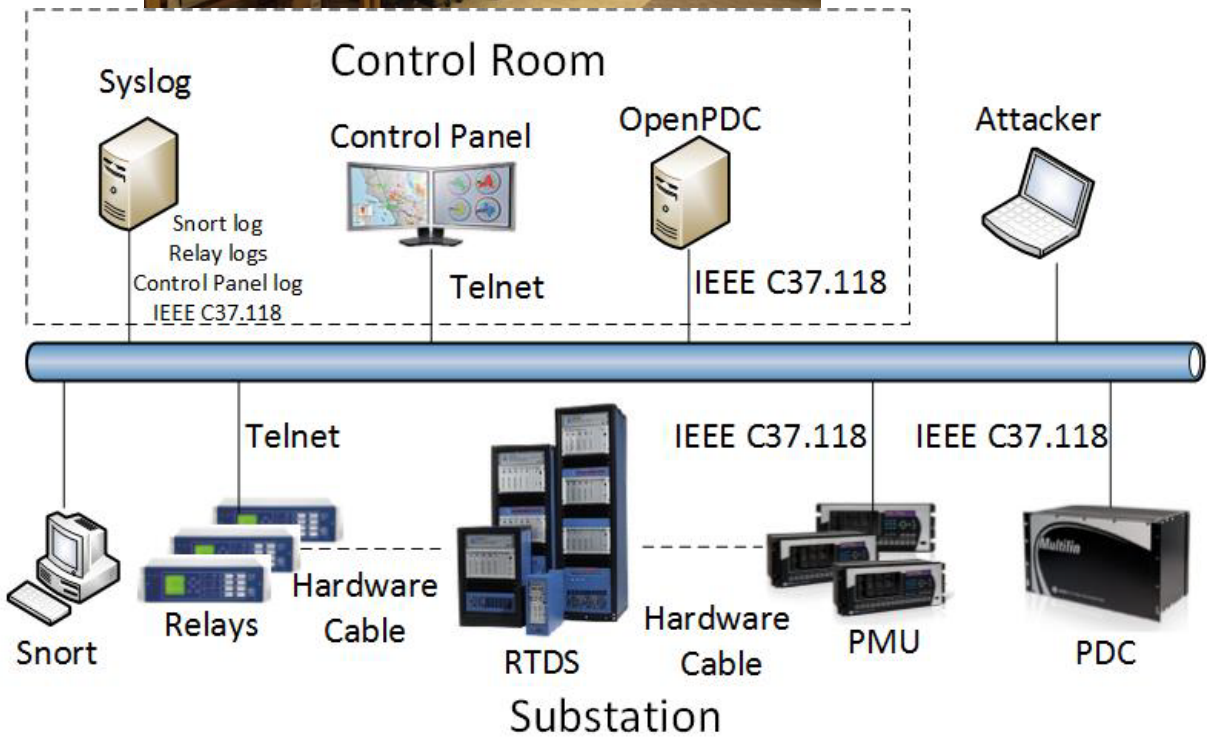
A CYBER-PHYSICAL POWER SYSTEM TEST BED FOR INTRUSION DETECTION SYSTEMS

Thomas H. Morris, Uttam Adhikari, Shengyi Pan

Testbed Overview



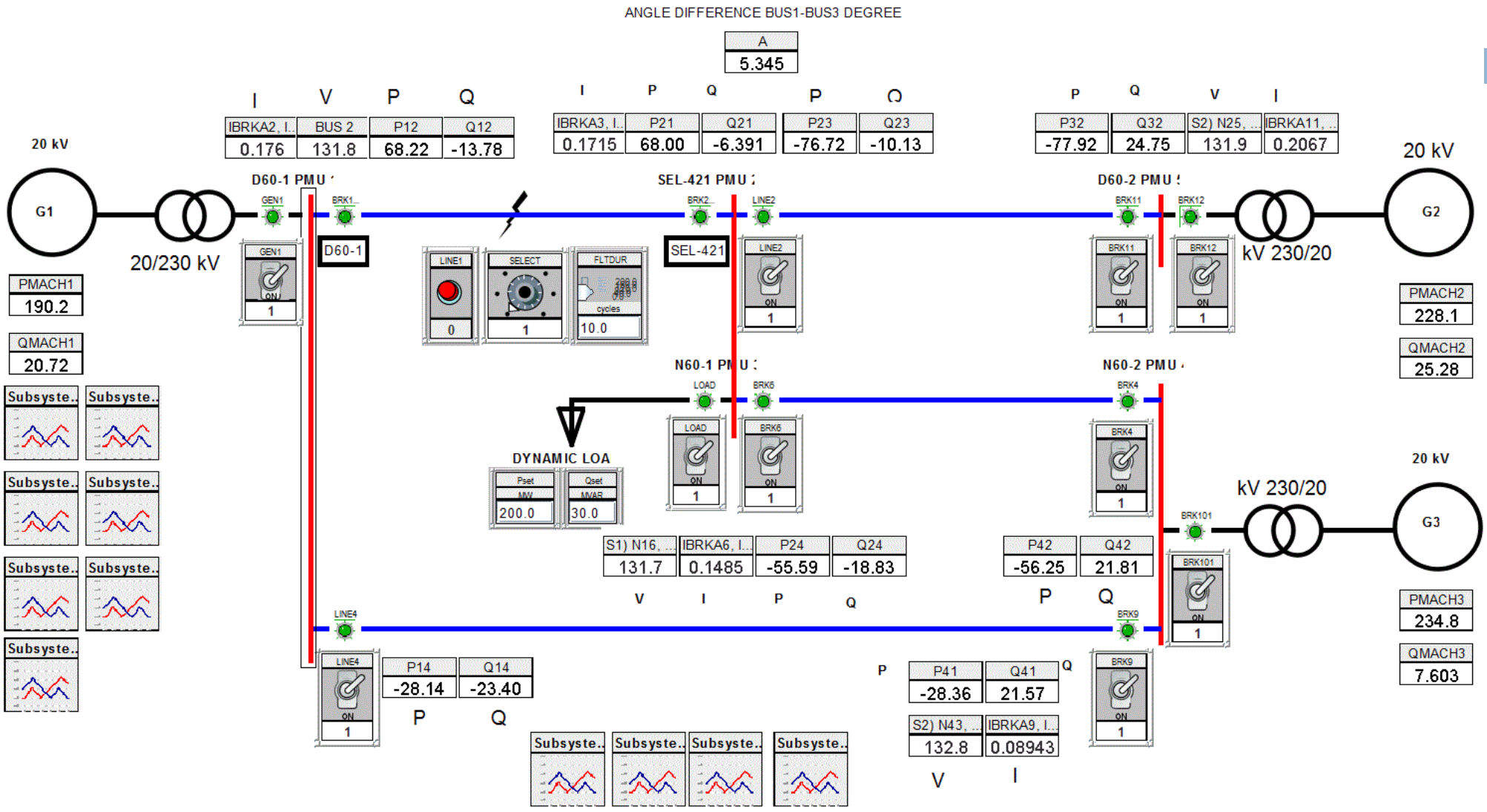
Testbed Goal

- Hardware in the loop transmission system simulation
  - Distance protection, over current protection w/ automatic reclosing
  - Simulate power system disturbances
  - Simulate cyber security attacks
- Datasets
  - Train and validate intrusion detection system algorithms
  - Fusion of multiple sensors
    - Network logs, phasors, Snort, relay logs, control panel logs
- Automate attacks and disturbances for random simulation
  - Run at night to create large datasets of
    - steady state, disturbances, control actions, and attack data
    - random order

Key Ingredient - Synchrophasors

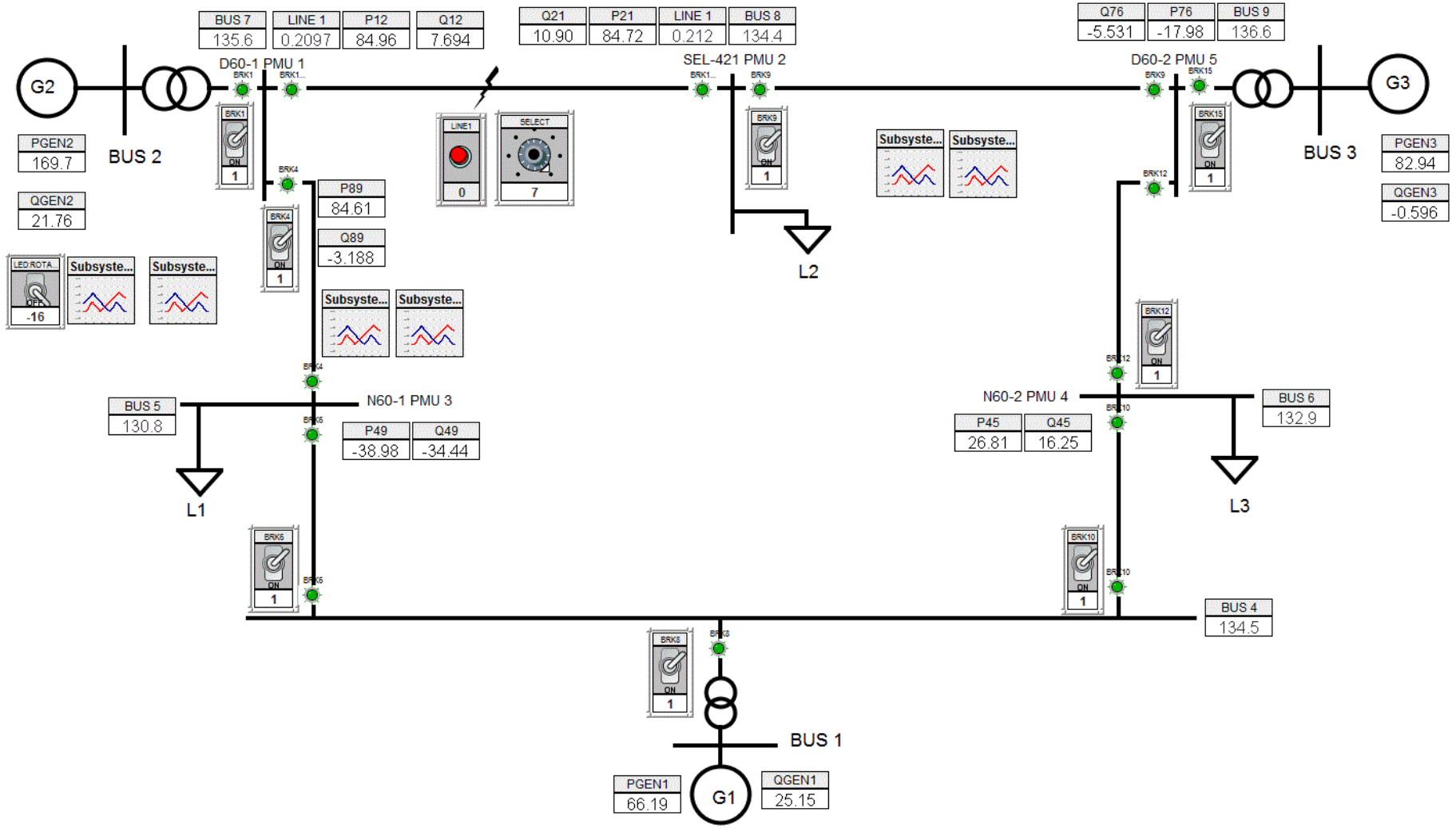
- Intrusion detection systems (IDS) use sensors to learn system state.
- Synchrophasor is a new sensor for power system IDS.
  - Redundant information
  - High granularity

Power system models



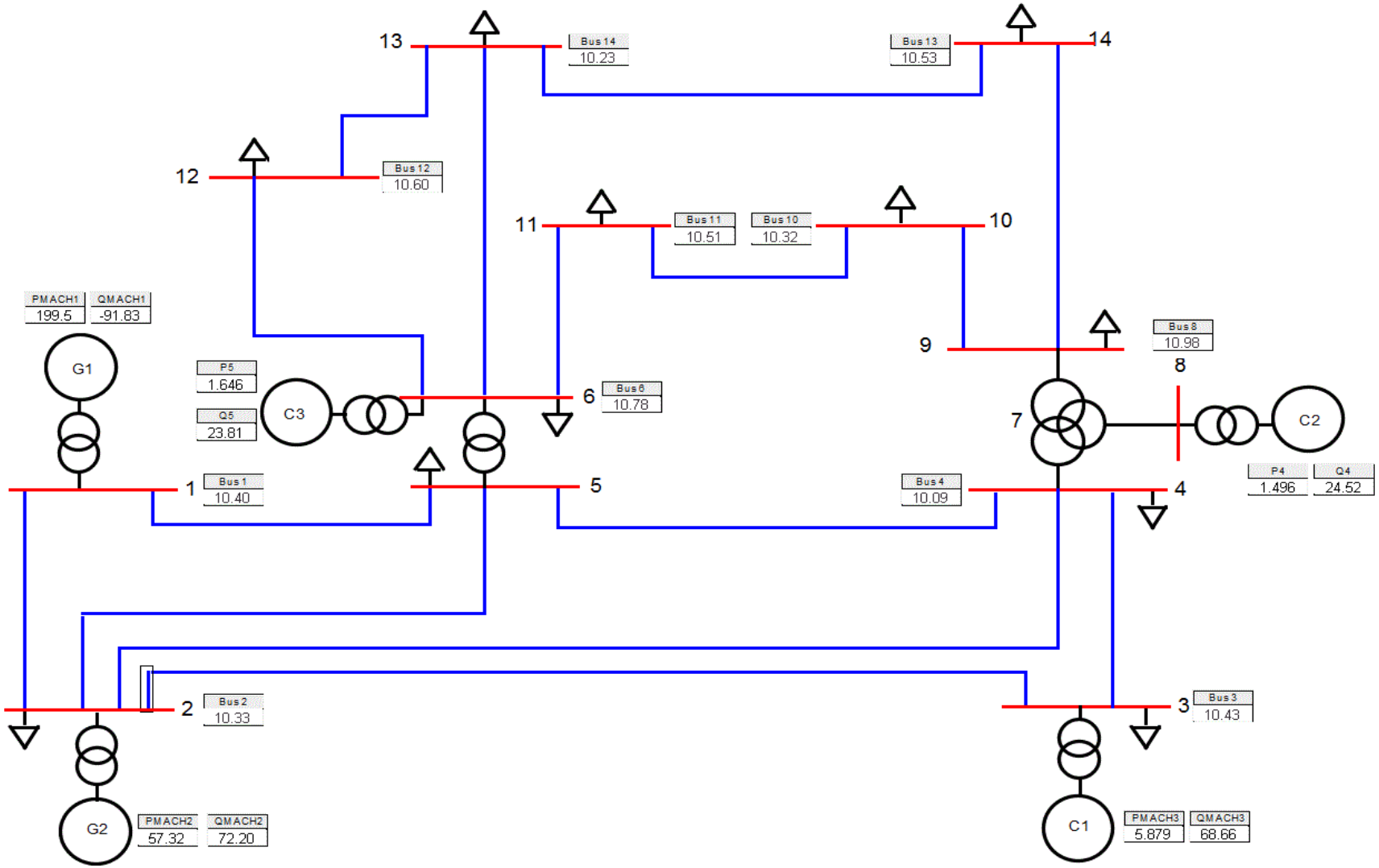
Three generator four bus system

Power system models



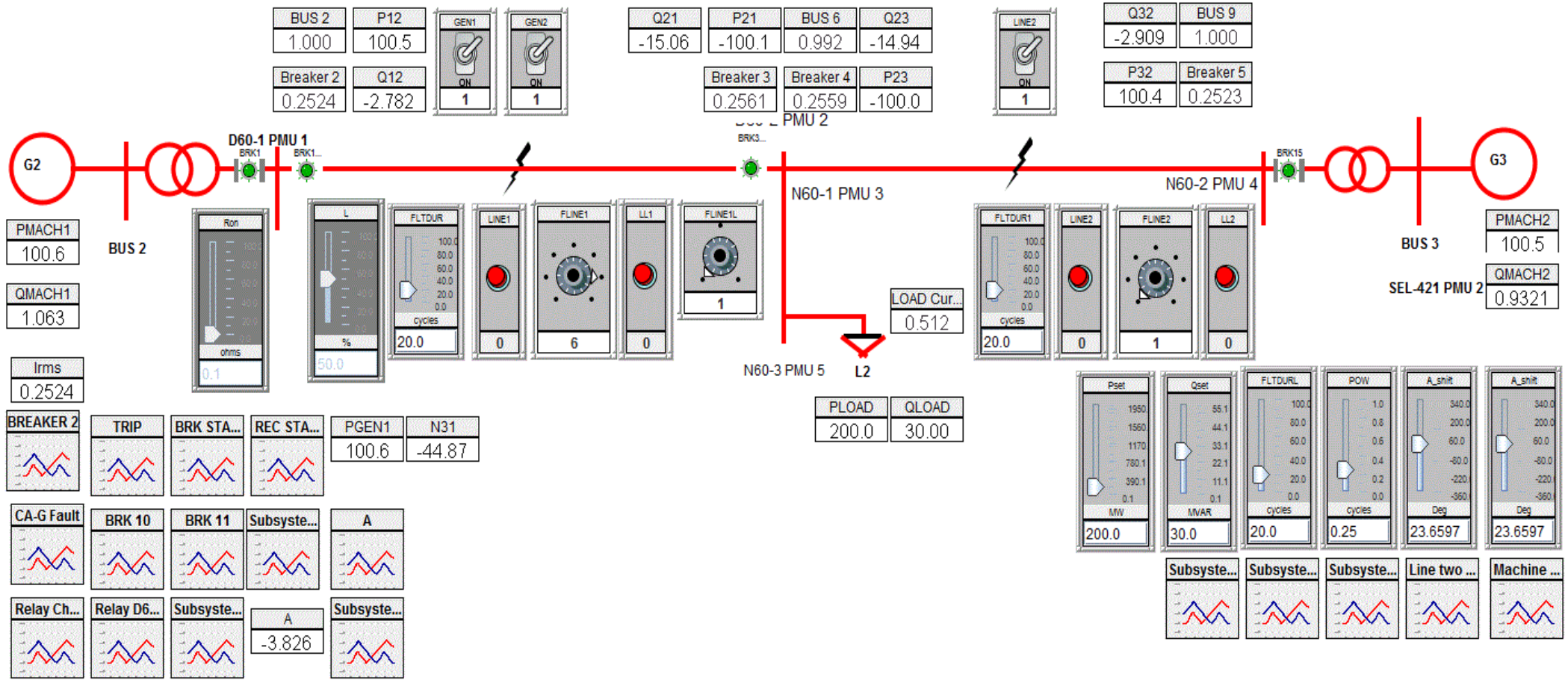
IEEE 9 bus system

Power system models



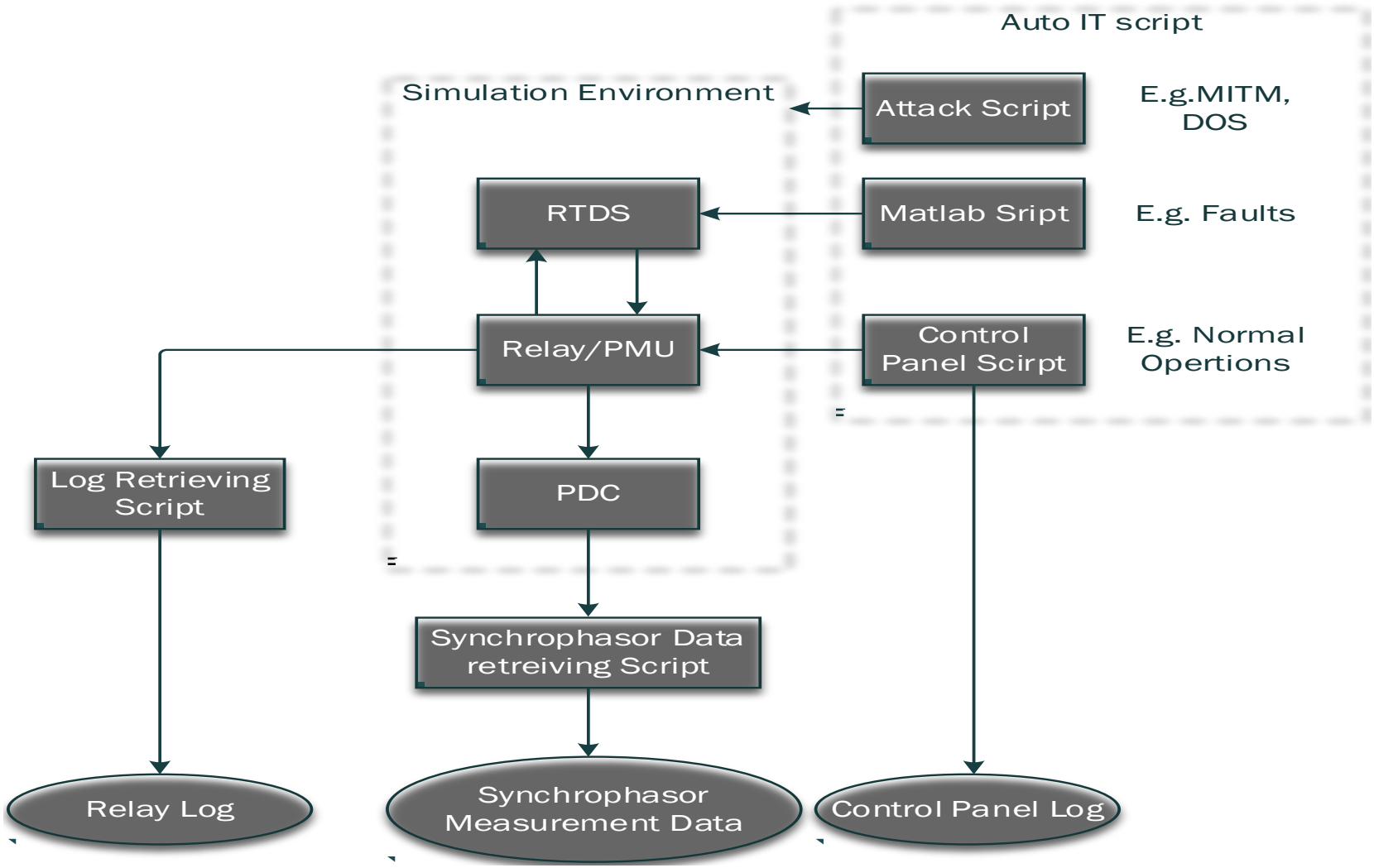
IEEE 14 bus system

Power system models



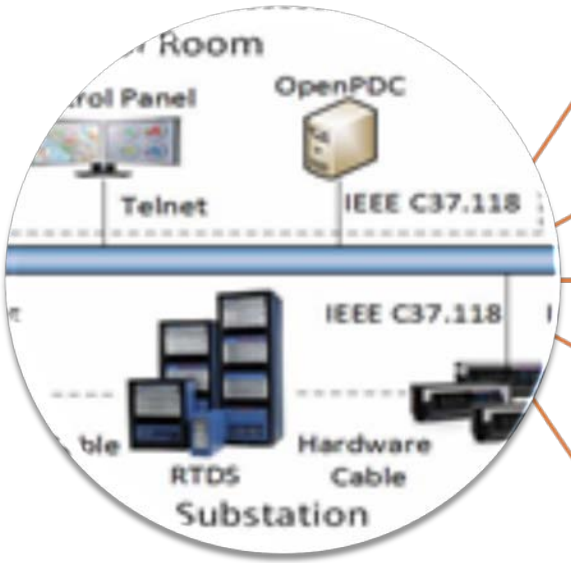
Modified two generator three bus system

Simulation control and data processing



- Auto IT = windows clicker script
- Auto IT calls sub-functions in random order
  - Attacks
  - Faults
  - Control actions
- Matlab interfaces with RSCAD
  - execute fault at 1% increments
  - change load, generation
- Control panel script
  - trip relays for maintenance

Data collected



- PMU
  - V, I, F, dF, P, Q
- Relays
  - Breaker Status, Events
- EMS
  - Maintenance logs, Control logs
- MATLAB RSCAD
  - Impedance
- Snort
  - Network Activities, Flags, logs, Alarms

- All data sources time stamped
- Merged comma separated data sets

- Data captured during steady state, disturbances, control actions, and attacks

- Simulated 10000 instances of 41 total scenarios in random order
  - PMU sample rate 120 samples per second
  - 38 GB

Power system and attack scenarios

Attacks

- Remote trip relay(s)
  - replay MODBUS packets
  - mimics line maintenance
- Altered PMU data
  - mimic relay not operating for fault
- Altered PMU data + remote trip to impersonate fault
  - man-in-the-middle IEEE C37.118
  - mimic fault
- Disabled relay
  - replay MODBUS packets

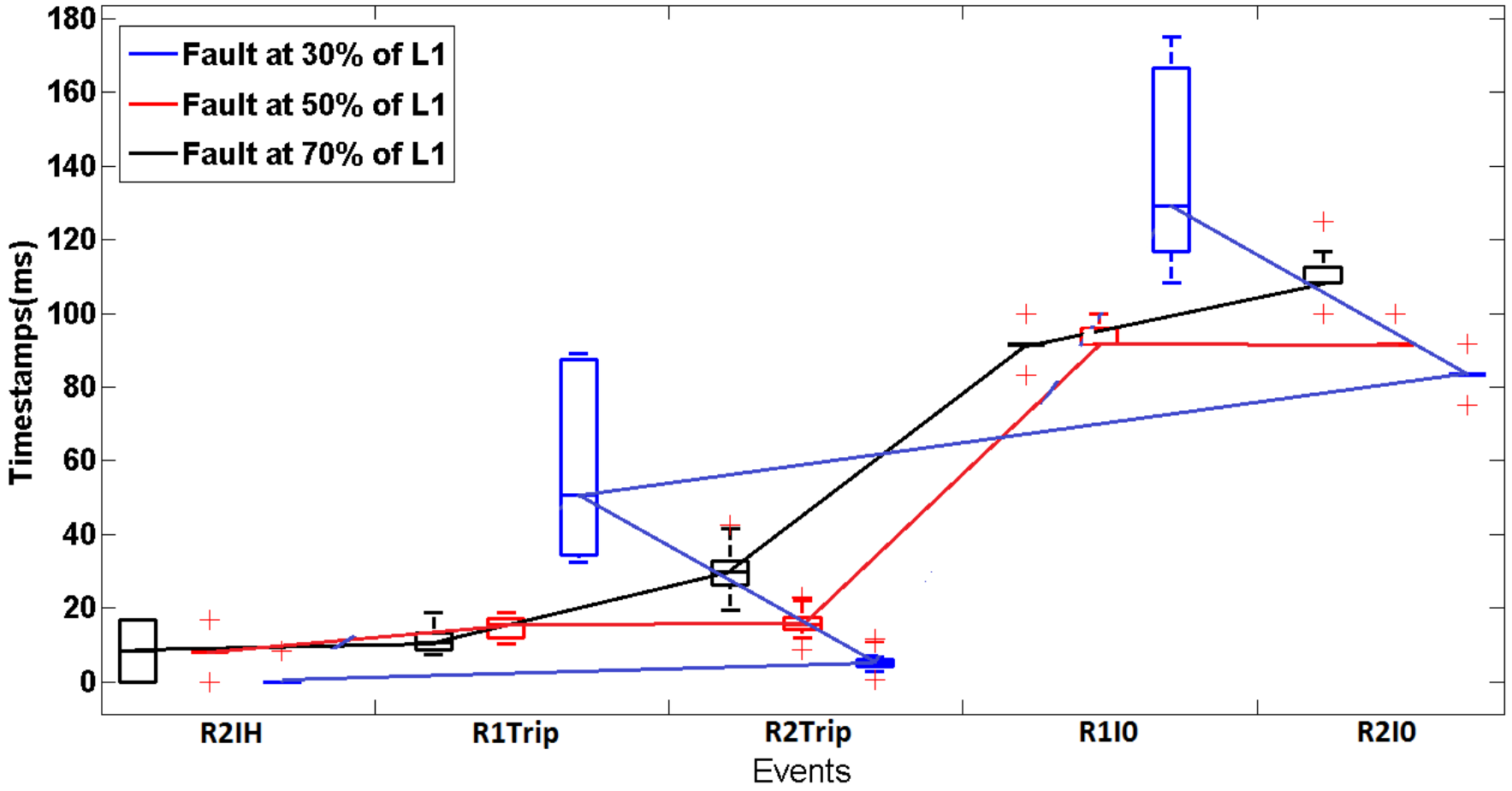
Disturbances and Control Actions

- Transmission line maintenance
- SLG Faults
  - random location
- Load variation
  - periodic random load changes

Data sets for anomaly detection

- Collaborating with Justin Beaver and Raymond Charles of Oak Ridge National Laboratory
  - Feasibility of using machine learning algorithms to classify behaviors
  - Evaluate common classifiers available in WEKA
    - Each scenario stand alone
    - Grouped scenarios
      - Steady state + disturbances + control actions vs. attacks
      - Normal vs. disturbances + control actions vs. attack
  - Most promising results come from grouped scenarios.
  - Approx, 90% accuracy.

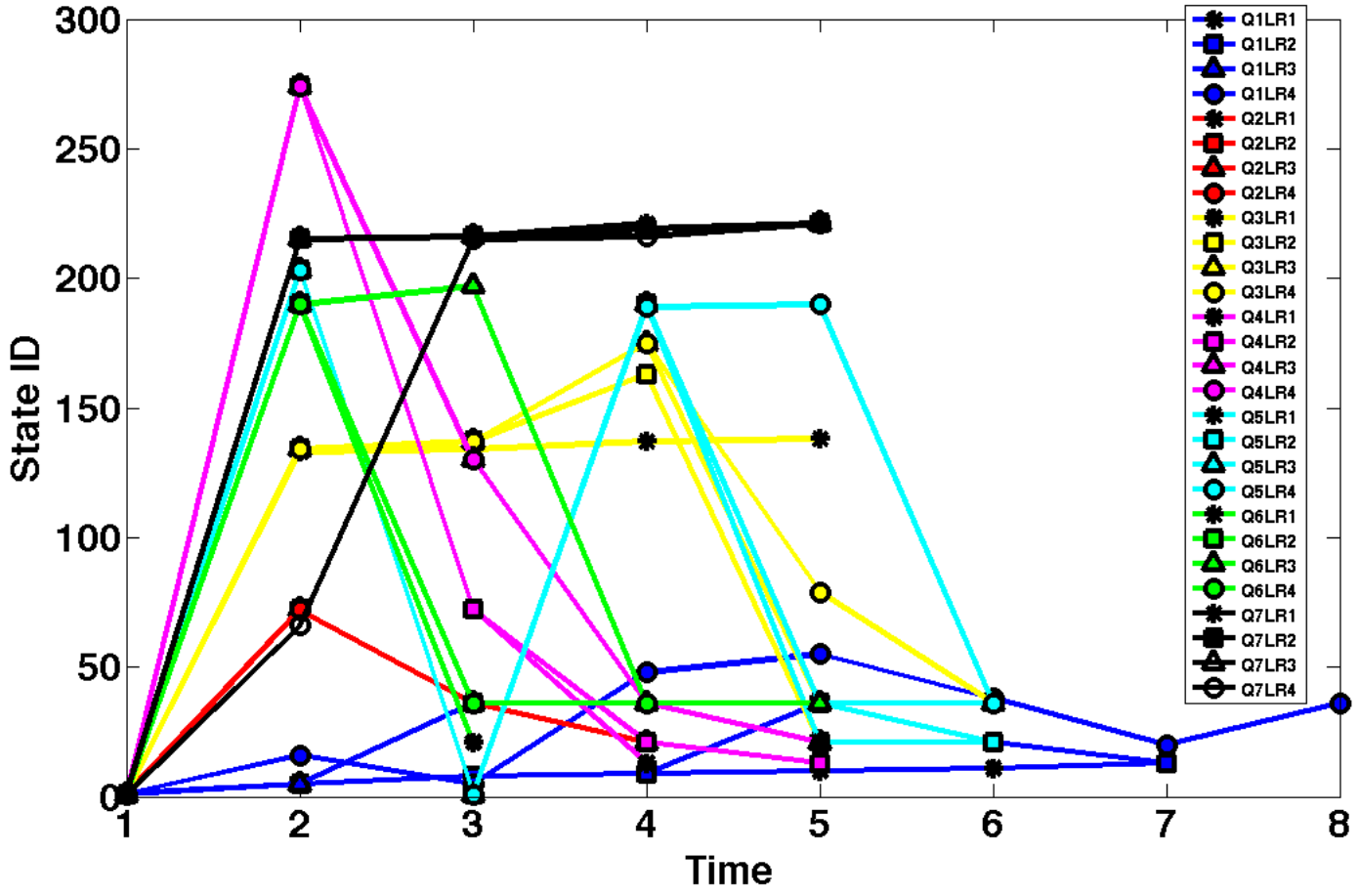
Event order provides signature effect



We call signature which includes multiple states over time a “path”

Auto path detection

- Automatically detect paths from data logs
- State ID represents unique set of measurements across all sources (PMU, relay log, Snort, control panel log)
- Difficulty minor variations lead to many paths for same sc
- Data mining to discover "comm
- Currently approaching 90% accuracy



Final Challenge

- Build the IDS
  - incorporates data from all sources
  - real time classification and alerts
  - currently we are limited to offline classification