MILCOM'12
TRUSTED COMMUNICATIONS...AWARENESS TO ACTION
SAND2012-9419C

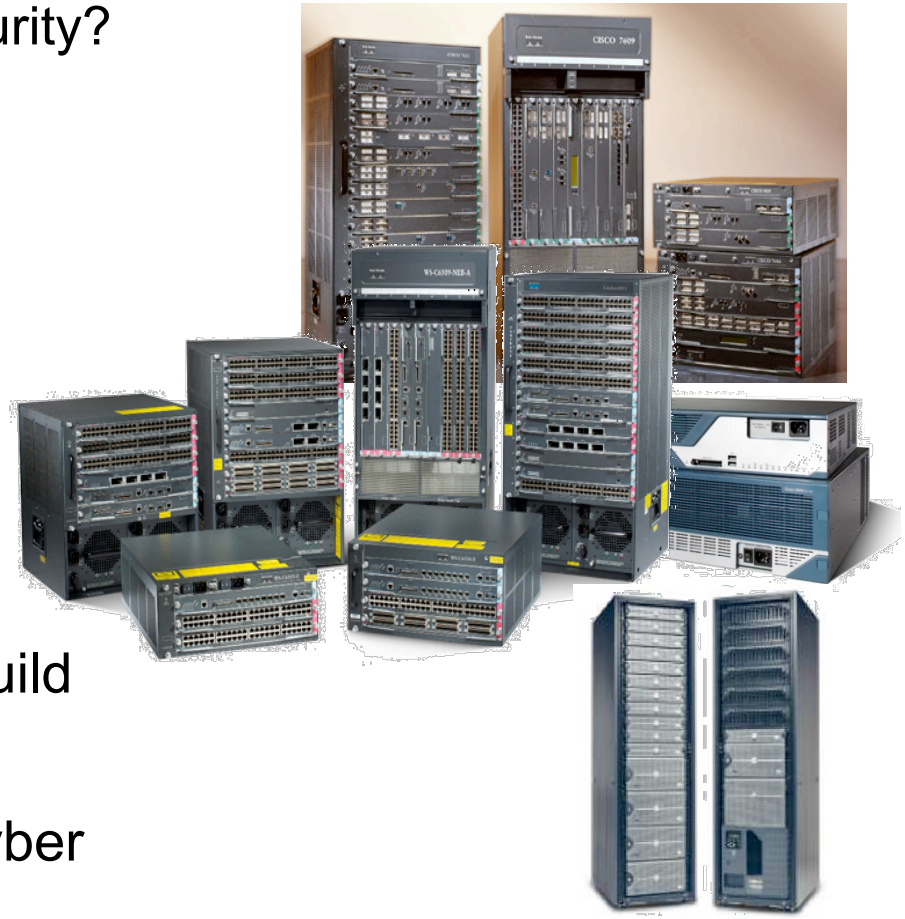
Supervisory Control and Data Acquisition (SCADA) System Cyber Security Analysis using a Live, Virtual, and Constructive (LVC) Testbed

Sandia National Laboratories
Albuquerque, NM

Testing challenges

How can I investigate SCADA system security?

- Experiment on the actual network
- Experiment on a testbed network
  - Real
  - Emulation
  - Simulation



Issues:

- In-situ testing is often forbidden
- Physical testbeds are expensive to build and operate
- It's hard to analytically model most cyber threats correctly

We suggest using a scalable, high-fidelity LVC testbed for this analysis

Cyber-physical systems analysis challenges

Understand how cyber threats operate on particular physical systems

Options	Complications
Live system testing	Can put lives/equipment in danger
Test bed systems	Test beds are expensive to build, maintain, reconfigure, and operate
Laboratory-scale systems investigating components in isolation	Some issues are only exposed in larger context
Network simulation	Mapping network attacks to physical systems is difficult

Objective

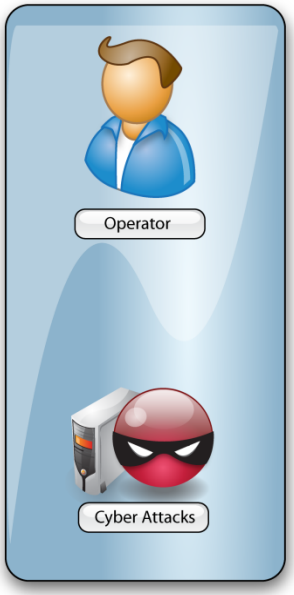
- Construct a live, virtual, and constructive environment to support cyber operations research and analysis
- Represent SCADA system and threat with sufficient fidelity, modularity, and operational confidence to assess the affects of cyber adversarial behavior

Live, Virtual, Constructive (LVC)

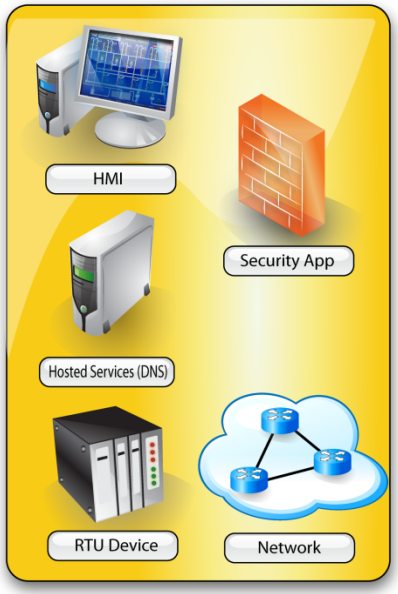
- Live – real hardware, real software
- Virtual – surrogate hardware, real software
- Constructive – surrogate hardware, modeled software

Virtual Control System Environment

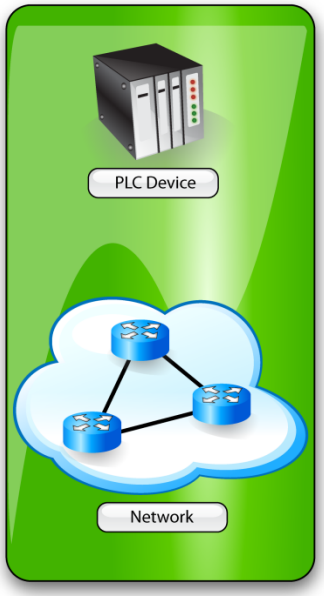
Human



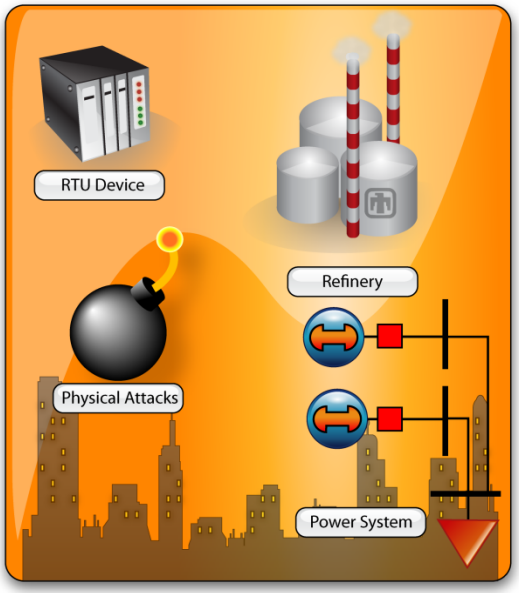
Live



Virtual



Constructive



Virtual Control System Environment

Represent control system devices using VCSE

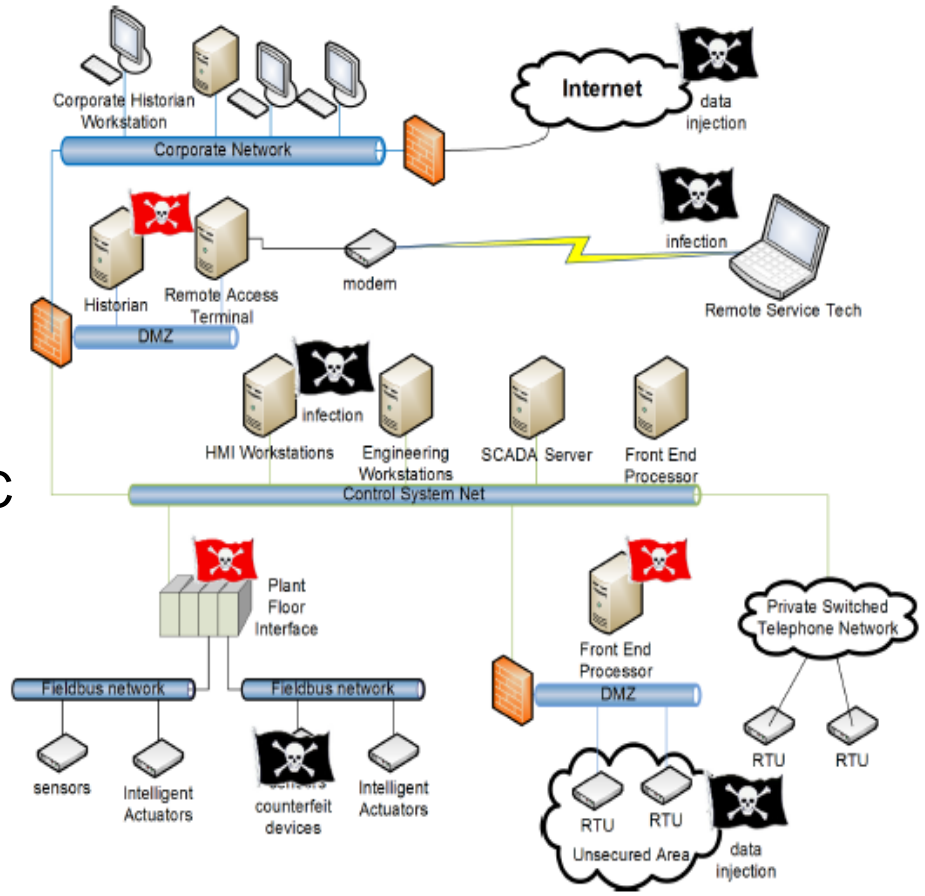
- Remote Terminal Units (RTUs)
- Programmable Logic Controllers (PLCs)
- Protection Relays

Represent control center servers/services

- Actual SCADA/EMS/DCS software running on real or virtualized hardware

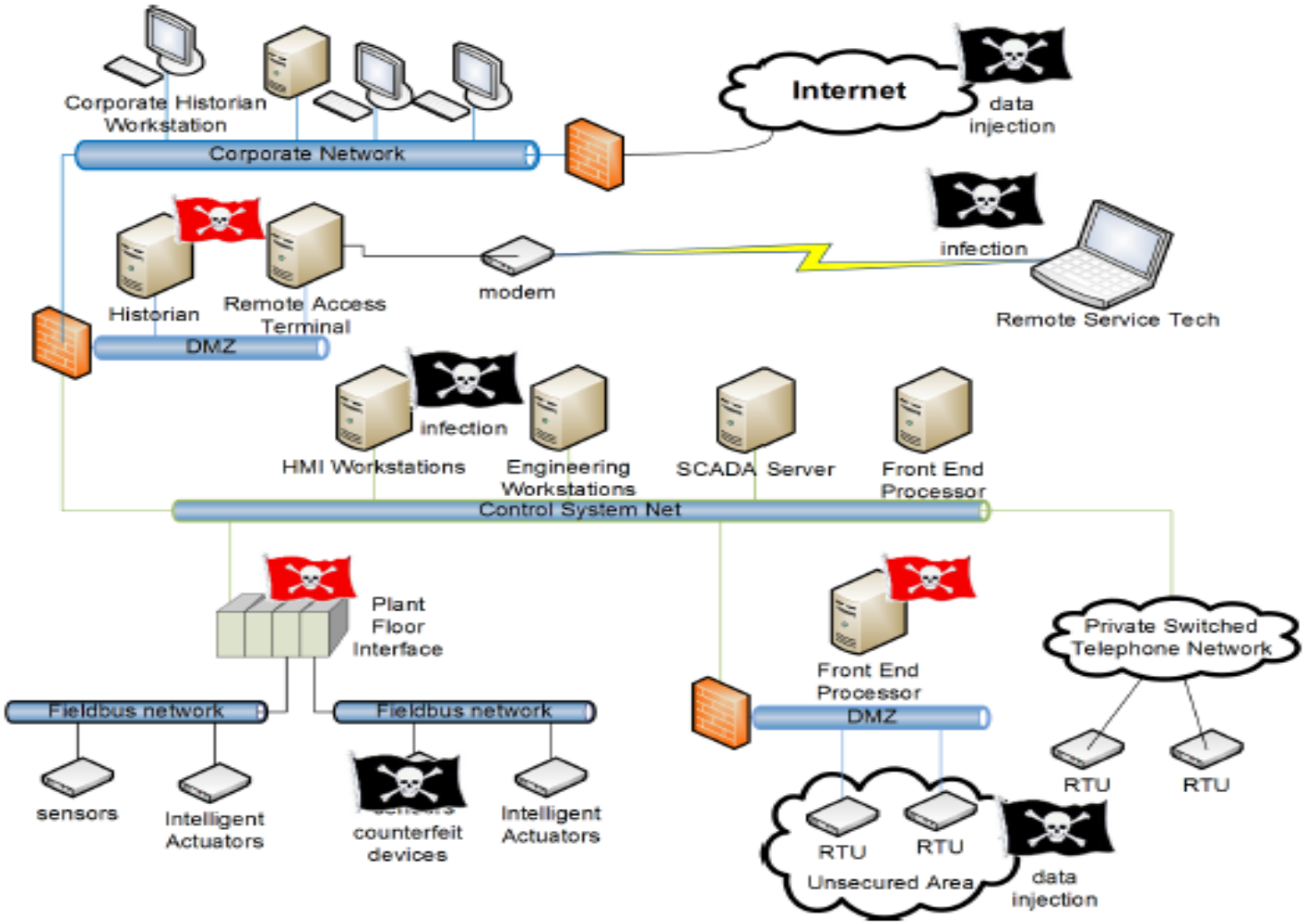
Represent communication network using LVC

- Real devices (routers, switches, etc)
- Emulated devices (Dynamips, Vyatta, etc)
- Simulated devices via OPNET Modeler

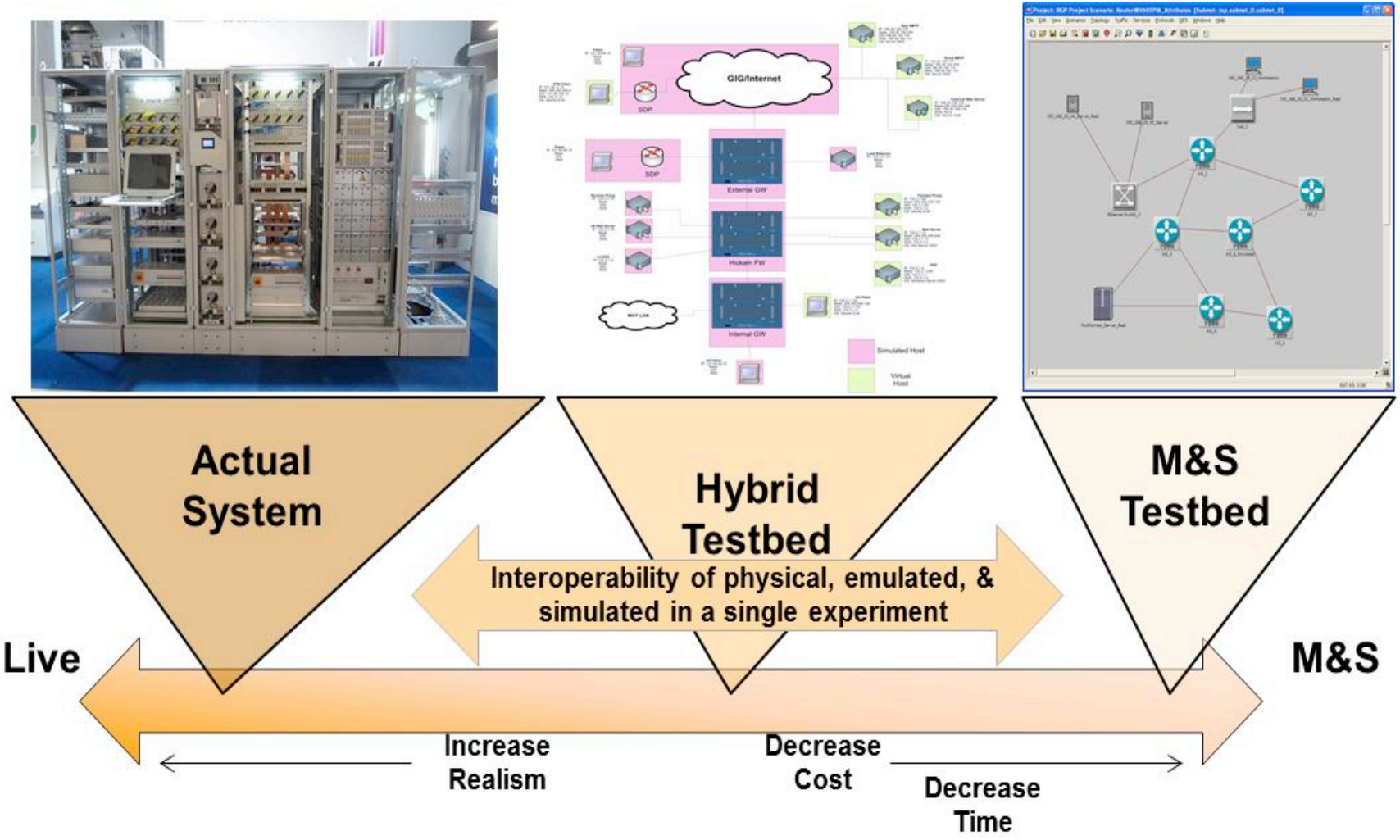


The result is a live, virtual, and constructive experiment to support cyber operations research and analysis of SCADA systems

SCADA system under test



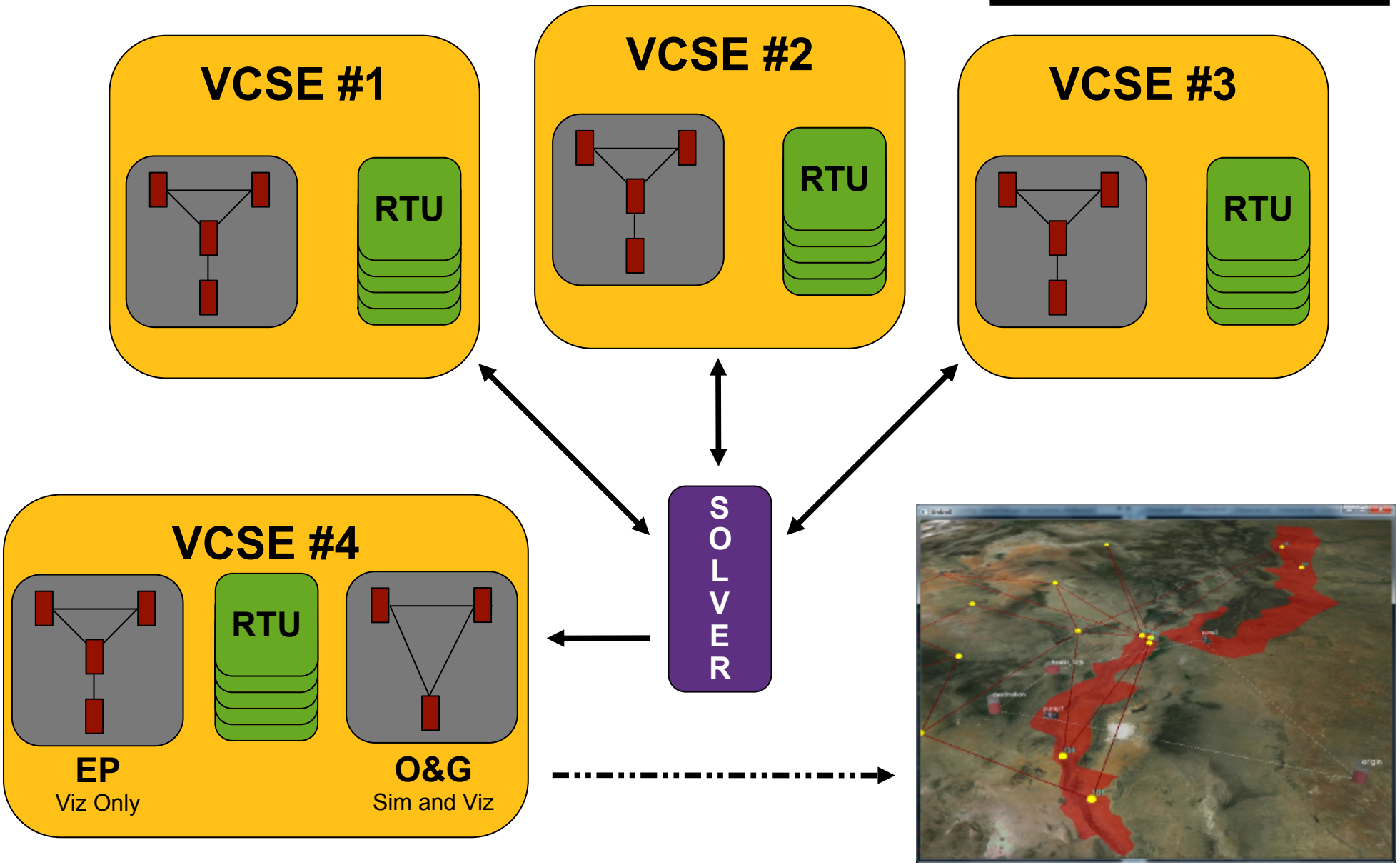
Live, virtual, constructive analysis



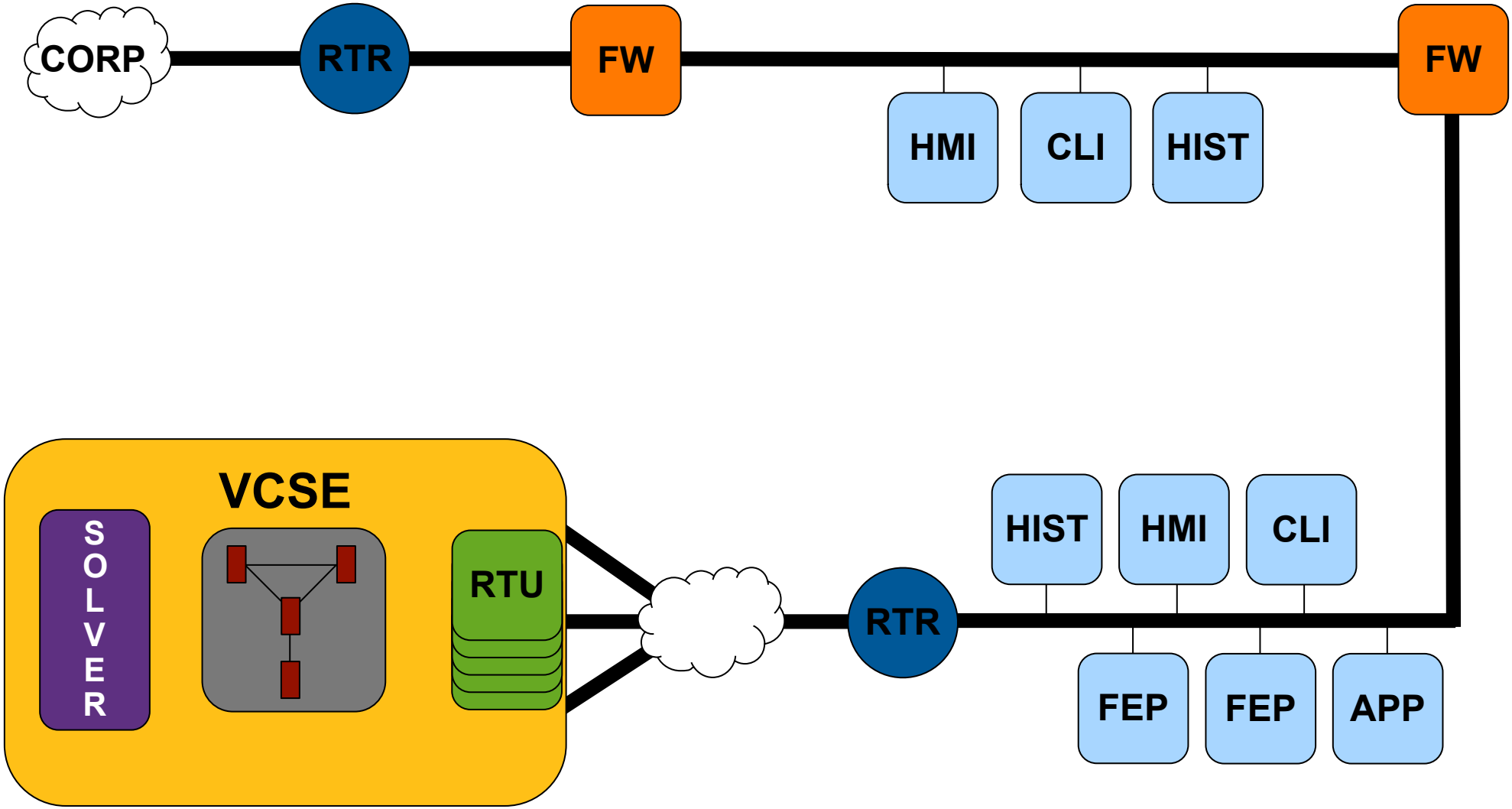
Cyber-physical test environments

Domain	Live	Virtual	Constructive
Control	SCADA, PLC, RTU, relay	Virtual SCADA server, SoftPLC, VMWare	PLC, RTU, relay
Network	Cables, firewalls, routers	Dynamips, Vyatta, OpenVSwitch	OPNET, simple delay model
Process		RTDS, RT-Lab	Load flow, fluid flow

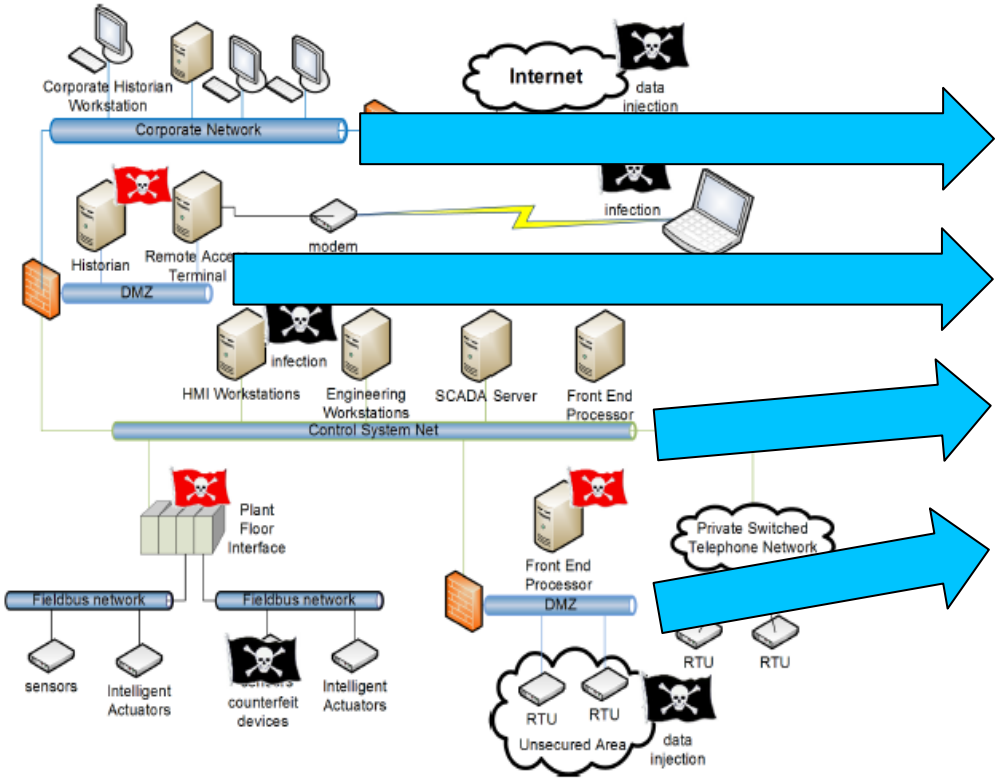
Example VCSE deployment

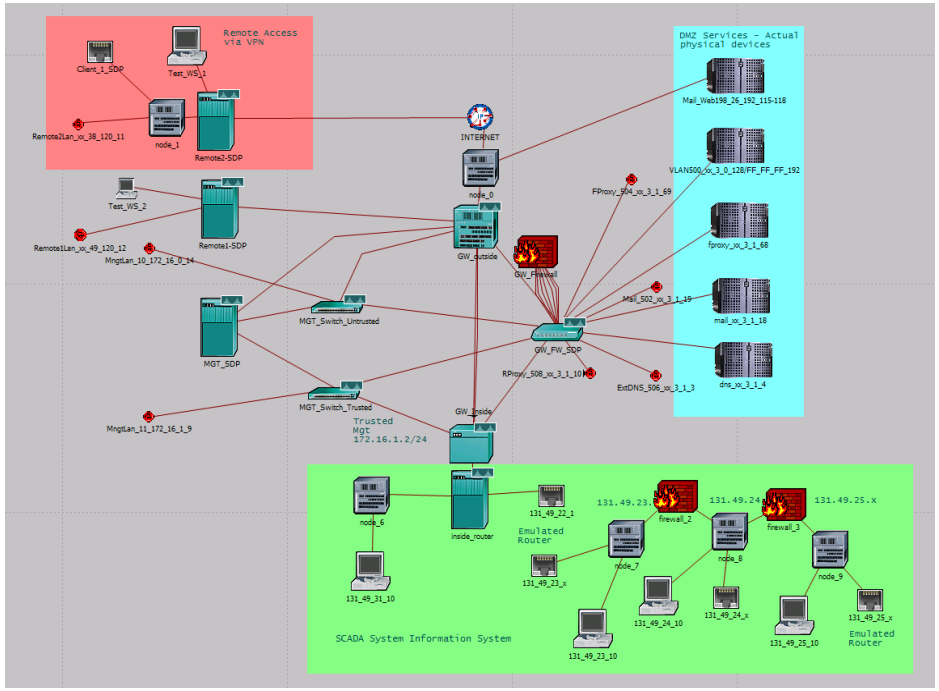


Example VCSE environment



Network architecture-to-model





Cyber analysis of SCADA systems

- Analysis of cyber attacks targeting the business network
  - Reconnaissance – what data/info can be collected
  - Resistance to common hacker tools – response to hacker tools such as Metasploit
- Analysis of cyber attacks targeting the control system network
  - SCADA specific protocol manipulation (DNP3, ModbusTCP, etc)
  - Man-in-the-middle attack susceptibility
  - Effects of malware on control HW/SW and process operation
- Analysis of mitigation technologies for control system networks
  - Effectiveness of mitigation against attacks
  - Impact of mitigation on process control system

Conclusions

- LVC enables construction of scalable, high-fidelity testbeds
  - Put highest fidelity where it is needed
  - Couple with simulation to achieve scaling
- LVC experiments are reconfigurable
  - Graphical user interface
  - Experiment configuration schema
- LVC allows an analyst to verify configurations before they “go live”
  - Actual hardware coupled to VMs and simulators

Contact

MILCOM'12
TRUSTED COMMUNICATIONS...AWARENESS TO ACTION

Bryan T. Richardson
Sandia National Laboratories
VCSE Program Lead

505.845.2386 (UNCLASS)
btricha@sandia.gov (NIPR)
btrichas@sandia.doe.sgov.gov (SIPR)
abricbt@doe.ic.gov (JWICS)