Craig Rieger, INL, PI

John Bell, Dylan Reen, Pierce Russell, Justin Welch, INL Team

Brian Johnson, UI, Lead Prof.

Milos Manic, VCU, Lead Prof.

Jeff Pack, Power Engineers

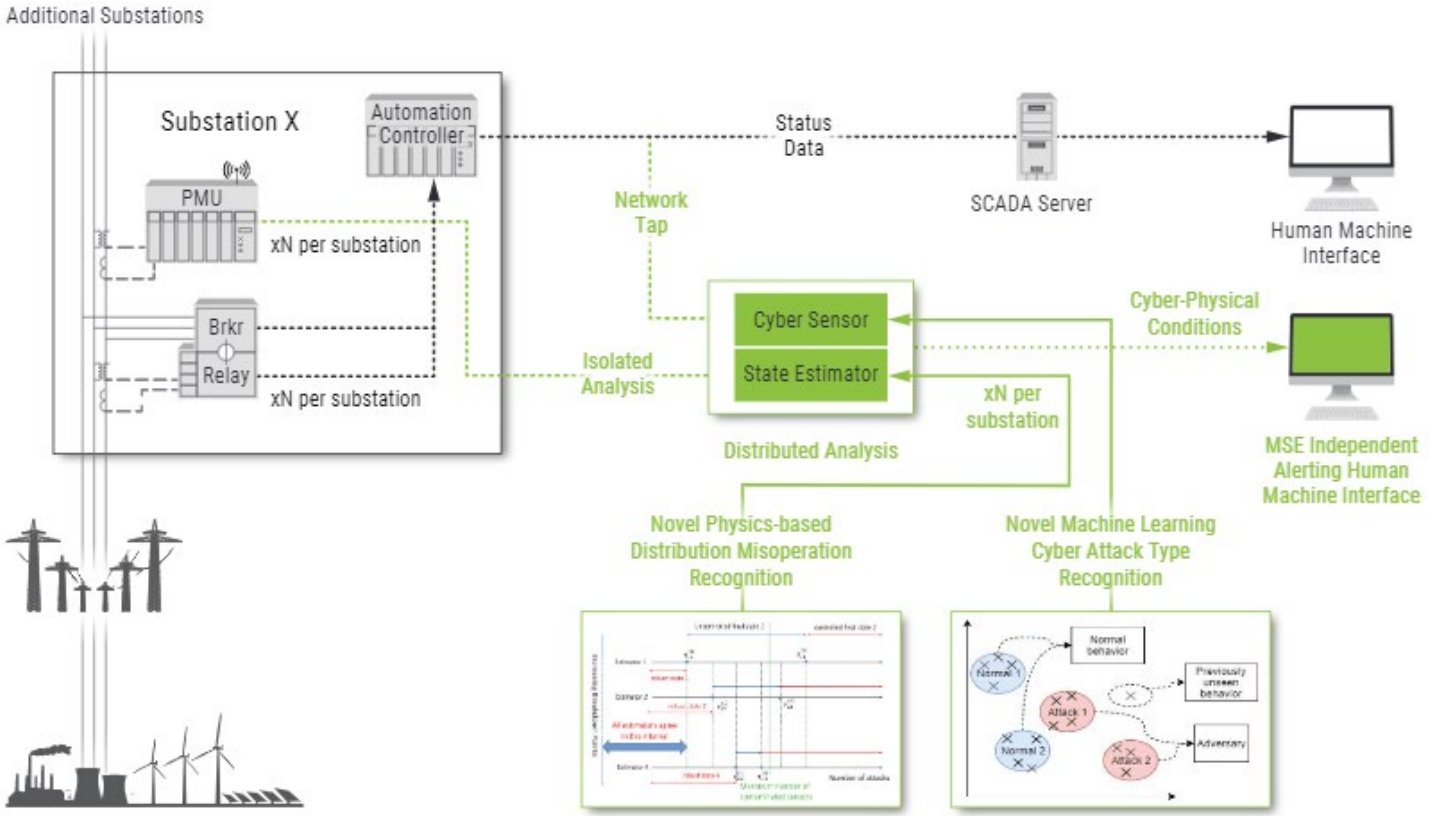
July 13, 2022

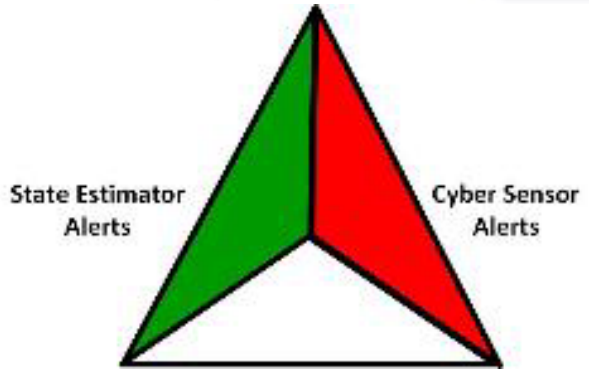
Master State-awareness Estimator (MSE)

Idaho National Laboratory

MSE Detailed View

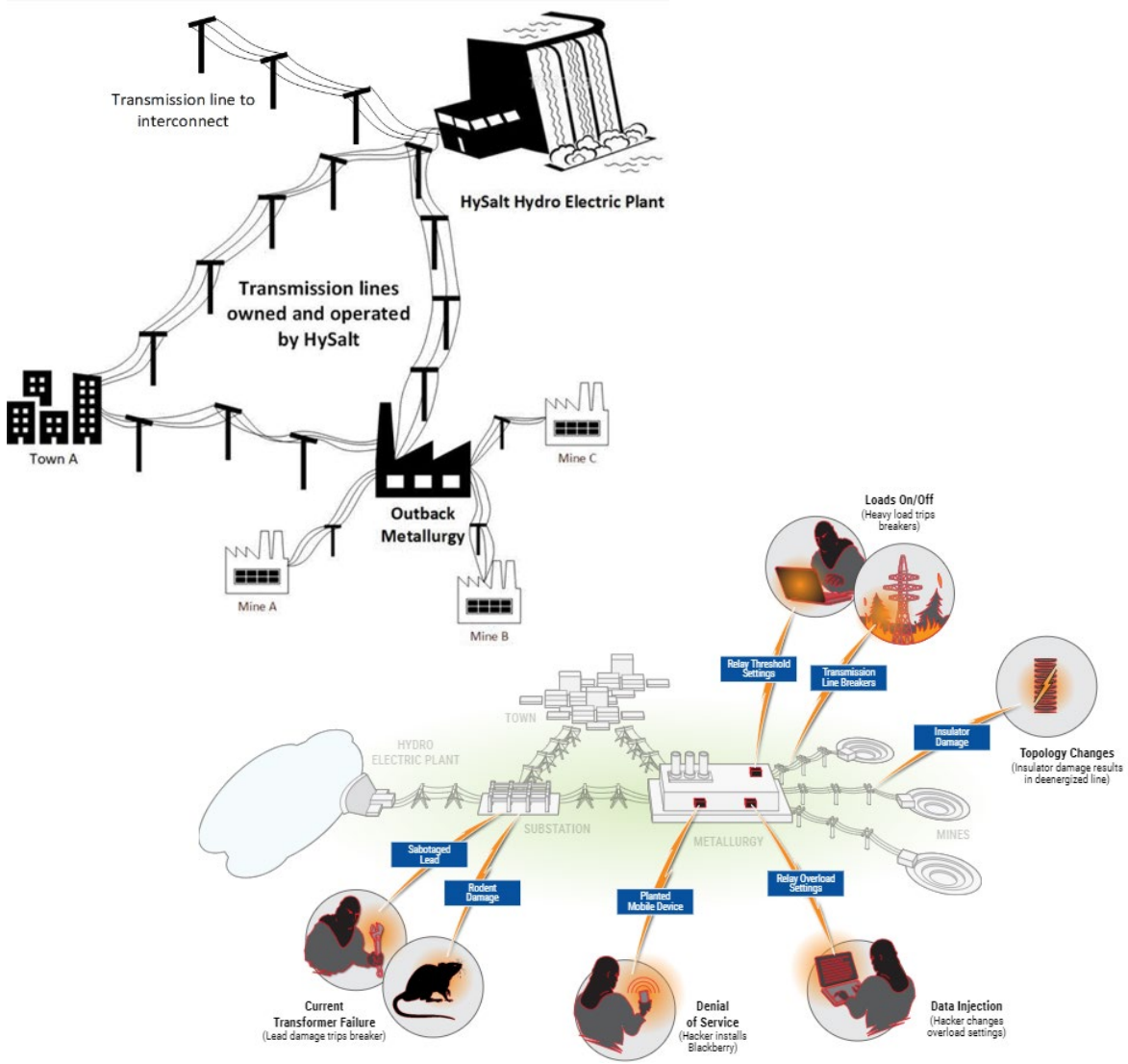
- **Cyber-Physical Integrated Analysis**
  - Independently evaluates cyber and physical information, through network and state estimation analyses
  - Sits on a network that is out of band from substation
  - Network analysis passively monitors isolated network, in addition to substation network, baselining normal traffic
  - State estimation analysis collects information out of band from phasor management units (PMUs)
- **Response**
  - Informs human machine interface (HMI) of bogus state and root cause of issue
    - The triad flashes red relative to recognized cyber sensor or state estimator alert
    - Prevents operator and device-initiated cascading failures through phased approach





Cyber-Physical Scenario Relevance

- HySalt Energy (HE) is a major power company that works in the generation and transmission across several parts of the national grid.
- As a result of their responsibilities, HE employees have direct access to several critical assets, including protection and control system devices.
- Cyber scenarios could entail a disgruntled employee, such as the engineer who programs their protection coordination devices but is declined continued employment.
- Physical scenarios could entail transmission line faults or nefarious manipulation of a substation equipment. The initiator of the physical scenarios could entail a forest fire near the transmission lines.

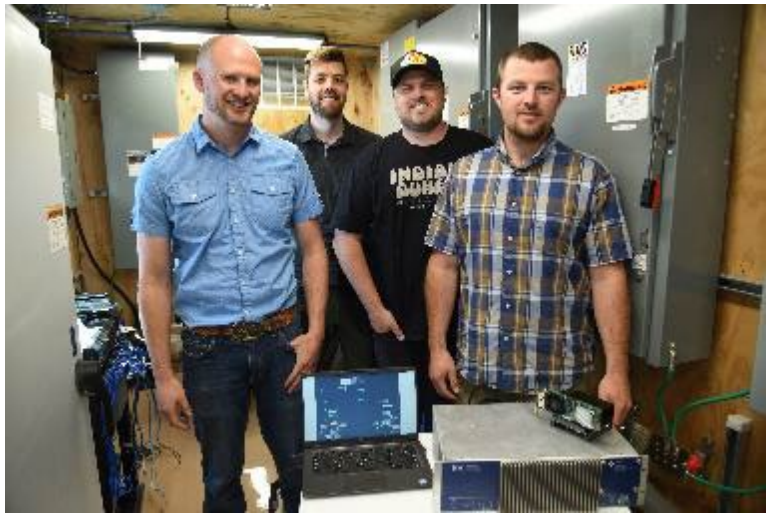


Cyber Test Scenarios

- **Detect data injection attack**
  - A successful log in to the relay at a level high enough to implement a settings change, change the CT ratio settings, then the MSE will be tested to verify it can sense a settings change.
  - A successful test will show that the MSE anomaly sensor detected the settings change.
- **Detect failed log in attempt**
  - The anomaly sensor will build a system baseline and understand what ‘normal’ looks like.
  - Once the MSE anomaly detection device is running, a log in with incorrect passwords will be attempted.
  - The test will be a success if the anomaly detection device detects the failed log in.
- **Detect denial of service (DOS) attack**
  - Once the MSE anomaly detection device is running a DOS test will commence using cyber flooding tools.
  - This will overload the communication to and from the protection device, verifying the MSE anomaly sensor is able to detect as a minimum, the creation of an abnormal traffic latency.
  - The test will be a success when a latency is noticed by the MSE algorithm. The anomaly detections system will also be able to notice a change of network traffic and report an error.

Physical Test Scenarios

- **Test the accuracy of the MSE estimator to detect emulated false data attack**
  - Adjust the current transformer ratio settings on a protective relay device such that it is producing inconsistent measurements.
  - A successful test will be the MSE sending an alert because the relay is consistently sending faulty data, based on the surrounding PMU monitoring devices.
- **Test the accuracy of the MSE at tracking system load/generation changes and resulting system state**
  - Implement change in load – switch load off-line or on-line.
  - The resulting change will cause voltage magnitudes and angle to change as well as power flows.
  - State estimator should correctly track these changes.
- **Demonstrate the ability to sense large changes in topology**
  - A recloser will be opened, changing system topology from a loop to two radials feeders. The MSE will monitor PMU data. The recloser will be closed to restore a loop.
  - The MSE should see a change in the flow of power above a detection threshold based on the PMU and signal an alert that the topology has changed.



Cyber Scenario Demonstrations

(Linked Demonstration Video)

Physical Scenario Demonstrations

(Linked Demonstration Video)


INL
Idaho National Laboratory