Exceptional service in the national interest

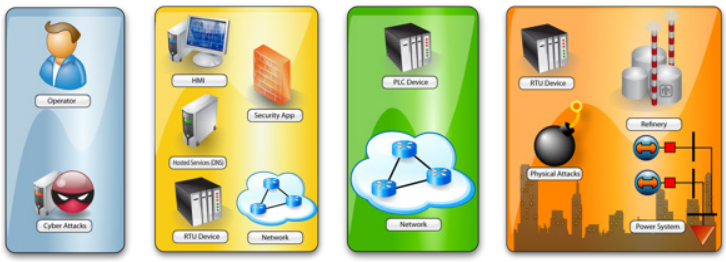
Sandia National Laboratories

SCEPTRE

SCEPTRE provides a cyber-physical environment to analyze how cyber-initiated events affect the physical world.

Sandia Capabilities

SCEPTRE is an application that uses an underlying network emulation and analytics platform (EmulyticsTM) to model, simulate, emulate, test, and validate control system security and process simulations. Traditionally, tools and techniques for simulating and emulating control system field devices have been limited because



Human Live Emulated Simulated

the physical processes being controlled are omitted. SCEPTRE leverages proven technologies and techniques to integrate the device and process simulations, with control hardware in the loop, providing an integrated system capable of representing realistic responses in a physical process as events occur in the control system and vice versa. SCEPTRE is a proven control system environment platform, having been fielded for many R&D applications, operational joint tests, and exercises supporting testing, training, validation, and mission rehearsal.

Modeling & Simulation

SCEPTRE is comprised of simulated control system devices, such as remote terminal units (RTUs), programmable logic controllers (PLCs), protection relays, and simulated processes, such as electric power transmission systems, refinery processes, and pipelines. The simulated control system devices are capable of communicating over Internet Protocol (IP) networks using standard Industrial Control Systems (ICS) protocols such as Modbus, DNP3, IEC 61850, and others.

SCEPTRE also includes support for hardware-in-the-loop, wherein real field devices under study (i.e. a specific model of PLC) can be connected to and interact with the physical process being simulated. This allows the user to include high fidelity systems where they are needed without sacrificing scalability.

Security Analysis

SCEPTRE provides an analysis capability for assessing and improving the cyber security of control systems used in the energy sector. SCEPTRE provides an environment where hardware and software upgrades and new mitigations can be evaluated before installation in an operational environment.

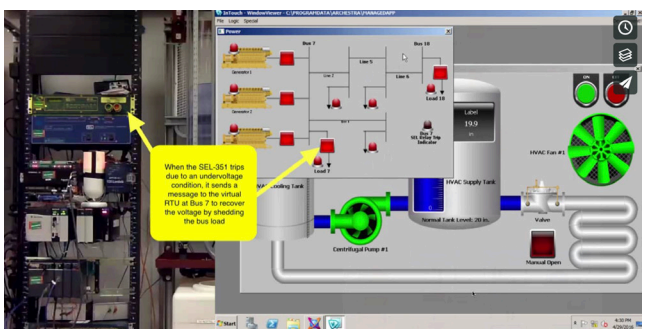
SCEPTRE Components:

- Control Systems devices.
- High fidelity Industrial Control Systems (ICS) protocols enabling technology that allows communication between real and simulated devices.
- Process simulation leveraging industry standard software.

Benefits:

- Create large-scale control system test environments suitable for cyber security experiments.
- Leverages modeling, simulation, and test bedding techniques to deploy scalable experiments in a more cost effective way than real or lab-scale tests.
- Use of standards-based ICS means 3rd party ICS and cyber security testing applications can be used and supports emulated network environments.

For more information contact:
Derek Hart | Ph: (505) 284-8880
Email: derhart@sandia.gov



SCEPTRE Online Demo: https://vimeo.com/178492617

SCEPTRE Use Case: Cyber Threat Analysis of the California Electric Grid

US Energy infrastructure is reliant on advanced control systems that are complex and increasingly connected to the internet. Protection is difficult and must consider new vulnerabilities and potential attacks. Sandia created the Integrated Cyber Physical Impact Analysis (ICPIA) Framework to address the problem. ICPIA integrates an array of modeling and simulation capabilities to manage this risk and secure our control systems. Use cases include:

- Support New Threat Analysis - Explore the impact of previously unidentified threats and vulnerabilities
- Provide test bed for integrating systems - an Intrusion Detection System (IDS) can be installed and tested in the network emulation
- Help design secure architectures – evaluating protective measures (detection, deter, respond) such as encryption
- Act as a training tool - for Red Team attackers or for Plant Operators to develop cyber attack response procedures
- Identify R&D gaps – for modeling and simulation improvements
- Supports integrated risk management - attack difficulty metrics, impact and consequence analysis, moving to "all hazards" analysis

Electric Power Transmission Disruption Demonstration

Goal: Demonstrate use of SCEPTRE within the ICPIA framework to analyze a hypothetical cyber attack scenario for a large-scale electric power disruption.

Drawing upon our experience in vulnerability analysis and our multi-disciplinary cyber and physical capabilities, Sandia has developed the ability to emulate control networks of large scale power systems. This demonstration draws upon those capabilities, utilizing the ICPIA framework, to analyze a hypothetical cyber attack targeting the disruption of power generation and transmission in the Western Electricity Coordinating Council (WECC).

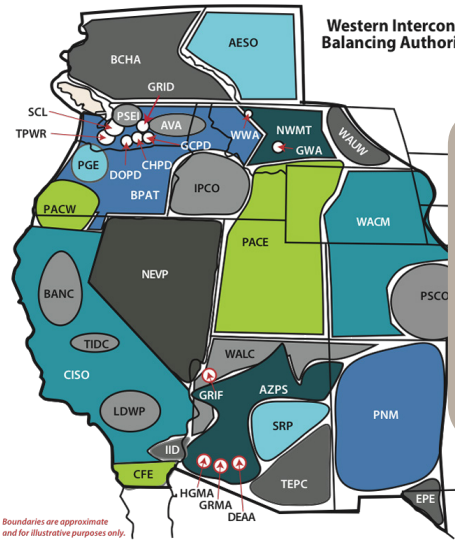
Integrated Cyber Physical Impact Analysis (ICPIA)™

Full Spectrum Modeling Framework

Next Steps Needed to Achieve Capability Maturity

Vet the hypothetical disruption scenario with electric utilities and identify a suite of additional scenarios of interest to the electricity sector. Areas of focused capability development include:

- evaluate emerging attack technologies,
- integrate analysis from different domains across the framework,
- methodologies to identify resilient systems, and
- automate analysis to support multiple scenarios.



WECC Base Case Analyzed: Heavy Summer 2014

- Load: 170,000 MW
- Area: nearly 1.8M sq mi
- Generators: 3,850
- Buses: 19,500

Elements of Cyber Attack and Cascading Consequences

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-8095 08/16

Sandia National Laboratories