RESUMEN

Titulo: Plataforma para emulación ciber-física distribuida de redes eléctricas inteligentes
Código del Proyecto: EQM250011
Investigador Responsable: Juan Gómez Quintero

La plataforma para emulación ciber-física distribuida de redes eléctricas inteligentes es una plataforma de alta fidelidad para investigación orientada al fortalecimiento de la resiliencia y ciberseguridad en redes eléctricas actuales y su transición hacia redes eléctricas inteligentes distribuidas Esta plataforma permite, por medio de hardware de electrónica de potencia, la emulación a escala de redes eléctricas de potencia y su integración computacional con redes de comunicaciones bajo esquemas de control distribuido. Esta plataforma combina software reconocido por la industria y la academia (Artemis, RT-Lab y EXata CPS), con hardware desarrollado para simulación en tiempo real, permitiendo replicar escenarios de operación, perturbación y falla de redes de distribución, así como también eventos de perturbación, falla o ataque a las redes de comunicaciones necesarias para la operación de esquemas de control distribuido utilizados en las redes eléctricas de última generación. La configuración seleccionada para esta plataforma permite el rápido prototipado de controladores distribuidos y su validación experimental a escala en escenarios ciberfísicos realistas y escalables. El hardware y software que componen la plataforma provienen de OPAL-RT (computador de tiempo real y amplificador de potencia) y Keysight (simulador de comunicaciones EXata). Esta última herramienta ha sido validada para simulación de ciber-ataques tipo Denial of Service, Man-in-the-middle, Packet modification, y propagación de malware, permitiendo escenarios de evaluación compatibles con los lineamientos de la normativa NERC-CIP escogido como Estándar de Ciberseguridad del Sistema Eléctrico Nacional (SEN). Gracias a sus capacidades de integración, simulación en tiempo real, y análisis detallado de la interoperabilidad entre elementos distribuidos, esta plataforma será clave para: i) Analizar y replicar perturbaciones eléctricas o de comunicaciones que pongan en riesgo la operación y seguridad de redes eléctricas que se encuentren en periodo de modernización. ii) Evaluar el cumplimiento técnico de estándares de ciberseguridad requeridos en la regulación nacional, incluyendo la capacitación de personal. iii) Diseñar estrategias de detección y respuesta que fortalezcan la resiliencia y robustez operativa de las redes eléctricas inteligentes.