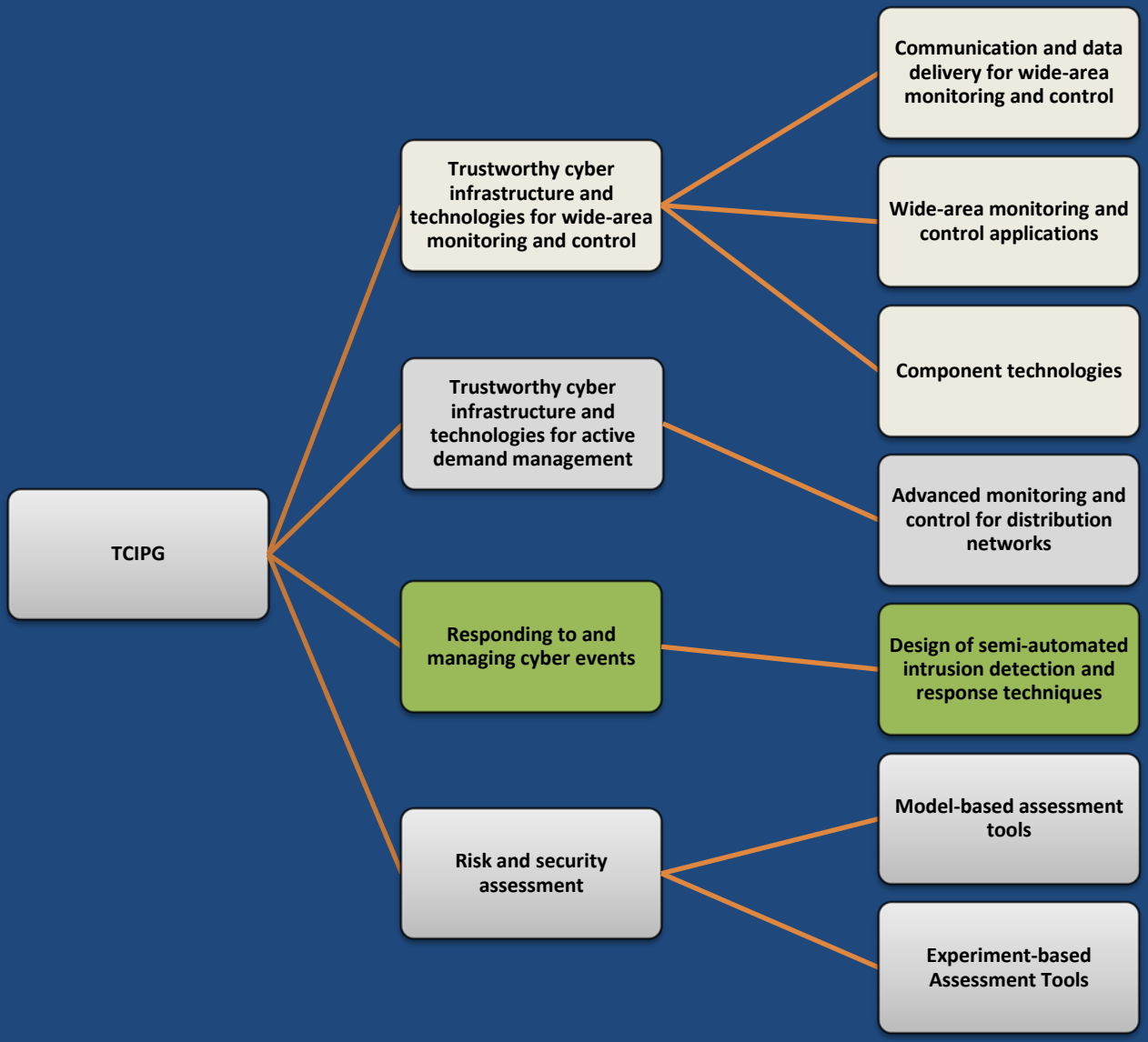
# Responding to and Managing Cyber (and Physical) Events

Bill Sanders

# TCIPG Cluster Arrangement



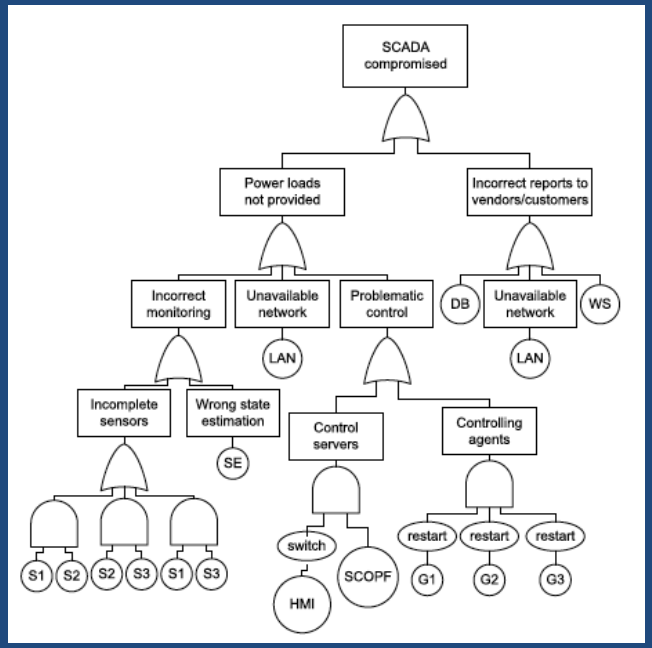
# Cluster Overview

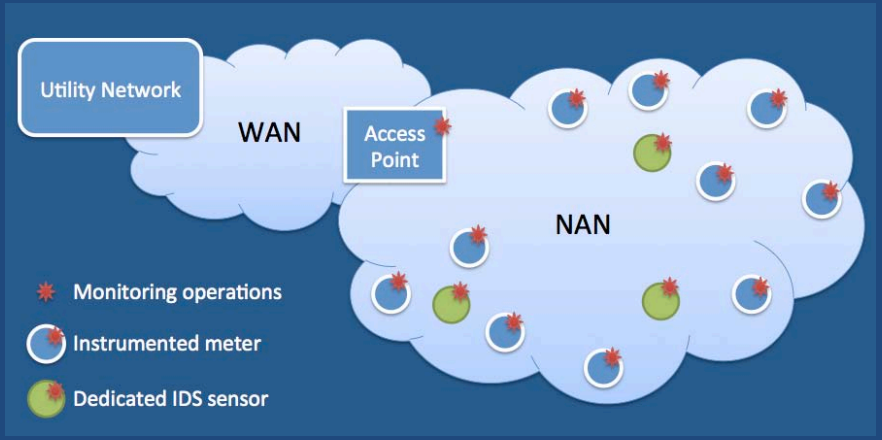
- Combined cyber and physical attack detection, response to detected attacks, and recovery from attack consequences is essential to providing resilience
- Existing detection and response methods are *ad hoc*, at best, and rely on assumptions that may not hold
- Aim to detect and respond to cyber and physical events, providing resilience to partially successful attacks that may occur:
  - Making use of cyber and physical state information to detect attacks
  - Determine appropriate response actions in order to maintain continuous operation
  - Minimize recovery time when disruptions do occur

# Cluster Objectives

Create complete detection, response, and recovery environment, at all necessary levels of abstraction:

- Physical level
  - Taking into account noise and malicious manipulation of values
- Hardware level
  - Respecting embedded and cost sensitive nature of power system components
- OS / Platform level
  - Dealing with lack of source code other observability limitations
- Computer network level
  - Accommodating observability limitations due to encryption and protocols



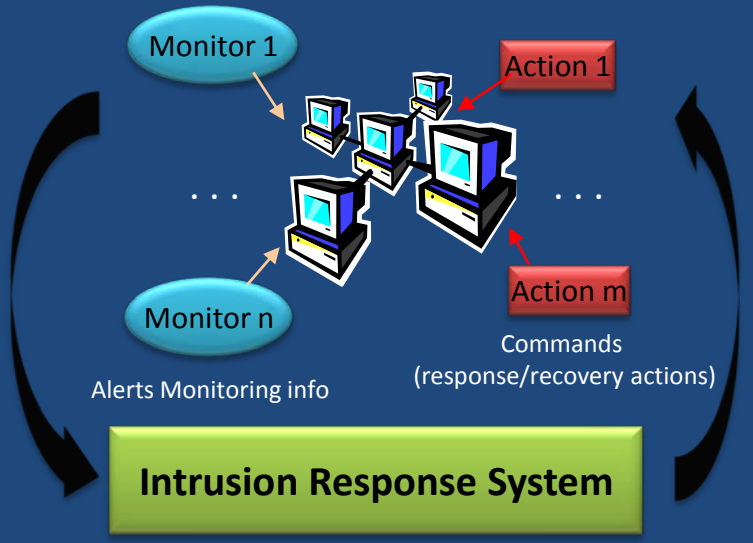



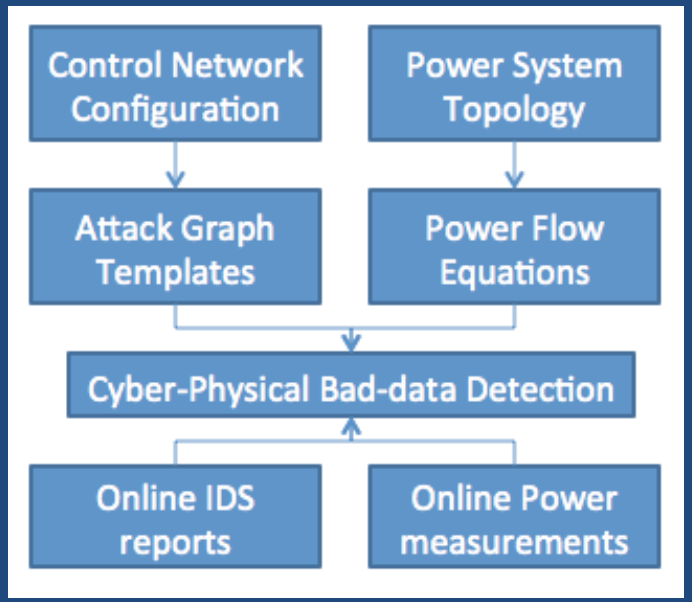
# Cluster Activities (with more details in posters)

- Ongoing
  - A game-theoretic response and recovery engine
  - Assessment and forensics for large-scale Smart Grid networks
  - Coordinating black start operations using synchrophasors
- New Starts
  - Hardware-based IDS for smart meters
  - Usable management tools for the smarter grid's data avalanche

# Cluster Accomplishments and Impacts

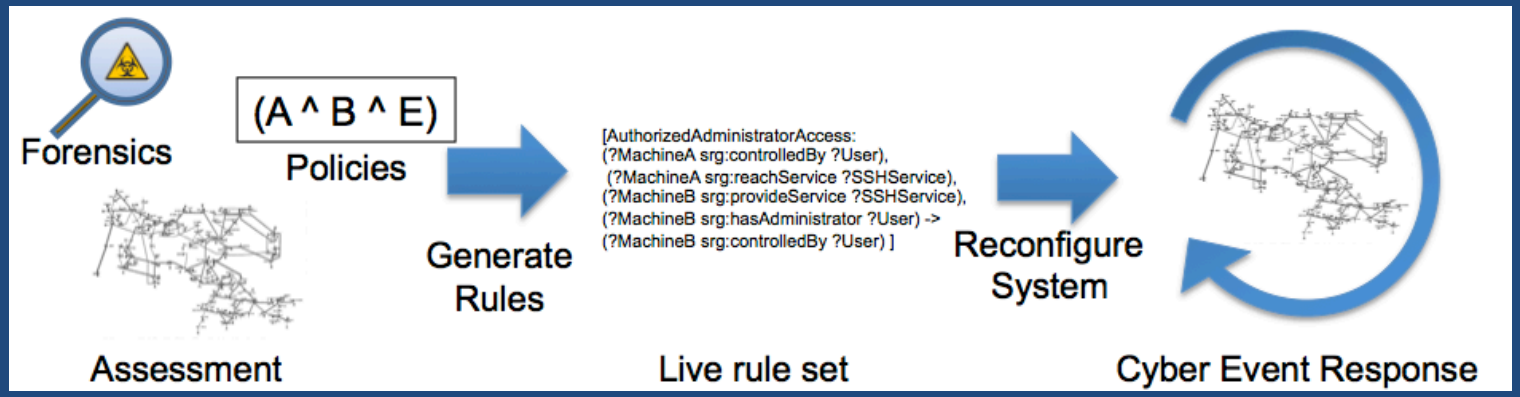
- Built and demonstrated prototype RRE implementation that can:
  - Automatically generate and learn system-wide dependency graphs
  - Estimate security state of cyber-physical power system from cyber-side IDSs and physical sensors
  - Estimate consequence-based security metric to provide power system operators with global situational awareness support



# Cluster Accomplishments and Impact, cont.

- Developed and demonstrated analog signal-level hardware-based IDS for smart meter and other embedded infrastructures
- Developed OS-level policy based online forensics engine to drive host level response.

# Cluster Directions for Coming Year

- Perform sensor gap analysis to determine if sensor set considered is sufficient, or addition sensor development necessary
- Expand range of data used in decision making, and methods used for decision making, as part of “data avalanche” activity
- Integrate cluster work with TCIPG work on malicious data detection
- Implement second version of RRE engine, using symbolic data structures to achieve scalability
- Integrate results from cluster activities and related work going on in other clusters to form complete demonstration, likely in AMI area

# Questions and Discussion