SAND2016-4768PE

Exceptional service in the national interest

Sandia National Laboratories

SCEPTRE Overview for Workshop 2016

Derek H. Hart

Casey Glatter

Jordan Henry

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. SAND NO. 2011-XXXXP

Why does SCEPTRE exist?

Sandia National Laboratories

- Live system testing is impractical
  - Potential damage to the real system and dangers to human life
- Traditional test beds are burdensome
  - Expensive to build, maintain, configure, and operate
- Lab-scale hardware testing setups are insufficient
  - Effective at testing devices in isolation, but detrimental effects might only be seen in the context of a larger, networked system
- Network simulation
  - Mapping network events to physical process effects is difficult
- **SCEPTRE provides a cyber-physical interface to show how cyber-initiated events affect the physical world (and vice versa)**

SCEPTRE Components

Sandia National Laboratories

- Control Systems devices
  - Low fidelity simulated ICS devices
    - RTUs, PLCs, protection relays, FEPs
  - Emulated PLCs, HMI services
  - Real hardware relays, PLCs, RTUs
- High fidelity SCADA protocols
  - ModbusTCP, DNP3, iec61850
  - Written to specification
  - Enabling technology that allows communication between real and simulated devices
- Process simulation
  - Leverage industry standard software where possible (V&V)
    - PowerWorld, PyPower, PSS/E
  - Develop our own simulated process when needed
    - Water treatment, refinery, natural gas pipeline, railroad signaling

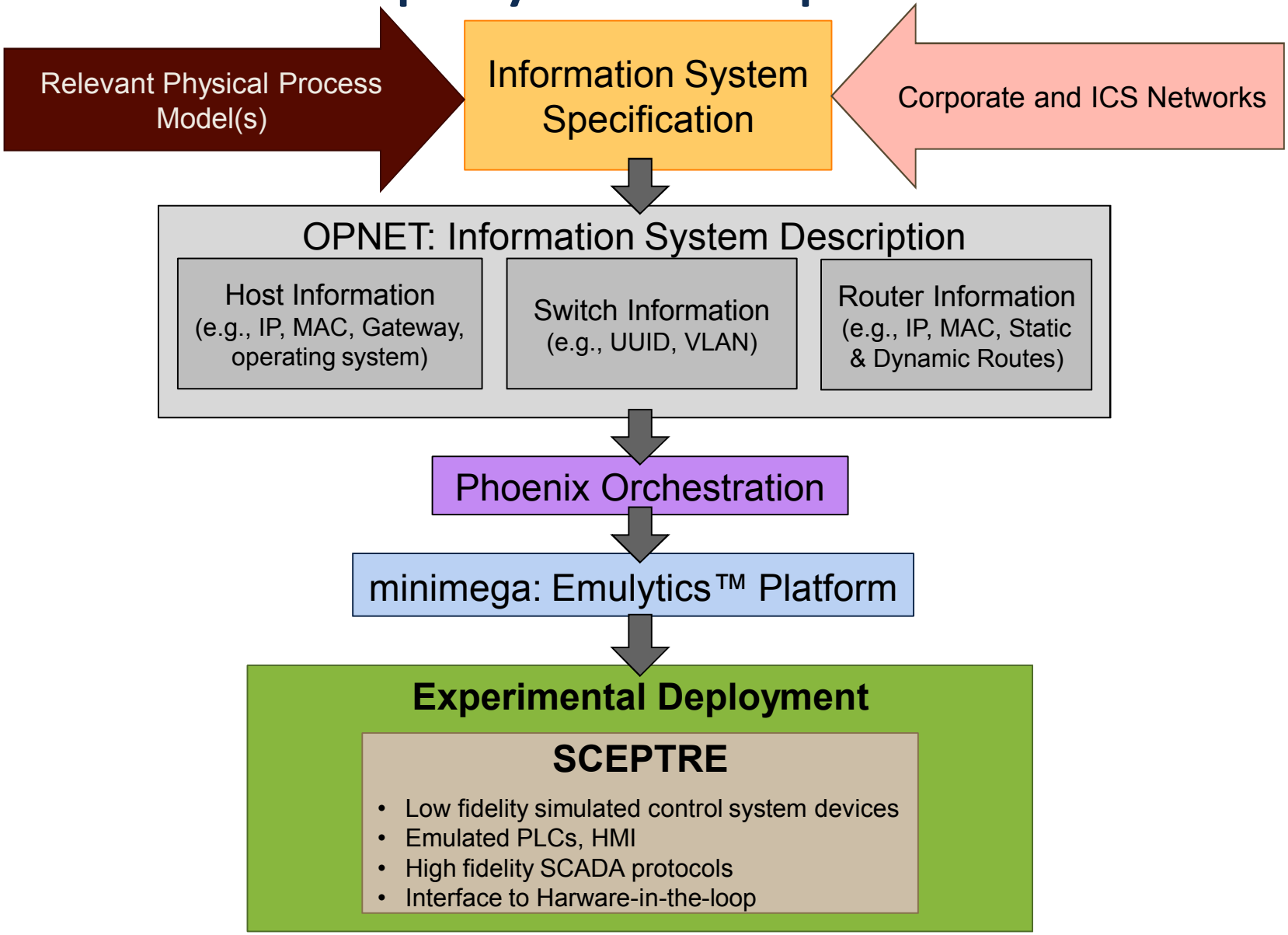
SCEPTRE Operational Overview

Sandia National Laboratories

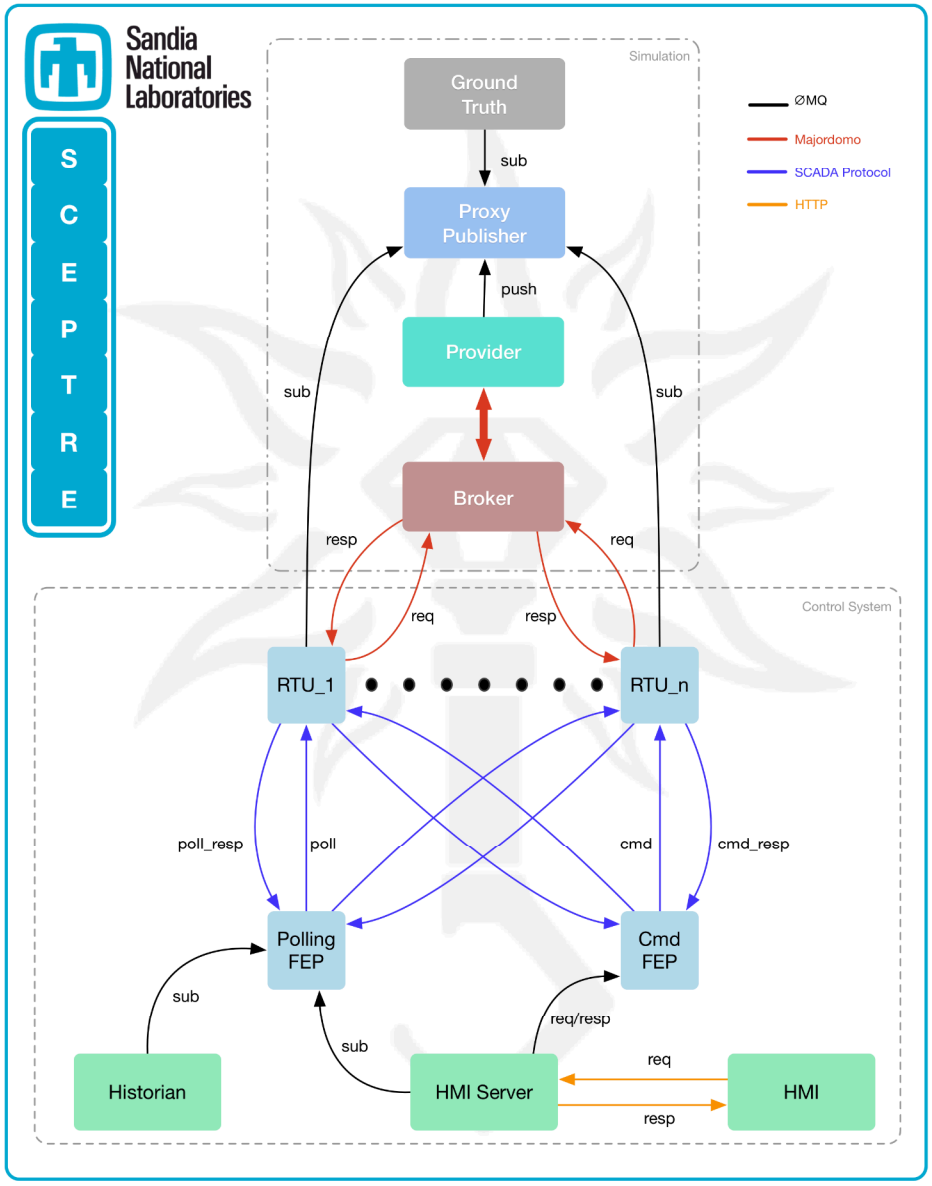
- SCEPTRE is an application that uses an underlying network (like Sandia's Emulytics™ Platform technology) to run
- ICS devices (simulated, emulated, real) communicate and interact via high fidelity SCADA protocols
- Process simulation data is provided to all the ICS devices
- All ICS devices are able to interact with the simulation, providing both updates and subscribing to the current state of the simulation
- When the simulation state updates, all devices receive the current state so there is a common view of the simulation
- Overall simulation is able to bridge multiple infrastructures into the same experiment to show interdependencies.
- Real-time vs discrete event simulations

SCEPTRE Deployment Pipeline

Sandia National Laboratories



SCEPTRE Functional Structure



SCEPTRE Use Cases

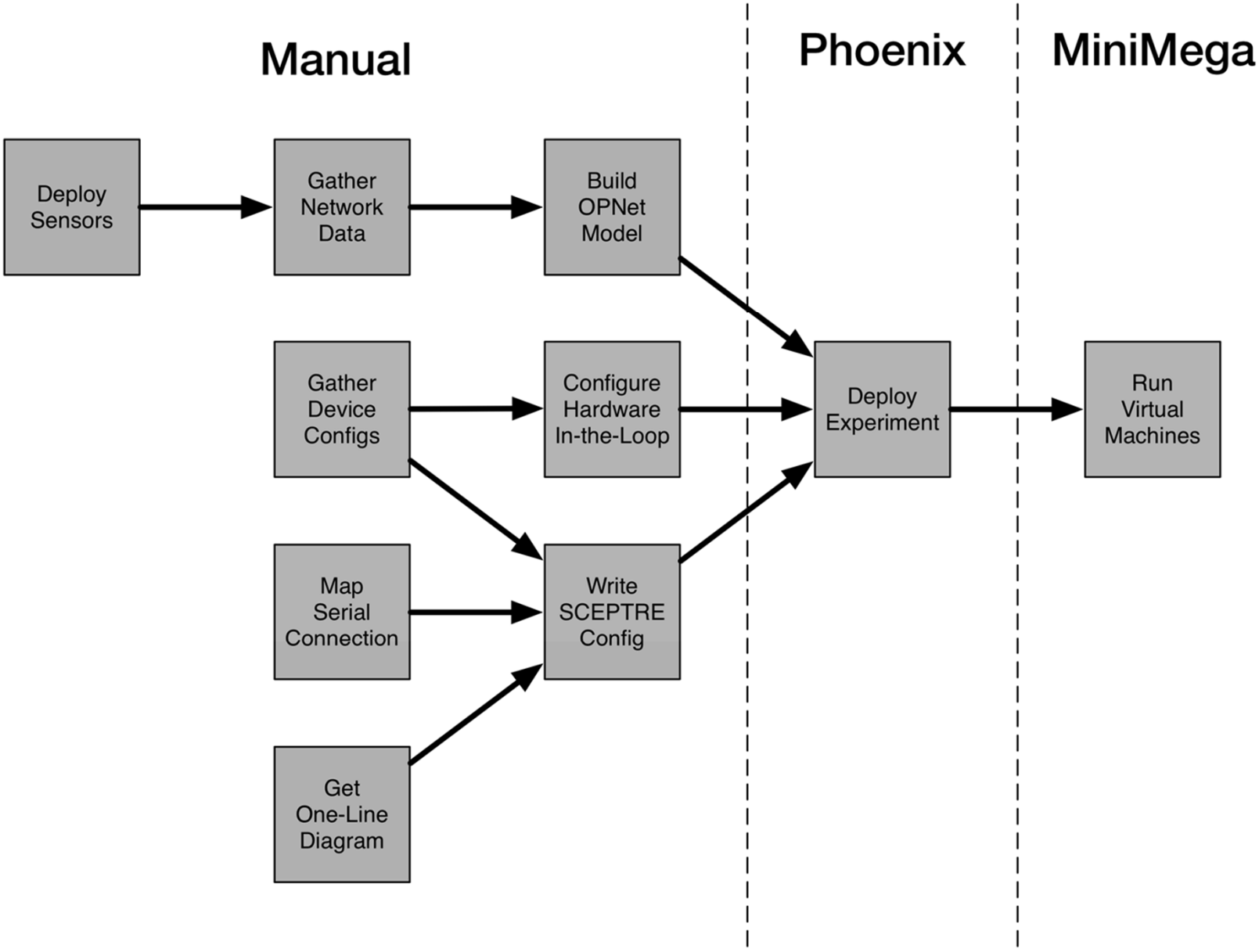
Sandia National Laboratories

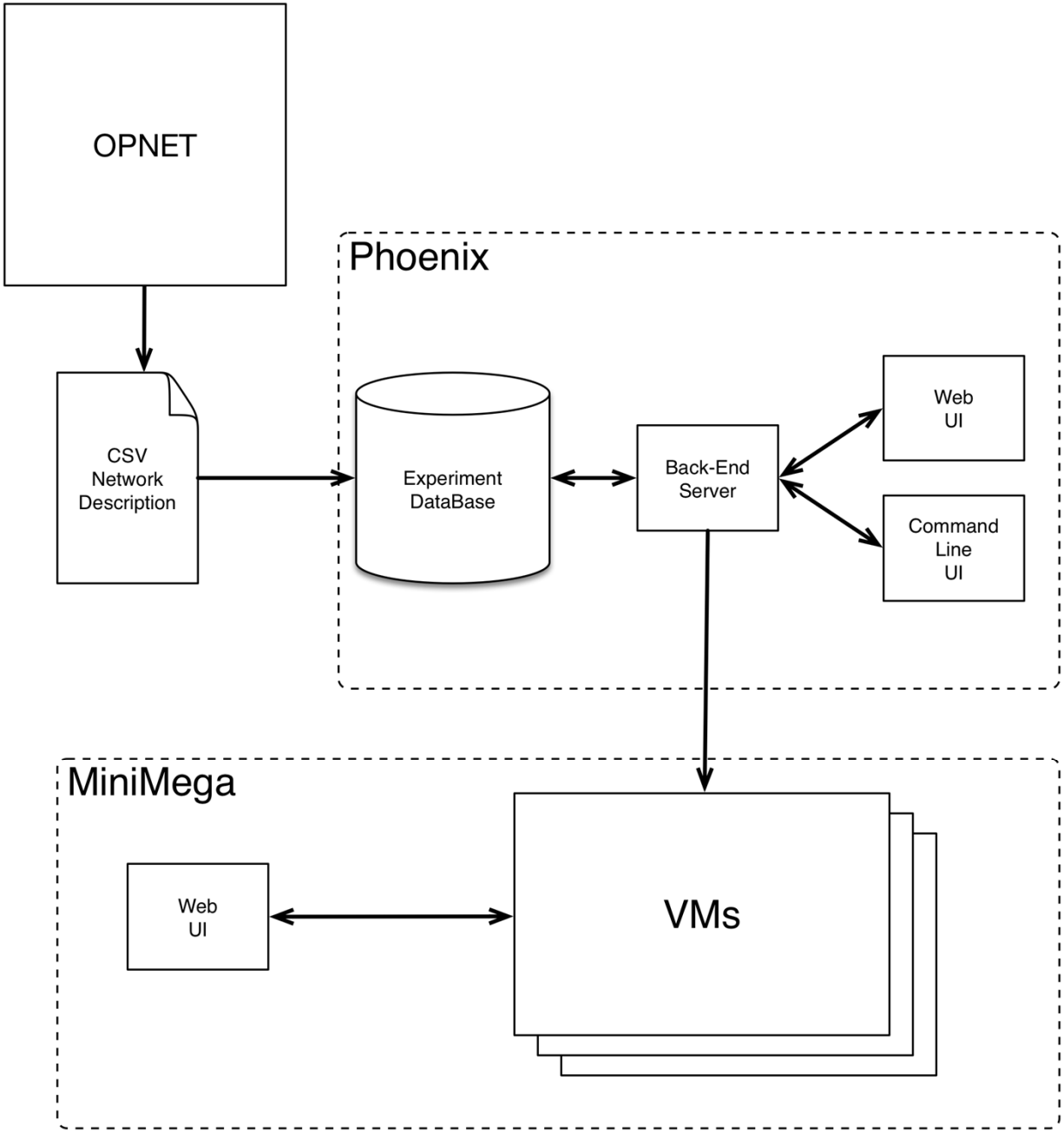
- Test and Evaluation
  - Hardware, architectures, TTP, technology solutions
  - Vary model fidelity depending on the questions being asked and scope
- Analysis
  - Deploy network of interest to understand vulnerabilities and exploitable avenues
  - Identify critical components on the control network and in the underlying infrastructure
  - Ability to model infrastructure interdependencies within the same simulation

SCEPTRE Use Cases (cont.)

Sandia National Laboratories

- Training and Exercise Support
  - Look-and-feel of real ICS networks by integrating industry HMI and service tools
  - Faithful protocol traffic for deeper network inspection
  - Ties to process models illustrate impacts of control system changes on physical systems
  - Provided SCEPTRE environments to support DoD exercises


Manual
Phoenix
MiniMega
Deploy Sensors
Gather Network Data
Build OPNet Model
Gather Device Configs
Configure Hardware In-the-Loop
Deploy Experiment
Run Virtual Machines
Map Serial Connection
Write SCEPTRE Config
Get One-Line Diagram


OPNET
Phoenix
CSV
Network
Description
Experiment
DataBase
Back-End
Server
Web
UI
Command
Line
UI
MiniMega
Web
UI
VMs