Testing the Susceptibility of Synchrophasors to GPS Spoofing

Jeff Dagle, PE
Chief Electrical Engineer
Advanced Power & Energy Systems
Pacific Northwest National Laboratory

October 17, 2012
Test Objectives

- Determine the susceptibility of GPS satellite clocks to spoofing that could undermine the accuracy of PMUs
- Tests carried out at the PNNL Electricity Infrastructure Operations Center (EIOC) December 2011 with Northrop Grumman and University of Texas-Austin
- Three different satellite clocks were utilized in the testing
Schematic of the Test Setup

- Rooftop Antenna
- Splitter
- Non-Spoofed GPS Time Reference Receiver
  - Reference PMU
- Spoofer
- Spoofed GPS Time Reference Receiver
  - PMU
- RF Shielded Tent
  - Spoofed Signal Transmit Antenna
  - Authentic Signal Repeater
  - Receive Antenna
RF Shielded Tent
Spoofting the Synchropahsor
Conclusions

- All three satellite clocks were susceptible to GPS spoofing
  - Some differences in the rate of change that could be implemented (defeating the internal error checking algorithms)
  - Some differences in how the clocks responded when the spoofing signal was turned off
- Need to find alternative methods for ensuring critical applications cannot be undermined