

# NERC CIP for Phasor Systems

Terry Bilke

Midwest ISO/NASPI OITT

October 7, 2009

# Background

- ARRA will cause step-change in phasor investment
- ARRA has a NERC-CIP (cyber security) expectation
- Second-hand information implies that in some areas a significant amount of \$ is being spent on CIP for PMUs
- Recommending an objective process or tool to determine CIP risk

# Recommendation

- Objective tool or process to assess risk
- Example questions on next slides

Microsoft Excel - Copy of PMURiskSurvey.xls

NO.	Question	Answer
1	Does the PMU also serve as a relay?	No
2	Is the data port separate from the maintenance port?	Not a relay
3	Does the PMU control a critical asset?	Yes
4	Are the PMU readings from a critical asset?	No
5	Does the data flow through a critical cyber asset's ESP (EMS, Operations WAN, etc.)?	No
6	Is the data from the PMU used for direct control (such as special protection)?	Yes
7	Is alternate data from the substation (SCADA, state estimator) available to the system operator for decision-making?	No
8	Is this PMU on your list of cyber assets evaluated for CIP compliance?	Yes
9	Is encryption used to protect the PMU datastream?	No
10	Is secure VPN or dedicated circuit used to protect the PMU datastream?	Yes
	<b>Total risk</b>	<b>Low</b>

**Use this Section to Create a Record**

Company	ATC
Substation	North Beaver Dam
Reviewer	Fred McMurray
Notes	
File name	NBD

28430 }  
 Improved Violation Risk Factors / AddQuestion /  
 Ready

# Risk Questions

- Is the PMU a relay?
  - If yes, is the data port separate from the maintenance port?
  - If yes, are other mitigation steps taken?
- Does the PMU monitor a critical asset?
- Does the data flow through a CIP electronic security perimeter?
- Is the data used for direct control (such as special protection)?

# Risk Questions (continued)

- Is there alternative data available to your operators for decision-making (SCADA, state estimation) for the same facility?
- Is the PMU/PDC in your list of evaluated systems for CIP risk?
- Is encryption used to protect the data stream?
- Is secure VPN or dedicated circuit used to protect the data stream?

# Summary

- Should phasor data have more CIP overhead than SCADA or ICCP data?
- Is the approach in this presentation workable?
- Are there other risk questions that should be asked?
- How do we communicate this to the Industry?
- Send suggestions to [tbilke@midwestiso.org](mailto:tbilke@midwestiso.org)