

NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Impact Analysis from Cyber Intrusion for Electric Power Systems

Jason Stamp, Ph.D.

Sandia National Laboratories



**U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability**



Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Threat-to-Consequence Framework



Challenges/Needs

- Develop ability to map impacts from cyber attack to grid effects
- Incorporate outages caused by cyber attack to conventional reliability analysis approaches
- Convert hybrid grid/control system to finite state approximation for analysis

Results/Benefits

- Models degraded grid reliability from vulnerabilities
- Reveals high-impact risk scenarios
- Determines mitigation tradeoffs
- Displays dynamic grid effects from cyber attack

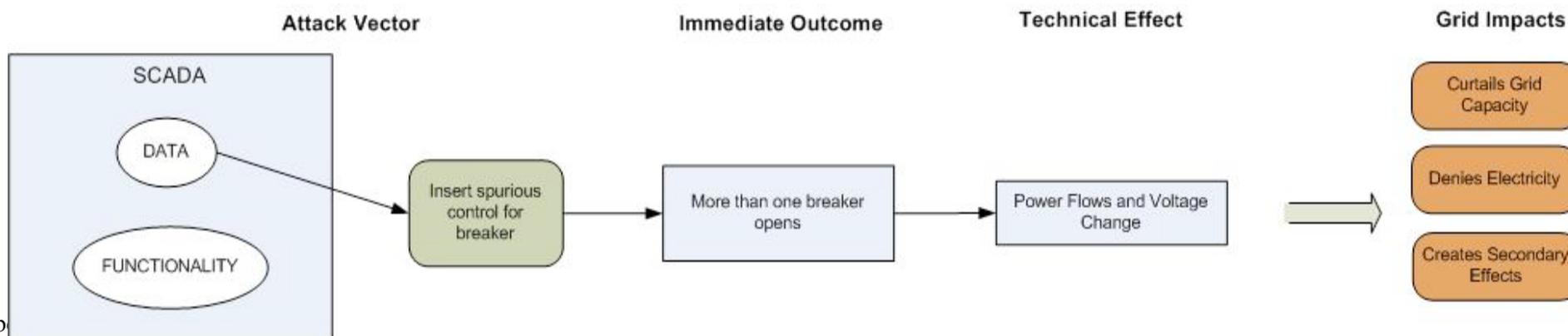
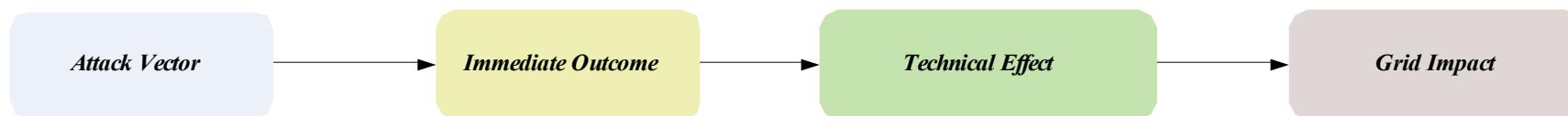
Threat-to-Consequence Framework



- How did the rogue software attack cross the cyber-physical bridge in the electrical system?
- What happened when the breakers tripped?
- How did this attack impact system reliability?
- What were the dynamic effects on the electric power grid?
- What control systems parameters were in place that allowed this attack to cause a significant electrical impact?
- How does system impact information feed into the threat-to-consequence framework?
- How can this analysis be used to prioritize risk reduction activities that address this rogue software attack?

Cyber to Physical Bridge – Approach

- Attack Vector
- Immediate Outcomes
- Technical Effects
- Grid Impacts

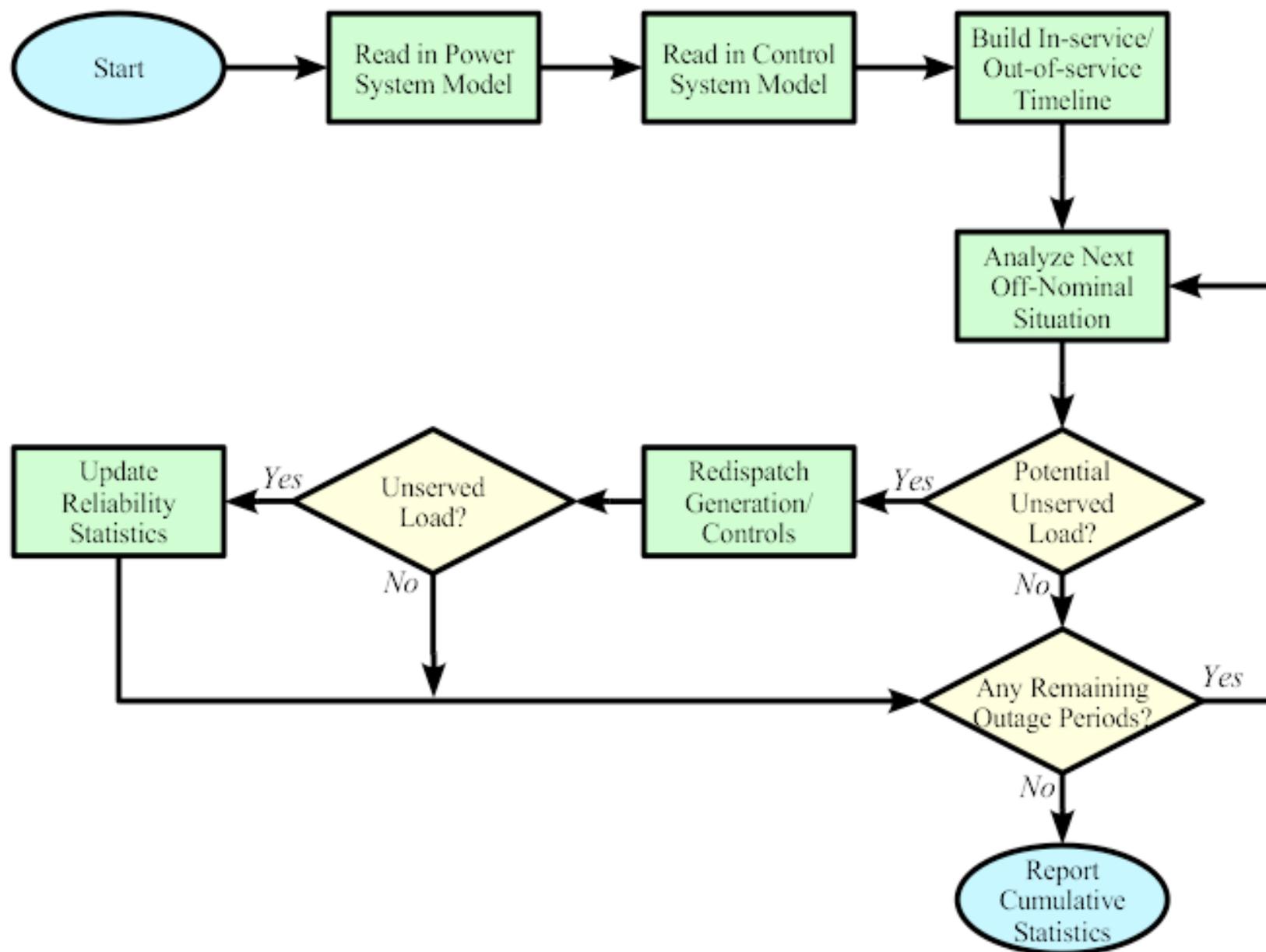


Reliability Impacts: Approach

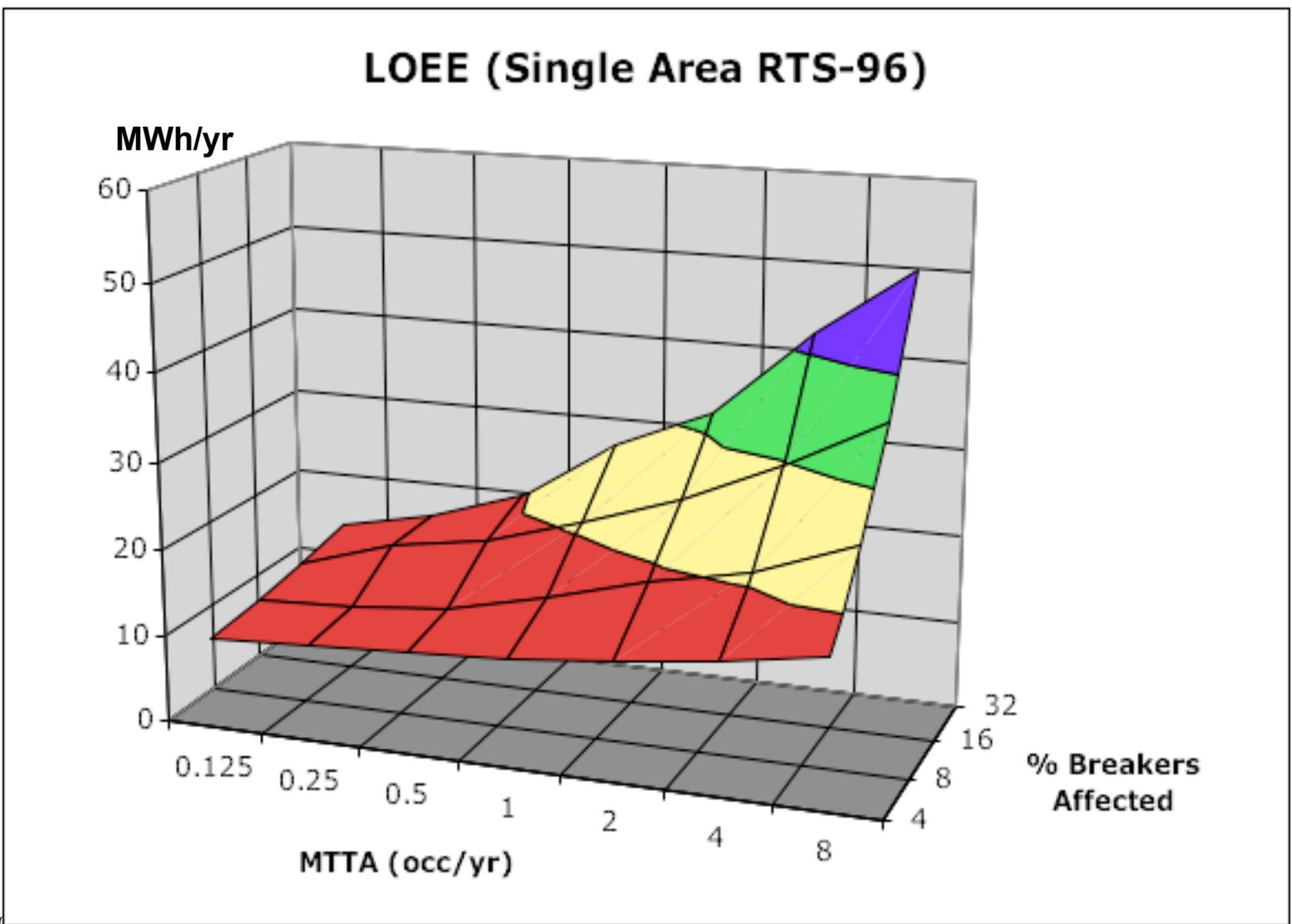


- Team Members include:
 - Annie McIntyre
 - Bryan Richardson
- Determine ratio of reliability degradation resulting from cyber attack
- Evaluate “what-if” scenarios based on recently discovered vulnerabilities to gauge impact to overall grid reliability
- Estimate impact reduction for various mitigation approaches
- Test model: single area IEEE RTS-96 (Reliability Test System)
- Cyber models
 - MTTA: Mean Time To (successful) Attack, in occurrences per year (exponential distribution)
 - MTTR: Mean Time To Recover, in hours (exponential distribution)
 - Rogue software attack will trip some percentage of system breakers
- Measuring reliability: LOEE (Loss of Energy Expectation) (MWh/yr)

Reliability Impacts: Flowchart



Reliability Impacts: Rogue SCADA Software

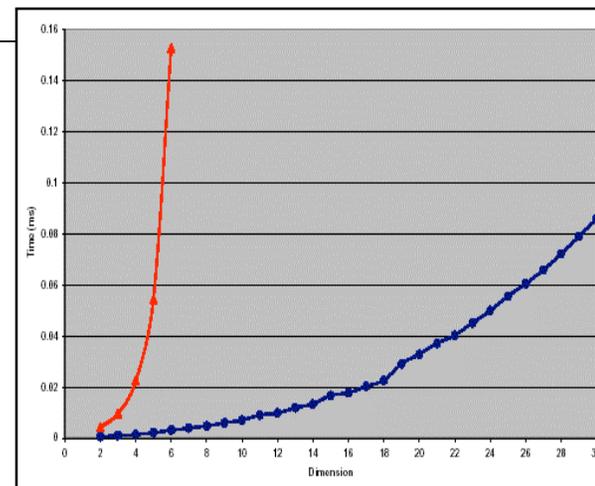
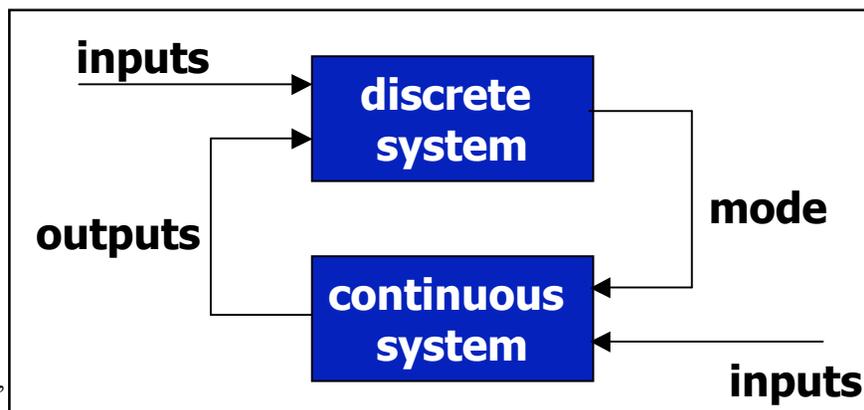
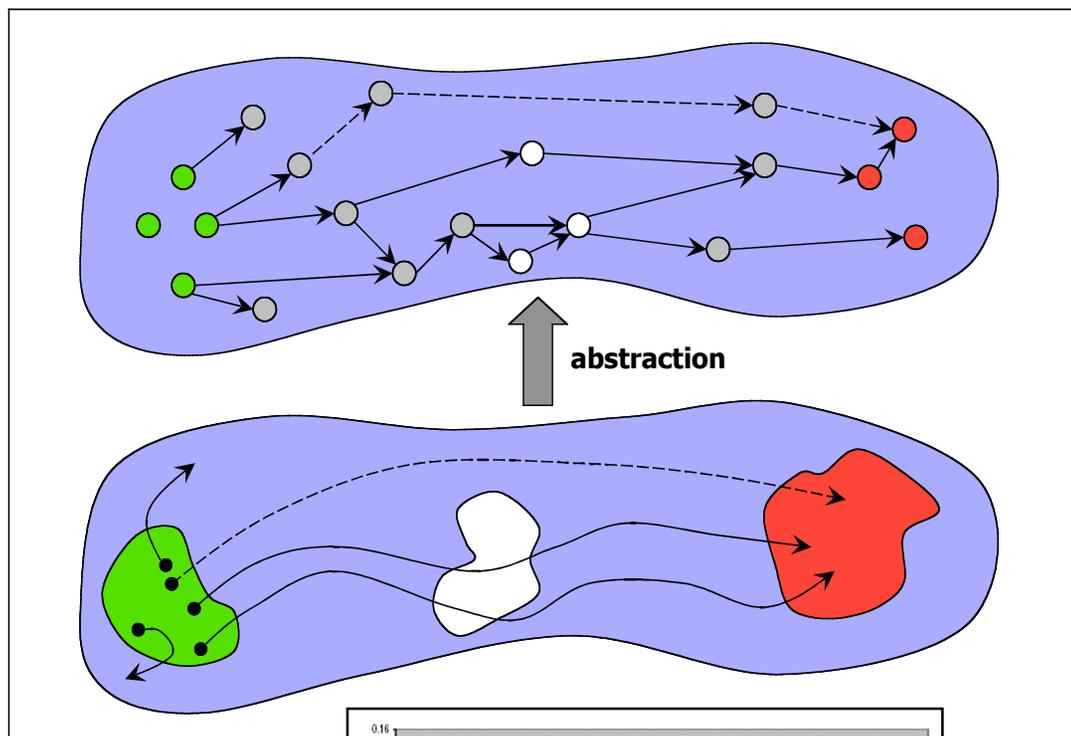


Dynamic Impacts: Introduction

- Team members include:
 - Rich Colbaugh*† †New Mexico Institute of Mining and Technology
 - Randall Laviolette* *Sandia National Laboratories
- Objective: obtain finite state models for infinite state power grid using property-preserving abstraction
- Benefit: efficient/automated/ formal impact analysis
- Intended to help answer the following questions:
 - Is system performance acceptable under some set number of permutations (including cyber attacks against control systems)?
 - If control settings are changed by an adversary, what are the impacts?
 - (future work) What is the sensitivity of control system settings to grid dynamic performance?

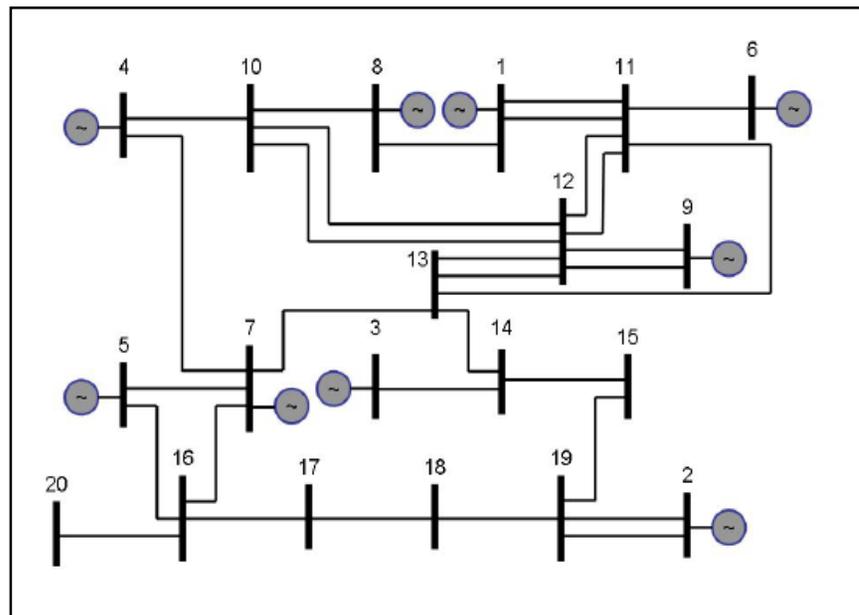
Dynamic Impacts: Finite State Abstraction

- Theory: two formulations
 - Abstraction as a *control system*
 - Abstraction as a *controlled system* (matches control laws presently implemented in grid)
- Computation: apply fast algorithms for computing finite state models with 10K state variables

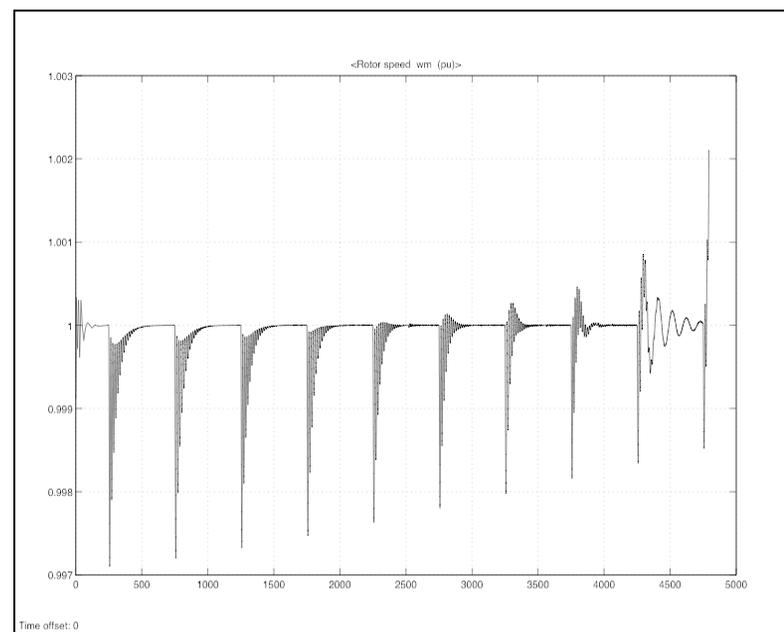
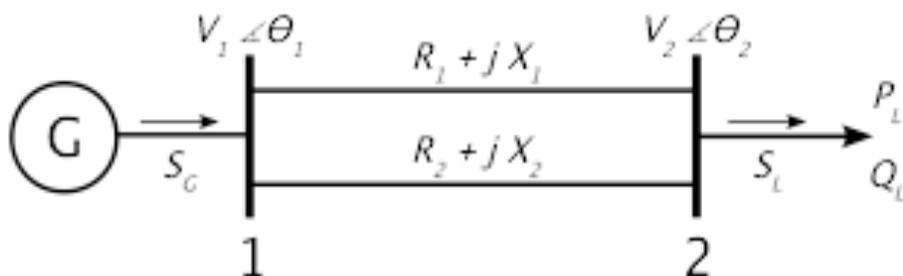


Dynamic Impacts: Finite State EP Models

- Control system formulation:
 - Simple bus model
 - Validation: reproduces observed cascading outages
 - Finite state model: exhibits identical propagation dynamics
 - Better 20 bus model
 - Validation: matches all test data
 - Finite state model: presently under development
- Controlled system formulation:
 - Presently under development
 - Includes instability mechanism caused by cyber tampering



Thanks to Kevin Wedeward (NMT)



Summary

- Reliability analysis provides quantitative cost information for the impacts of cyber attack in terms of grid reliability
- Dynamic impact analysis provides accurate modeling of grid impact from cyber attack over time, including control system effects on system trajectory
- Analysis of Rogue Software Scenario Impacts:
 1. Impact depends on extent of the effects
 2. Given a MTTA above 0.5 occurrences per year, a MTTR of 4 hours, and a percentage of breakers affected above 16%, then the amount of unserved load more than doubles

Conclusion: HIGH IMPACT

3. Reduce the spread of the attack to less than 4% or the MTTA below 0.125 to manage the risk
4. The analysis of dynamic impacts for the proposed scenario is TBD

Backup Slides

Threat-to-Consequence Framework



- How can cyber attack result in electrical outages?
- Might particular cyber vulnerabilities result in significant impacts?
- Are there scenarios for cyber attack that would cause high grid impacts that we were previously unaware of?
- How can we prioritize cyber security mitigation to reduce potential impacts?
- What dynamic impacts can tampering of control systems have on an electric power grid?
- What are the most attractive control system parameters to an adversary for a significant electrical impact?