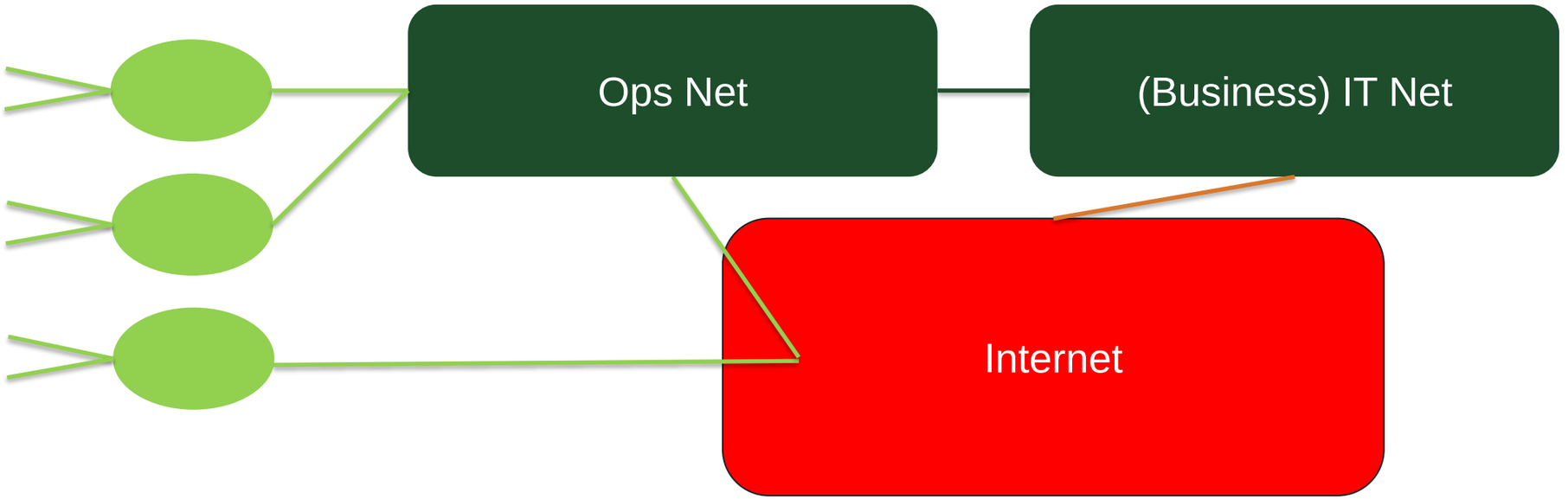
The State of Operational Energy Nets

Dr. Craig Partridge, Chair of Computer Science

Colorado State University

A Net Architecture Like This



Ops Net: Manages operational assets using SCADA, directly and over TCP. Also has both internal network and tunnels over the larger Internet to various assets. Run by Ops team.

IT Net: Runs business applications over TCP/IP. Run by corporate IT.

What Ops Team Tells Corporate IT Security

- “Our network is safe”
- “It is air gapped”
- ”Changing/updating ops net risks operational downtime and millions in revenue”

What We're Learning about Ops Net

- Specialists in network measurement (and security) are starting to get access to measure Ops Nets in various corporate settings. (E.g. see upcoming paper at ACM Internet Measurement Conference in late October by Mai et. al).
- What we are learning:
  - The Ops Network may **not** be airgapped.
  - In some cases, the Ops Network is interacting with equipment and systems of other energy companies (opportunity for one company's security failure to migrate…)
  - Some flux due to acquiring and selling assets (apparently w/o doing a security assessment)
  - The protocol implementations are often out of date and/or non-compliant (presumably contain security risks – keeping software up-to-date is usually a core requirement of any security profile such as NIST-800-171)