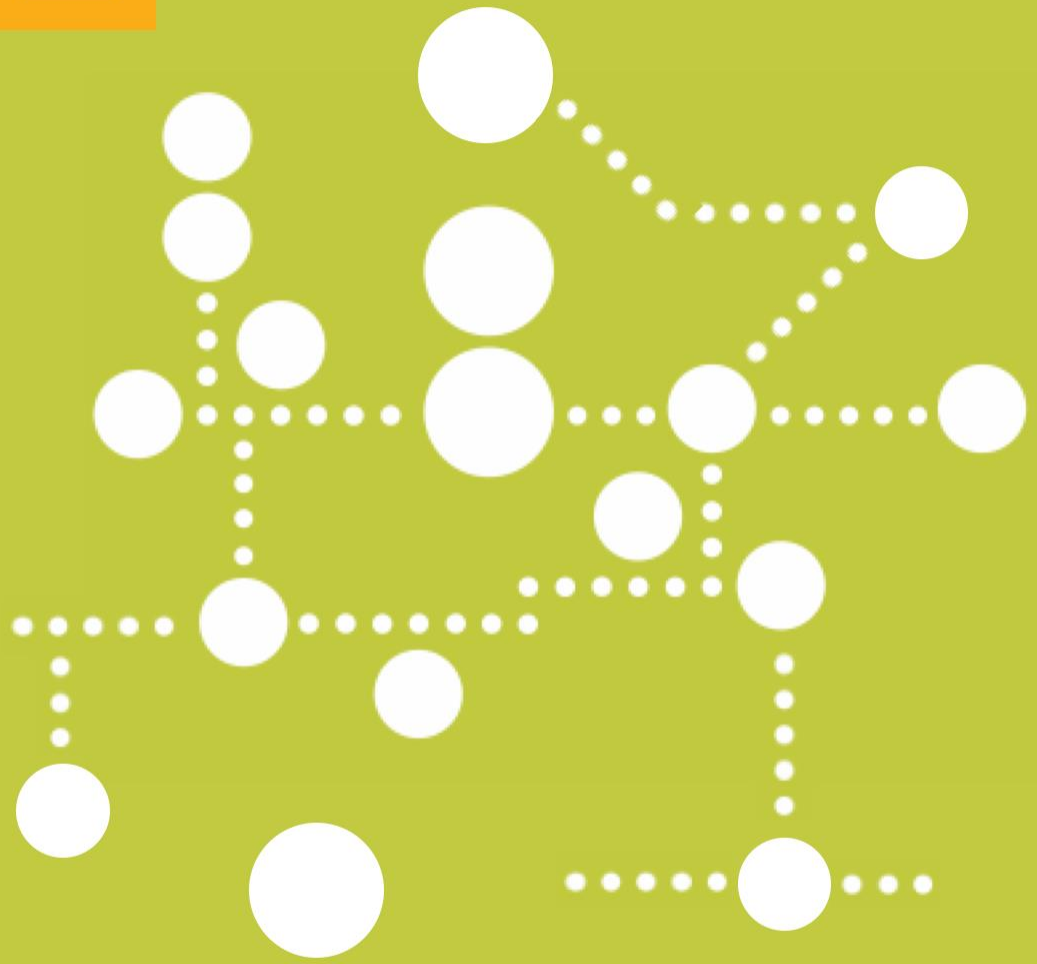

Energy Infrastructure Cyber Security: The Challenges and Opportunities ahead for the R&D Community

David M. Nicol
Franklin W. Woeltge Professor of ECE
Director, Information Trust Institute
University of Illinois at Urbana-Champaign

This work supported in part by DOE Contracts DE-0E0000679 and DE-0E0000780, and in part by DHS contract 2015-ST-061-CIRC01.
The views expressed are my own, and not the government's!

Challenges and Opportunities

(and how they can collide…)

The near-term future of security is in intrusion detection / reaction

- No matter what preventative technology is deployed, some breach will be possible

The near-term future of intrusion detection reaction is in

- Deeper analysis of data carried
- Correlations between data and physical system state
- Correlations between data and control state

And naturally, this must be done in real-time, with minimum footprint

But…

What should/can be done when an anomaly is detected?

- Should a command be ignored if a model predicts its implementation will cause harm?
  - What level of confidence can we have in a command, and how can we obtain it
    - “deep provenance?”
- Should a packet be dropped if out of context with the protocol
  - Real-time grammers can check….but what to do when an error is detected

Industry will not adopt technology solutions if seen as possibly interfering with legitimate system operations

- What incentivization is possible to study tradeoffs, possibly alter operations?