SAND2010-5471P

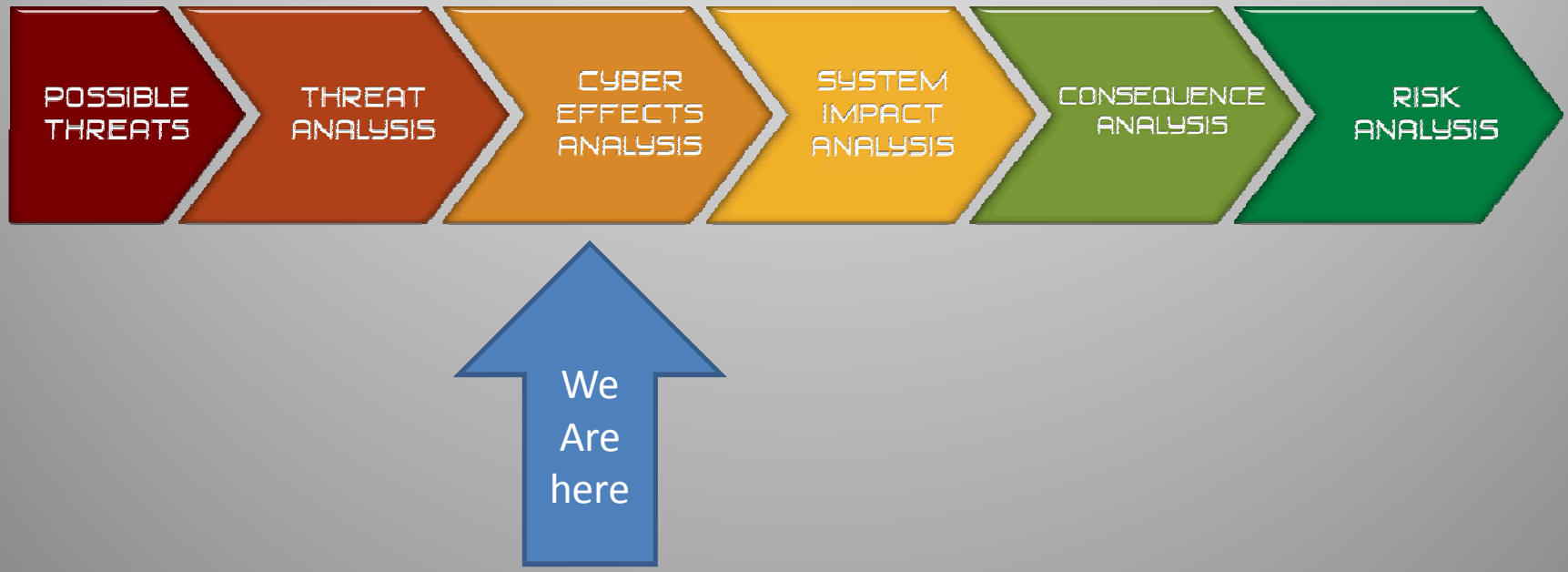
Virtual Control System Environment

12/10/2013

Sandia National Laboratories

Integrated Risk Analysis Approach

Cyber Effects Analysis: What can a hacker really achieve?

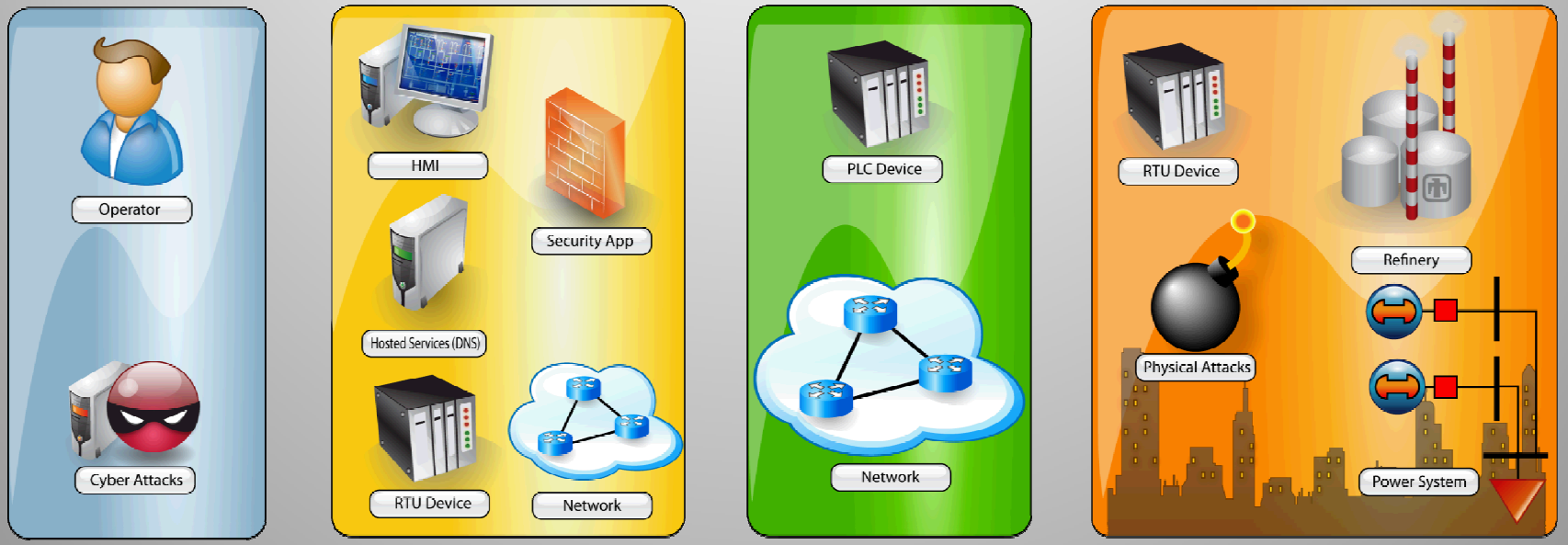


Cyber-Physical Systems Analysis

Goal: Understand how cyber threats operate on particular physical systems

Options	Complications
Live system testing	Can put lives/equipment in danger
Testbed systems	Testbeds 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.

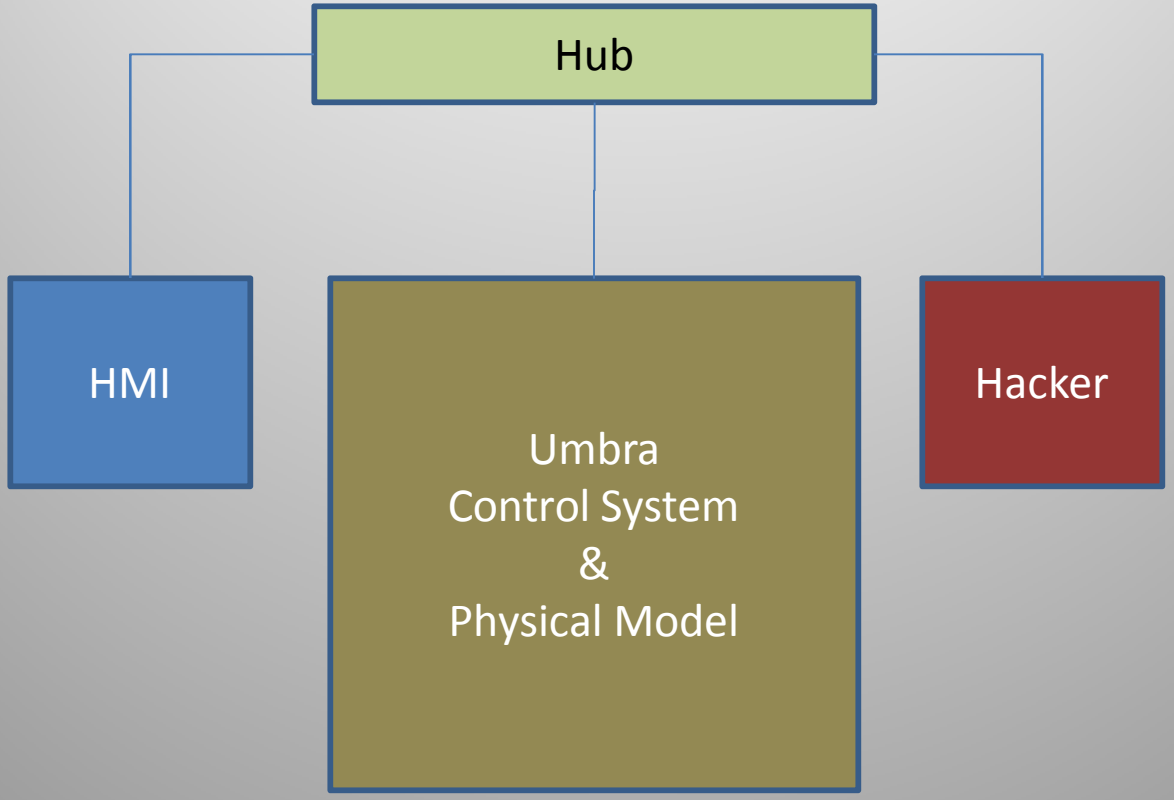
Virtual Control System Environment



Reboiler Demonstration

- A simple subset of common refinery process
- Commercial HMI (ClearSCADA)
- Simple hub networking
- Metasploit Attack
  - Compromise Windows on the HMI machine
  - From there, send Modbus commands to the RTUs within Umbra
  - Multistage attack demonstrates a general strategy for overcoming a system's safeties

Reboiler Demonstration: Network Layout



VCSE Use Cases

- Training Operators to recognize cyber attacks
- Training cyber assessment teams to work in control system environments
- Providing red teams with modeling beyond the “table top”

Questions?

Comments?