**Goals**

- Design an efficient monitoring architecture to detect and potentially prevent intrusions targeting or originating from an advanced metering infrastructure (AMI).
- Implement a prototype of this monitoring solution and validate its accuracy and applicability.

**Situational Awareness Solution**

**Research Results**

- Comprehensive monitoring architecture implemented:
  - Offline development process:
    - Protocol
    - Network
    - Use Cases
    - Build specification-based checkers
    - Mathematically prove coverage of security policy
  - Online operation process:
    - Display configuration on sensors in the field
    - Tweak policy to specific AMI

- Tested with real AMI equipment

**Fundamental Questions**

- What are the threats targeting AMIs?
- What detection technology should be developed to cover those threats?
- What monitoring architecture should be deployed?
- What is the best way to automatically respond to security compromises?
- What is the best way to provide large-scale situational awareness?

**Challenges**

- Large-scale environment.
- Real-time and cost efficiency requirements.
- Sensors to run on low-computation hardware with limited memory.

**Prototype in Development**

- Distributed Alert Correlation
- Visualization
- Security Policy
- Formal Policy

**Broader Impact**

- Definition of a rigorous process utilities and vendors can use to design and develop an efficient monitoring architecture.
- Discussion with industry partners (Fujitsu, EPRI, FirstEnergy, and Itron) to collaborate on development and evaluation, and to plan for technology transfer.