SAND2011-4989C

Cyber Security Analysis for the Power Grid Using the Virtual Control Systems Environment

IEEE PES GM2011

27 July 2011

Jason Stamp, Ph.D.

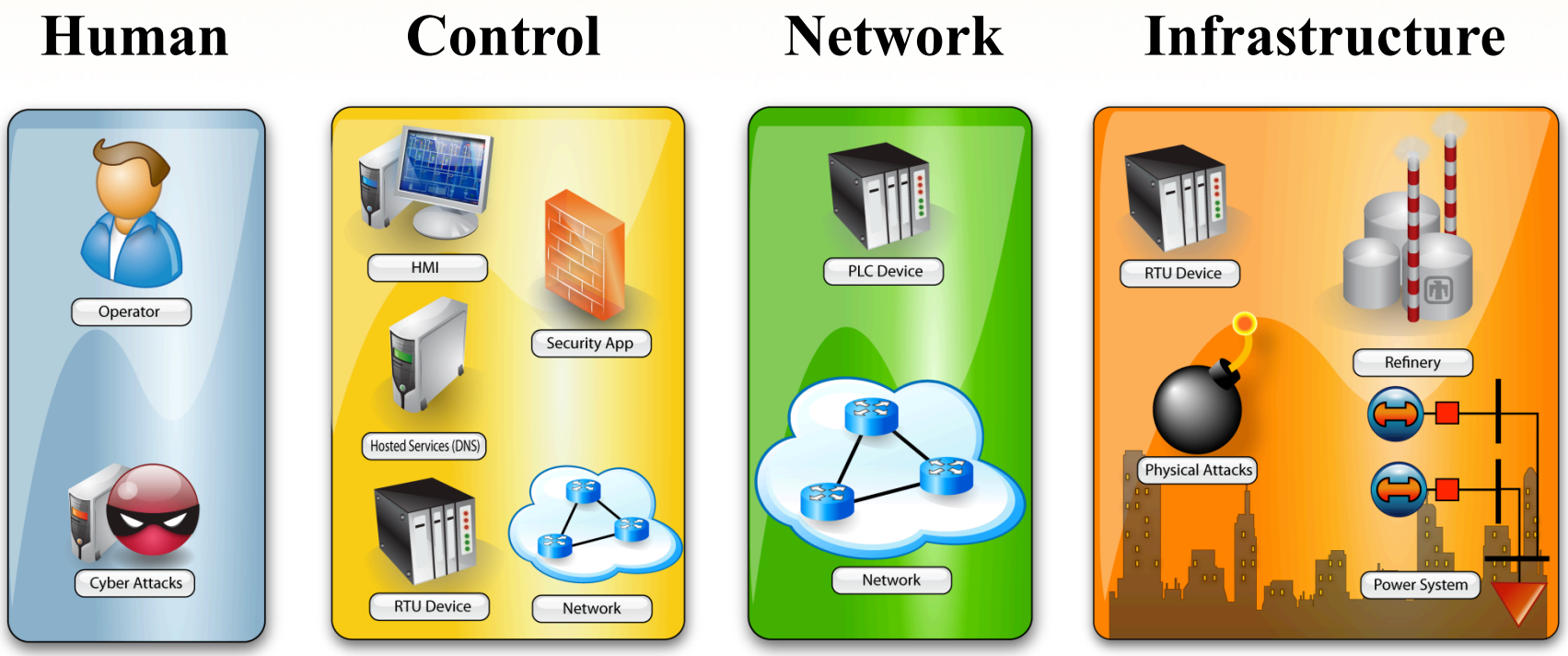
Sandia National Laboratories

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.

Part of an Integrated Risk Analysis Approach

Sandia National Laboratories

Cyber-Physical System Domains



Sandia National Laboratories

Cyber-Physical Systems Analysis

Goal: Understand how cyber issues affect physical systems

Options	Complications
Live system testing	Severely impacts service
Testbed systems	Testbeds are expensive to build, maintain, reconfigure, and operate; repeatability is a concern
Laboratory scale systems investigating isolation subsytems	Some issues are only exposed in larger context
Modeling and simulation	Problems with performance, fidelity, and veracity

Heterogeneous Systems Simulation

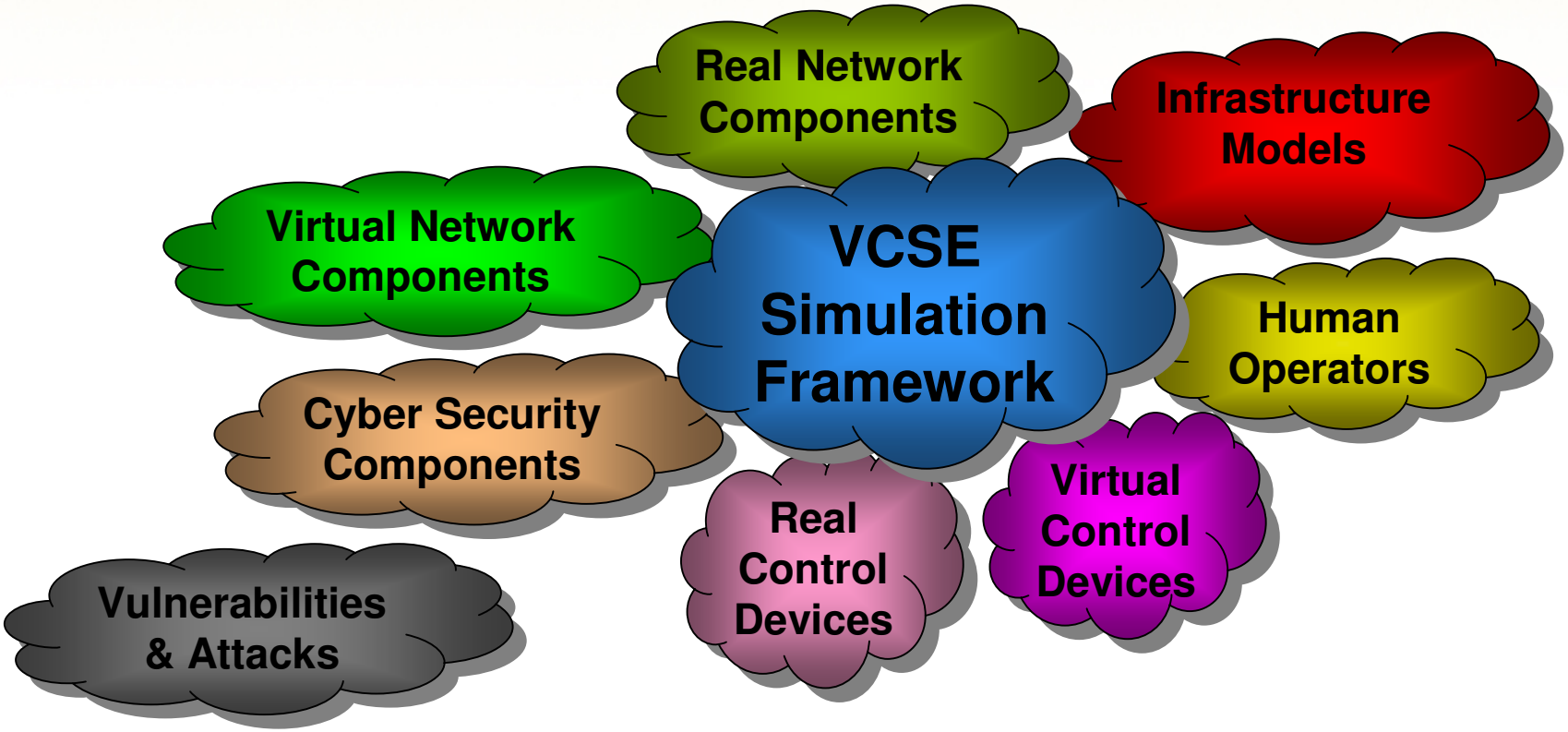
- **Three levels of abstraction:**
  - **Simulated (most abstraction)**
  - **Emulated/virtual (partial abstraction)**
  - **Physical (no abstraction)**
- **Benefits:**
  - **Lower cost (in time and equipment)**
  - **Flexibility (rapidly reconfigure)**
  - **Replication (experimental repeatability)**
  - **Variable fidelity (system- and network-under-test)**

Virtual Control Systems Environment (VCSE) Existing or Near-term Technologies

Domain	Physical	Emulated	Simulated
Control	PLC, SCADA, relays, historian…	Virtual SCADA server; Soft PLC; VMWare ESXi, virtual historian…	RTU model, relay model, simulated ladder logic…
Network	Cables, firewalls, routers, NIDS…	DynaMIPS (CISCO router); QEMU…	OPNET (SITL), routing model, wireless channel model…
Power Grid	(1)	N/A	Solar/wind models, SimPowerSystems, load flow software…

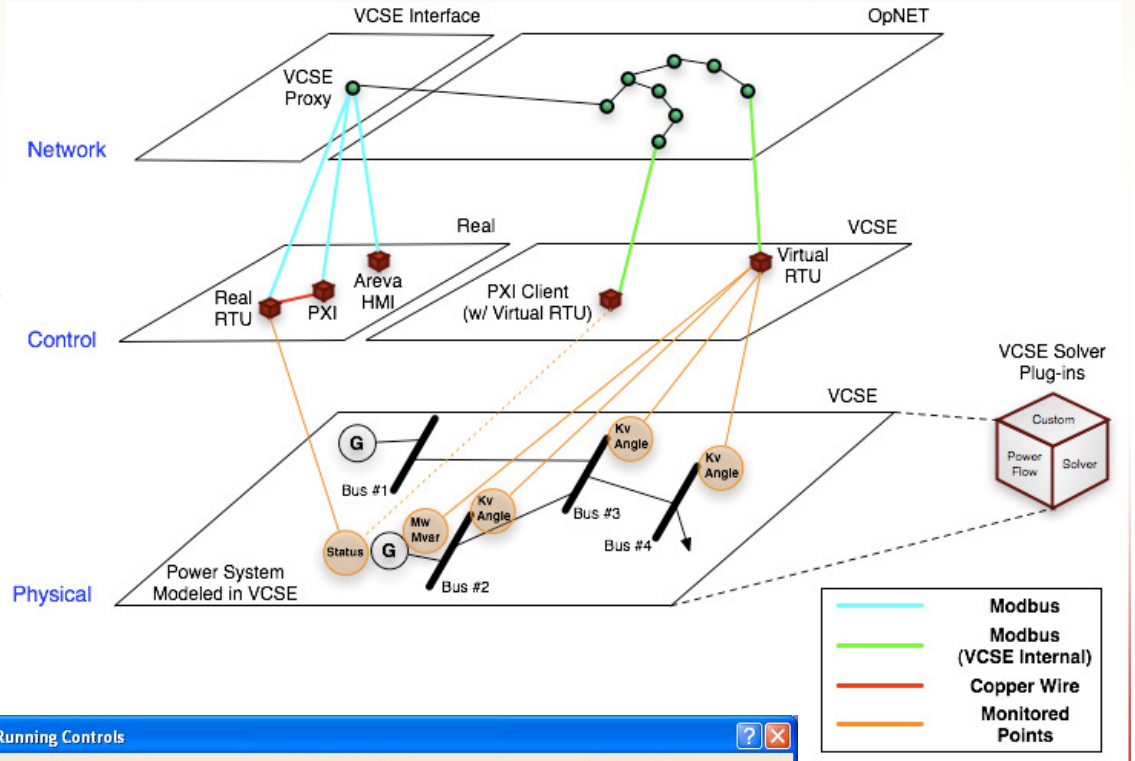
(1) Not yet integrated with VCSE, may include diesel generators, PV system, breakers, batteries…

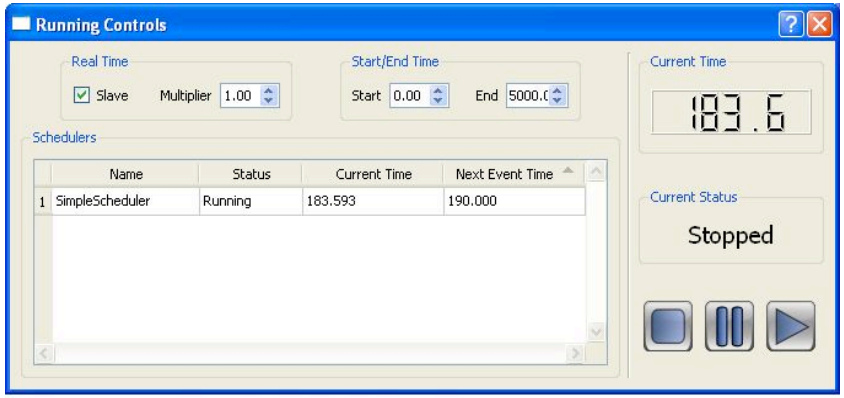
VCSE Primary Components



UMBRA™ as the VCSE Simulation Framework

- Flexible simulation engine and framework
- Directed graph approach
- Integrates physical, cyber, and behavioral elements at variable fidelity in a 3D environment
- Regularly works the range of S-E-P environments
- C++ modules
- Scripting interface
- XML configuration





Sandia National Laboratories

Cyber Testing (VCSE) Use Cases

- **Effects – What are the likely effects on the physical infrastructure from a postulated attack scenario?**
- **Usability – How difficult is it to install and maintain cyber security controls?**
- **Performance – How well do cyber controls function against various attack scenarios?**
- **Transparency – Do cyber security controls negatively affect system performance?**
- **Training – Help operators recognize cyber attacks, and prep cyber assessment teams to work in control system environments**

- **Each experiment will tend toward differentiated SEP architectures depending on the SUT and NUT designations**

VCSE Used in Cyber Security Analysis Process

Initial Experiment or Architecture Set

Development of broad issues applicable to data and functionality for the selected analysis topic.

VCSE Analysis Phase

Formulate experiments to gain necessary insight. Interim results may be complete, or necessitate experiments on physical grid equipment.

Physical Testbed Phase

Add physical grid equipment to testbed to improve precision, accuracy, and veracity as appropriate.

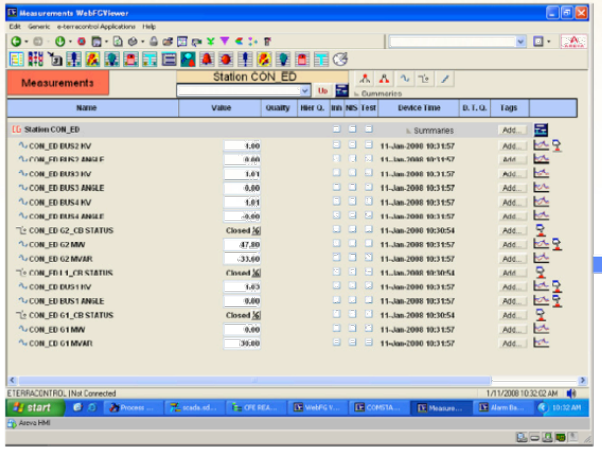
Report on the overall set of experiments.

Sandia National Laboratories

Application to Electric Power Systems

- **Four modes of control for the grid:**
  - **Protective relaying**
  - **Automated systems management**
  - **Human-in-the-loop control**
  - **Engineering configuration and management**
- **Analyses depend on careful selection of the SUT/NUT**
- **Some cases depend on SUT being physical to adequately represent the component or subsystem (e.g. control system vulnerability in its hardware)**
- **Other cases depend on the SUT being physical for to maintain the experiment's veracity**

VCSE Power Grid Model



Real Operator Control Software

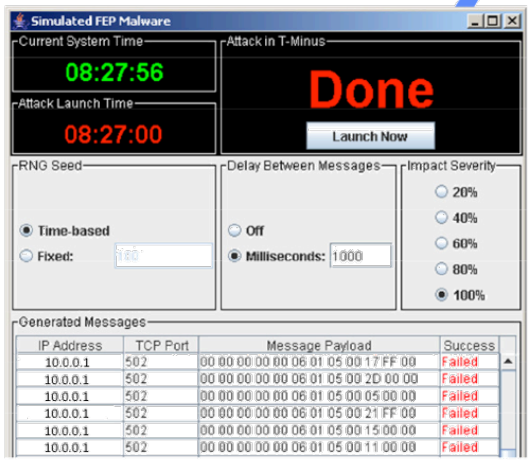
Simulated, Emulated, or Physical Networks

Ethernet

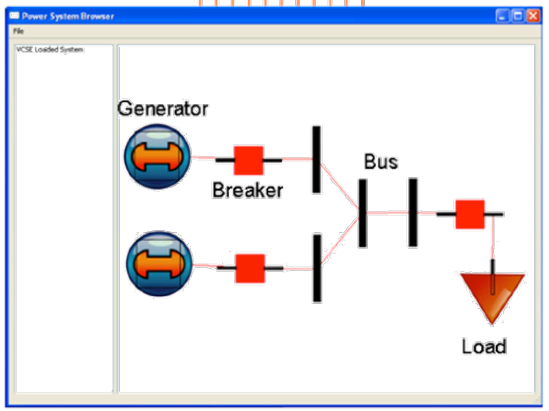
Ethernet

Ethernet Or sim interface

Simulated, Emulated and Real Control Interfaces



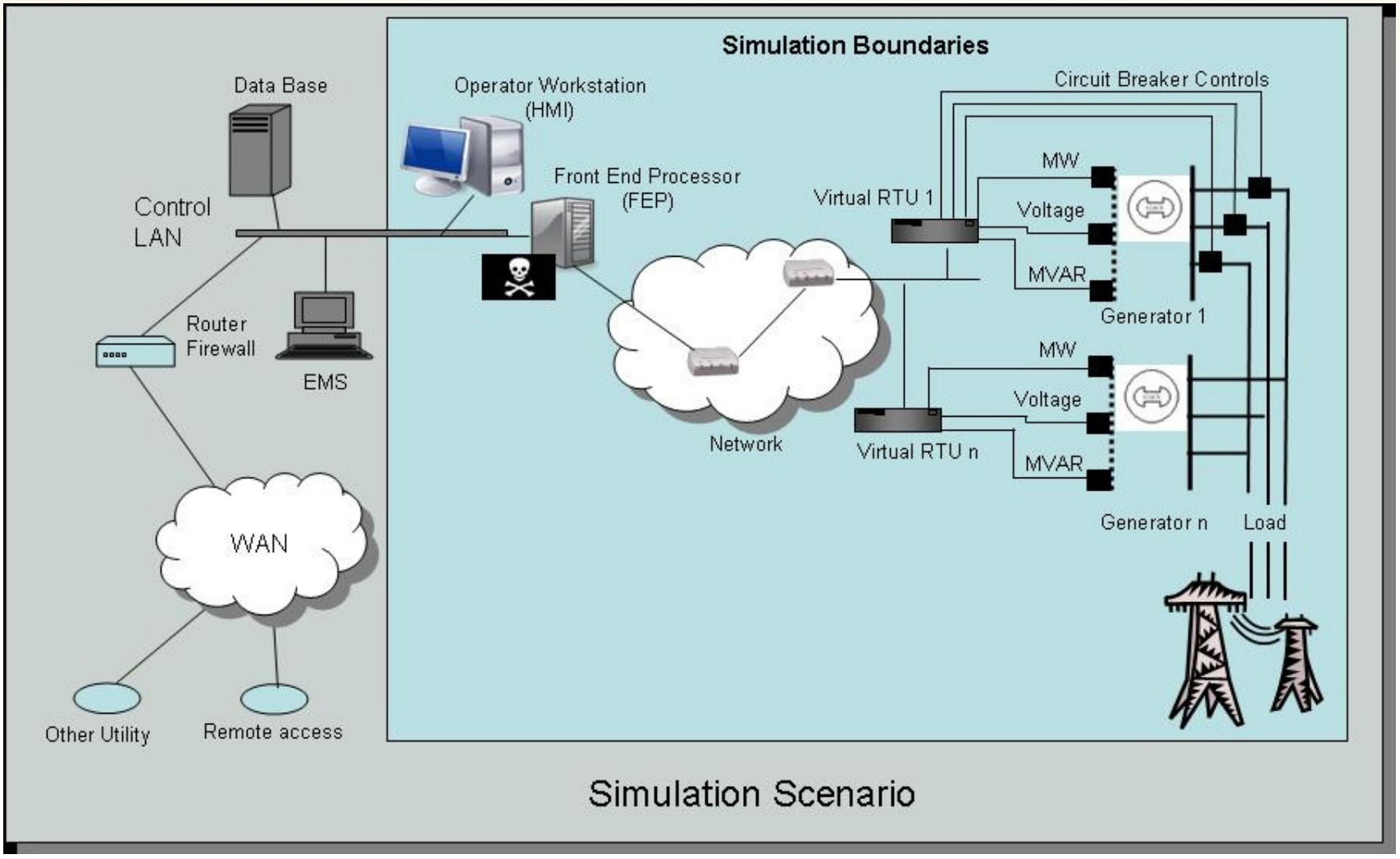
Threat Software Under Test



Simulated Power System

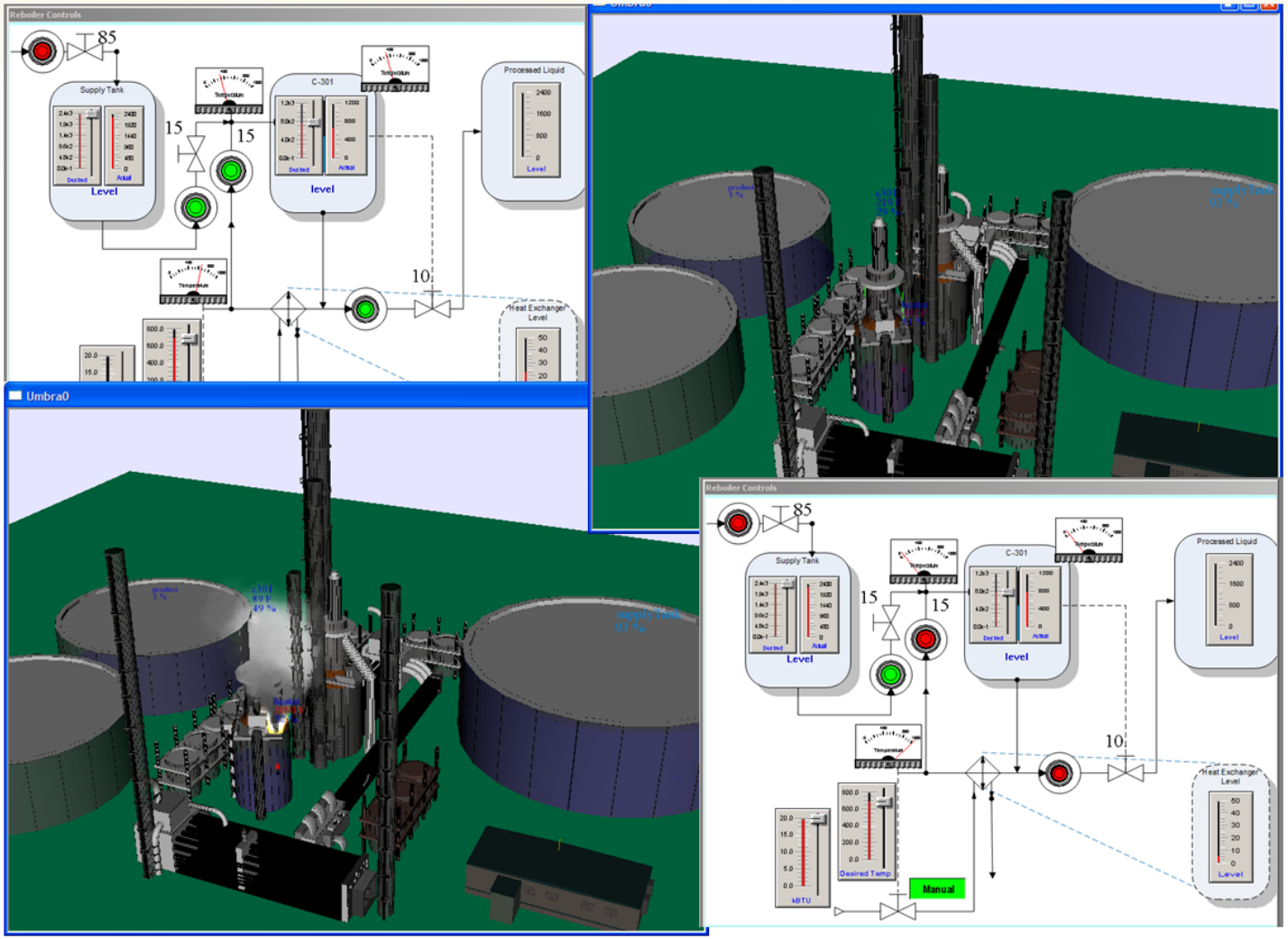
Sandia National Laboratories

VCSE Power Grid Model



Sandia National Laboratories

VCSE Refinery Model



Sandia National Laboratories

Future VCSE Work

- **Automated configuration and deployment tools for emulated/simulated components**
- **Integration of physical power system components into the testing environment**
- **Application to microgrid systems**

Author Contact Information

Jason Stamp, Ph.D.
Principal Member of the Technical Staff
Sandia National Laboratories
PO Box 5800, Albuquerque, New Mexico 87185-1108
505-284-6797, jestamp@sandia.gov

Bryan Richardson (Sandia VCSE Program Lead)
Senior Member of the Technical Staff
Sandia National Laboratories
PO Box 5800, Albuquerque, New Mexico 87185-0671
505-845-2386, btricha@sandia.gov

Vince Urias
Senior Member of the Technical Staff
Sandia National Laboratories
PO Box 5800, Albuquerque, New Mexico 87185-0933
505-284-5584, veuria@sandia.gov

Sandia National Laboratories