permitan proteger los sistemas y protocolos legados

Programa: CIEN (IDI-20170945)

Duración: 48 meses (2017 – 2021)

Presupuesto Grupo Ayesa: 800.748,00 €

Este proyecto ha sido objeto de ayuda con cargo al Ministerio de Economía, Industria y Competitividad

Cibrelec. Red Eléctrica Cibersegura

Consorcio: S2 Grupo; Ibermatica; Electrotécnica Arteche Smart Grid, Fanox Electronic, Ingeteam Power Technology, Isotrol, Sac Maker, Ziv Grid Automation; Universidad de Sevilla, Tecnalia.

Tecnología: Industria & Consumo; Ciberseguridad

Rol de Ayesa:

Ibermática desempeña un papel relevante en el proyecto, centrando su contribución en el desarrollo de soluciones avanzadas de ciberseguridad para redes eléctricas inteligentes y entornos industriales críticos. Su objetivo principal es generar conocimiento y tecnología que le permita ampliar su oferta hacia la monitorización, detección y protección frente a ciberataques en sistemas distribuidos.

En las primeras fases, participa en el análisis de requisitos de seguridad y en el estudio de vulnerabilidades existentes, aportando su experiencia en ciberseguridad aplicada a redes y sistemas industriales. También contribuye al diseño de la arquitectura de seguridad y al desarrollo de metodologías y herramientas para evaluar el nivel de seguridad de las infraestructuras en tiempo real.

Una de sus principales líneas de trabajo se centra en la detección de ciberataques, tanto conocidos como desconocidos. Para ello, participa en el procesamiento masivo de datos en tiempo real y en el desarrollo de algoritmos de análisis basados en machine learning, orientados a identificar patrones de ataque y detectar comportamientos anómalos en la red eléctrica.

Además, Ibermática investiga tecnologías criptográficas adaptadas a entornos con limitaciones de recursos, abordando aspectos como autenticación, confidencialidad, gestión de claves y comunicaciones seguras en arquitecturas distribuidas.

Finalmente, participa en las actividades de prototipado y validación experimental, evaluando las soluciones desarrolladas en entornos representativos y contribuyendo a su mejora. En conjunto, su papel es clave para garantizar soluciones de ciberseguridad robustas, escalables y aplicables a infraestructuras críticas.