SCEPTRE
scada-as-a-platform

Sandia National Laboratories

SCEPTRE provides a cyber-physical environment to analyze how cyber-initiated events affect the physical world. SCEPTRE uses an underlying network emulation and analytics platform 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 the physical processes being monitored and controlled are omitted. SCEPTRE leverages proven technologies and techniques to integrate the end device and process simulations, with control hardware-in-the-loop (HIL), 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 AND 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 Supervisory Control and Data Acquisition (SCADA) protocols such as Modbus, DNP3, IEC 61850, and others.
SCEPTRE also includes support for HIL, 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 and DoD. SCEPTRE provides an environment where hardware and software upgrades and new mitigations can be evaluated before installation in an operational environment.

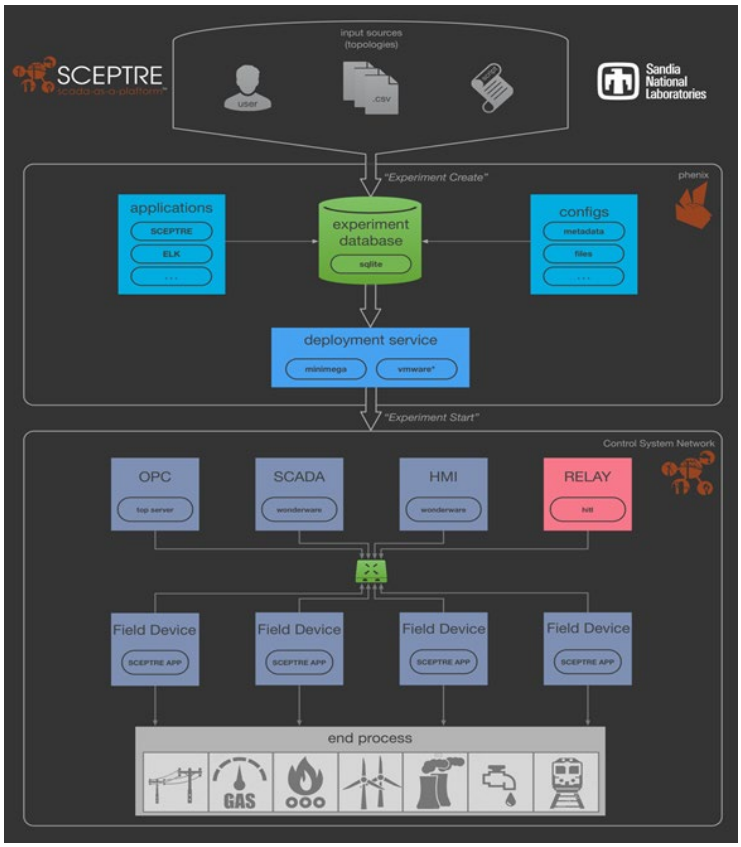
Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2019-11907 M

SCEPTRE COMPONENTS

- Virtual and physical control system devices
- Software defined networking with SCADA protocols written to specification
- Real-time end-process simulations leveraging industry standard software
- Integrated COTS SCADA applications

BENEFITS

- Quickly deploy and tear down large-scale control system 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 solutions
- Use of standards-based SCADA means 3rd party ICS and cyber security testing applications can be used
- phēnix orchestration tool and GUI allows users to easily manage many deployed experiments at once



SCEPTRE combines control system devices and physical process simulations in an integrated system that represents realistic responses in the physical process as cyber events occur.