U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

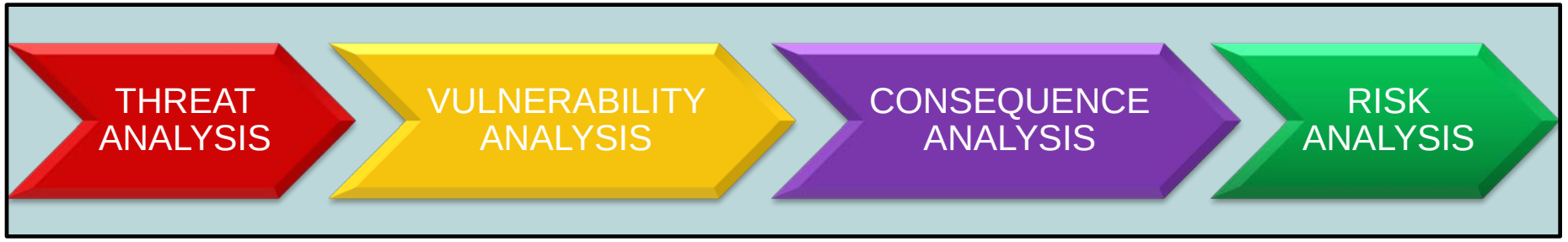
Alexandria, VA ♦ July 20-22, 2010

John Mulder

Sandia National Labs

Hard-Problems Analysis (VCSE Validation)

Integrated Risk Analysis Approach



What Threats are we Concerned about?

Evaluate effects of cyber vulnerabilities

What are the physical impacts?

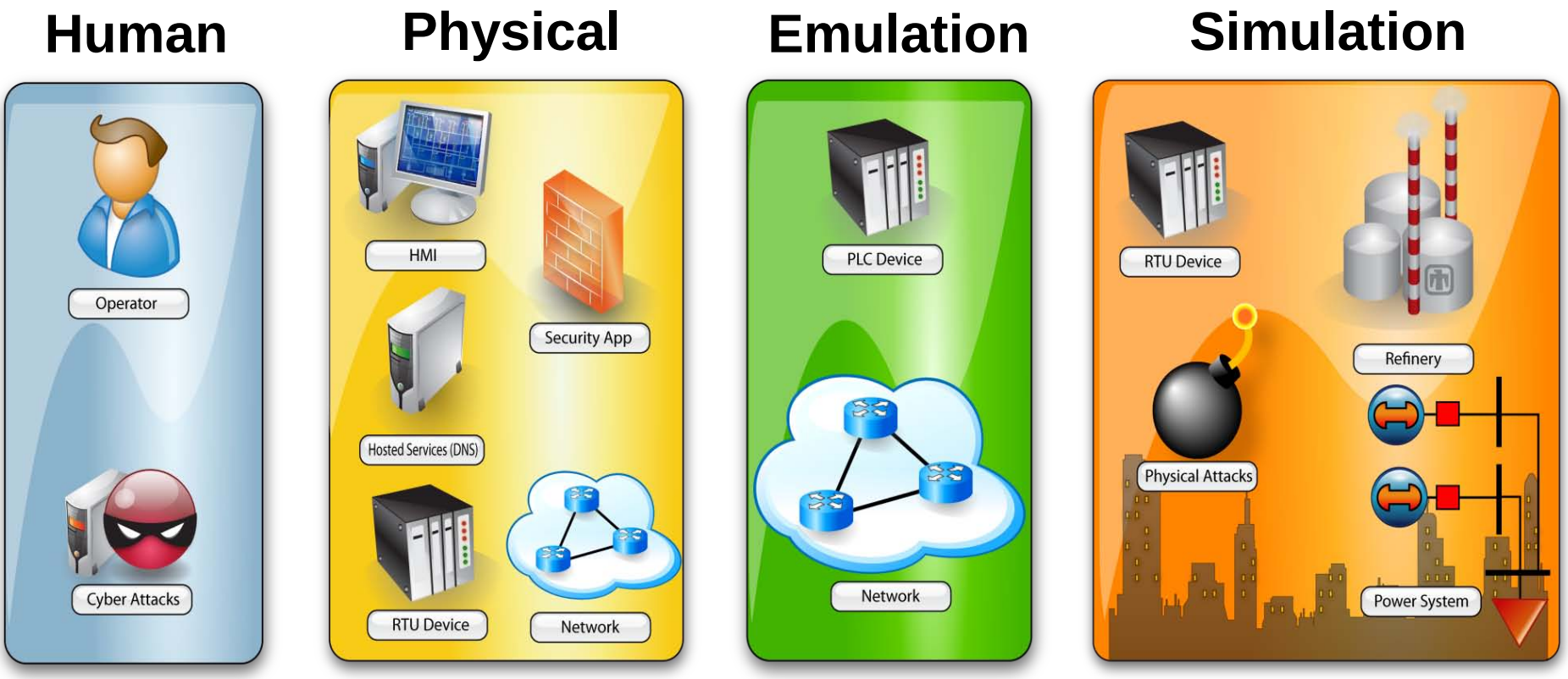
Assess and quantify the Risk?

We Are Here

Cyber Effects Analysis: *What can a hacker really achieve?*

Mission: To reduce the risk of critical infrastructure disruptions due to cyber attacks on control systems

Virtual Control System Environment



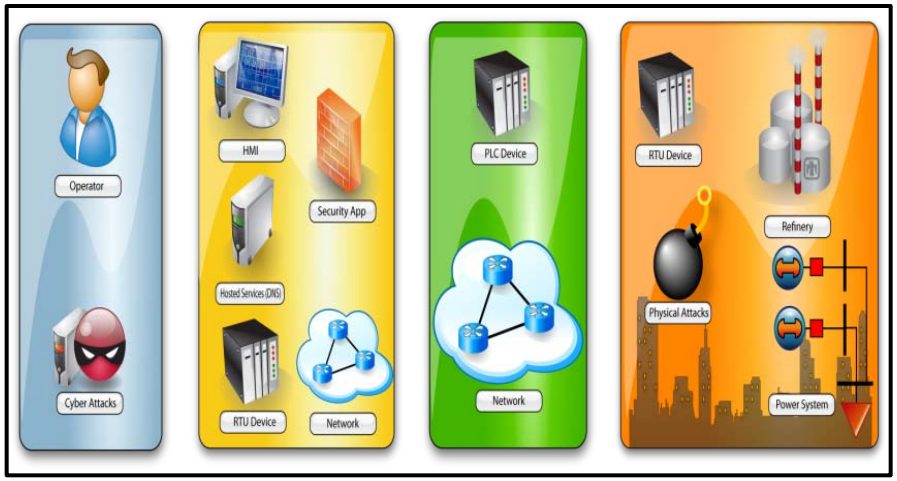
Summary Slide: Virtual Control System Environment

Outcomes: An industry accepted detailed *model* of a transmission substation's control system and automation architecture that performs as expected under specific use case scenarios.

Roadmap Challenges: Develop a scalable virtual control system simulation tool for evaluating security architectures and mitigation options.

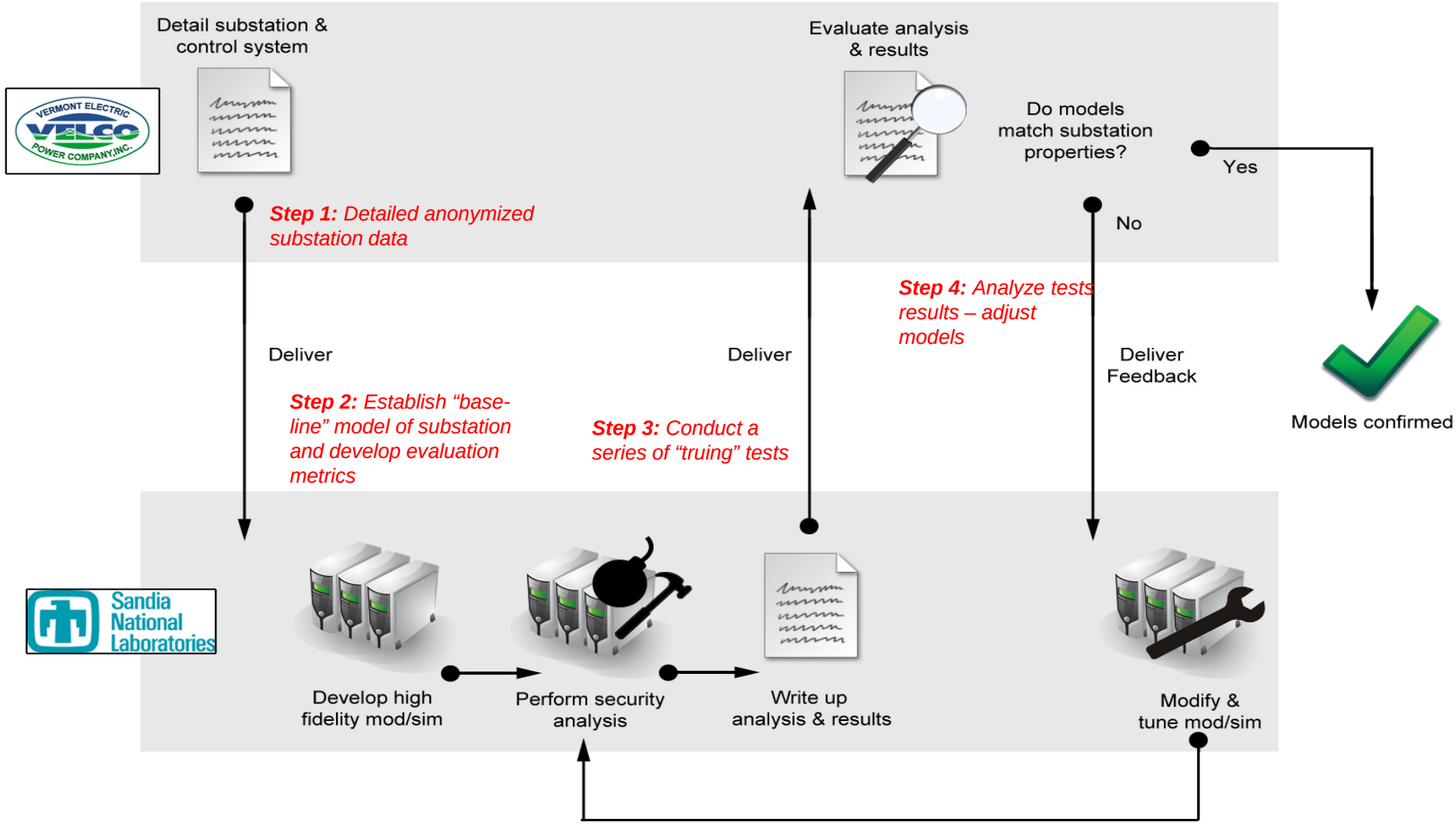
Major Successes:

- Industry non-disclosure agreement in place
- Conducted a face-to-face meeting with industry partner to discuss the technical details of the project
- Weekly t-cons have been established



- **Schedule:** Engage utility-3QFY10; Agreement on what will be modeled-3QFY10; Complete modeling & "truing" tests-4QFY10; Modeling results report-4QFY10
- **Level of Effort:** $500K
- **Funds Remaining:** $225K
- **Performers:** SNL
- **Partners:** Vermont Electric Power Company (VELCO)

Approach and Execution



Technical Accomplishments, Quality, and Productivity

- **Challenges to Success**
  - Lack of operational knowledge and site-specific technical data (Solution: develop partnerships with industry)
  - Combining various technologies into a single environment is complex (Solution: understand what questions are being asked to leverage physical, simulation, and emulation)
- **Technical Achievements to Date**
  - A stable VCSE development platform that integrates:
    - 3rd party power flow solver (PowerWorld), Modbus/DNP3 RTUs, communication visualization tool (NetEye), and 3D representations of electric power components

Technology Transfer, Collaborations, and Partnerships

- **Plans to gain industry input**
  - NDA has been signed
  - Joint meetings have been established
  - The process to anonymize the necessary information needed by SNL has started (sensitive names and IP addresses)
- **Plans to transfer technology/knowledge to end user**
  - VCSE is a *resource for industry* it is NOT intended to be a "shrink-wrapped" tool
  - Tools from VCSE have already been provided to other government researchers
  - Explore the possibility to open source the VCSE protocol libraries

Next Steps

- **Approach For Next Year**
  - Confirmation of additional VCSE components
  - New communication protocol stack development (targeted for Smart Grid architectures)
- **Describe potential follow-on work, if any**
  - VCSE is currently being used by several other projects at SNL to perform security assessments and to determine the value of security mitigations. These projects are scheduled to continue through FY11.

Questions?