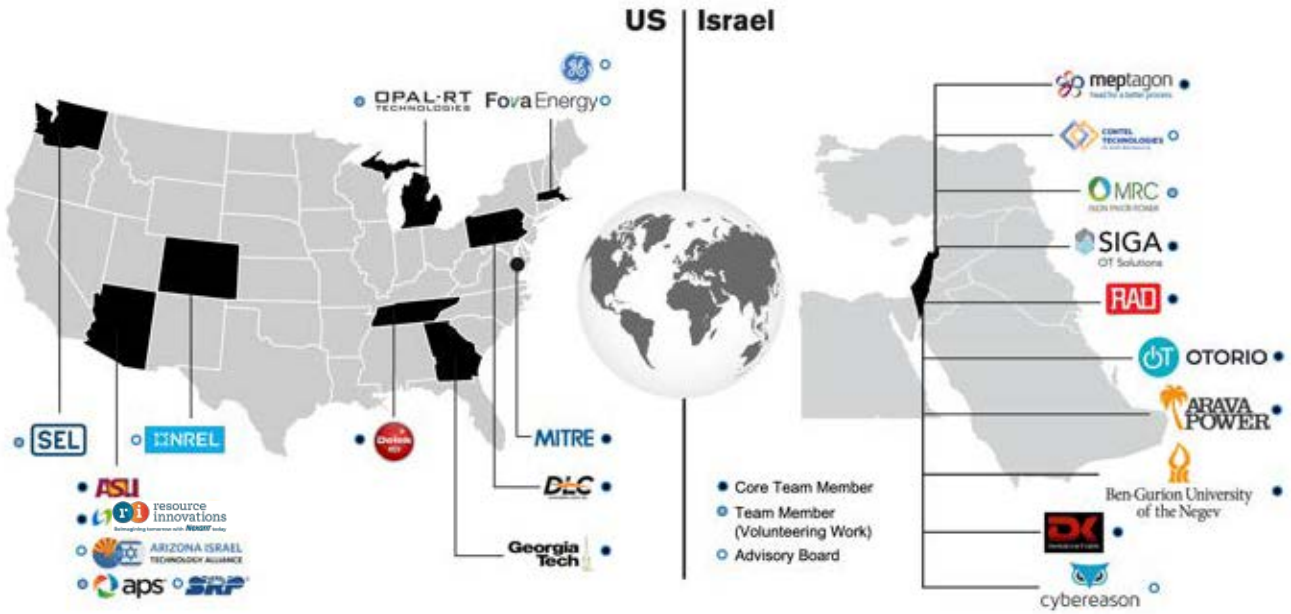
BIRD-ICRDE Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience

BIRD
Israel-U.S.
Binational Industrial Research
and Development Foundation

U.S.-Israel
Energy Center



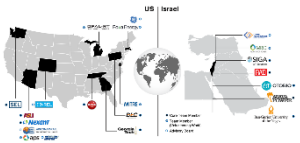
Converging Cybersecurity Solutions for Energy Systems to Practice

Grid360 Platform for Cybersecurity Threat Simulation, Detection, and Mitigation

John Dirkman P.E.
VP Product Management
Resource Innovations
jdirkman@resource-innovations.com

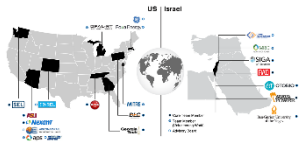
1 March 2022

Webinar Agenda



1. Grid360 Overview
2. Commercialization Approaches
3. State Estimation Applicability
4. Q&A

Grid360 Overview

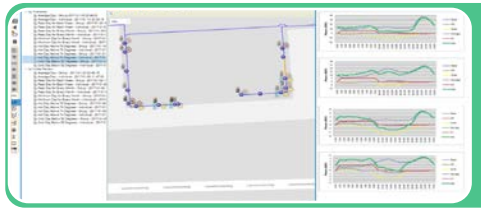


State estimation, optimal power flow, contingency analysis, fault analysis

- Determine the current operating state of networks using AMI/SCADA/sensor data, discover and eliminate data/topology/latency errors, and recommend sensor placement
- Calculate and display system loading and voltage warnings and violations, including contingency analysis, calculate fault level, run optimizations, generate alerts, recommending switching, and dispatch resources

Analysis of DR, DG, DER, PED, EV, microgrids, improved customer engagement

- Evaluate the current and near-term energy and economic state of distribution grids including demand response (DR), distributed generation (DG - solar and wind, including smart inverters), distributed energy resources (DER - energy storage), power electronic devices, electric vehicle (EV) supply equipment, microgrids, volt/VAR optimization (VVO), and Grid Interconnection programs, improving customer service



Load profiling, short-term, and long-term load and DER forecasting

- Create load profiles, develop short-term (days ahead) and long-term (months to years ahead) energy and economic forecasts including DR, DG, DER, PED, EV, and microgrids
- Generate alerts and dispatch resources based on forecast conditions

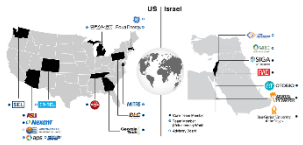
Management of independent grids and microgrids, reliability coordination/market operations

- Manage independently-owned commercial and industrial grids and microgrids
- Coordinated capacity calculation and security analysis, outage planning coordination, short- and medium-term adequacy forecasts

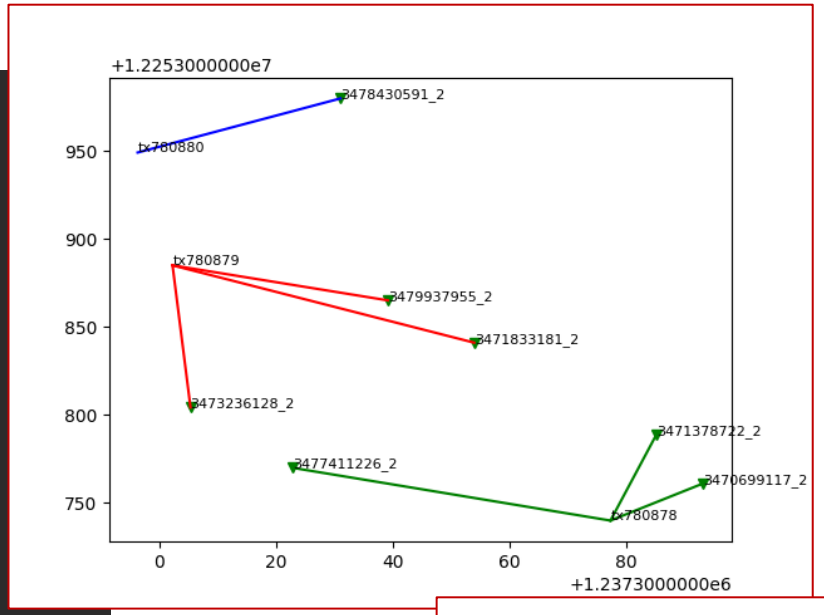
Advanced security, data quality, and reliability analytics

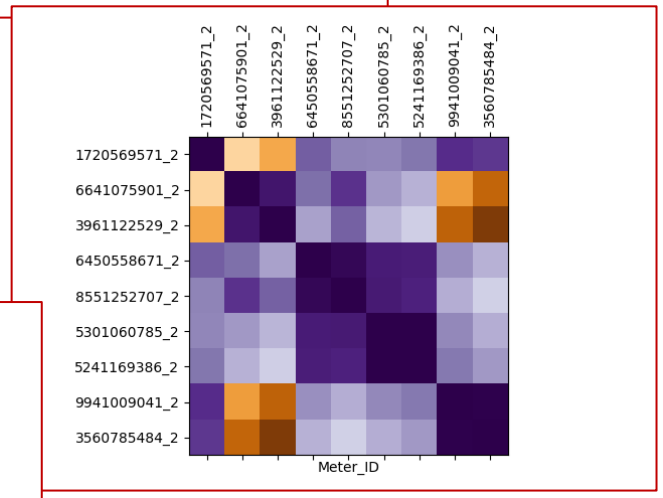
- Track critical and vulnerable assets, communication channels, protocols and encryption, patches and mitigations, ownership, and access and safety
- Analyze and improve transformer to meter assignment, phase assignment, sizing of devices and conductors, asset health forecasting, energy theft, outage causes and prediction, and other data quality and operational factors based on AMI/SCADA/sensor data and network models

Commercialization - ASU Topology Processor Engine



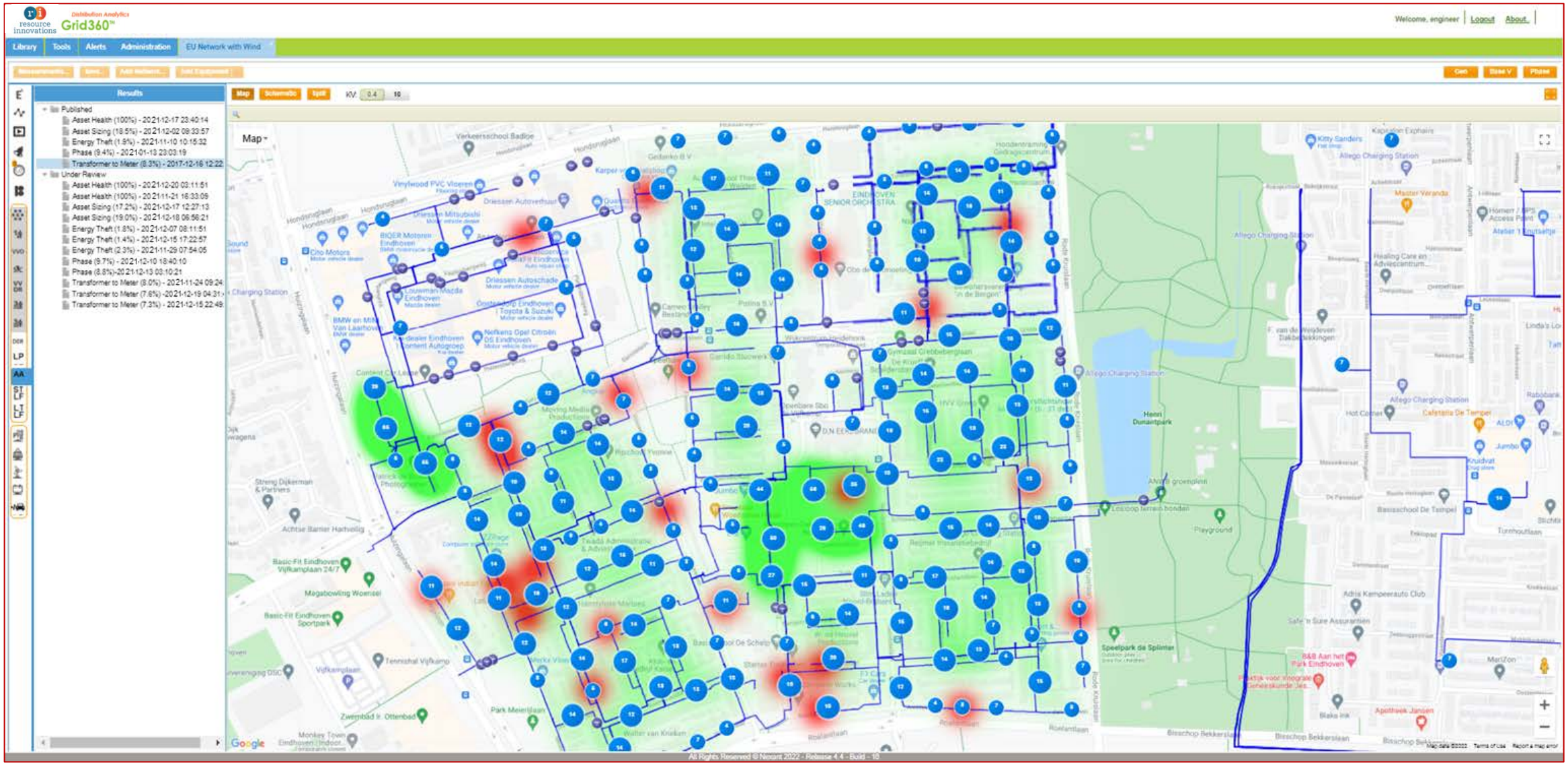
```
print("Extracting Connectivity from OpenDSS models")
# os.chdir("APS_model/")
exec(open('1connectivity_extract.py'.encode('utf-8')).read())

print("Extracting Grouped Loads Features from OpenDSS models")
os.chdir("..")
exec(open('2grouped_loads_features_extract.py'.encode('utf-8')).read())

print("Creating Distance Features")
os.chdir("..")
exec(open('3distance_features.py'.encode('utf-8')).read())

print("Generate Voltage Data using Connectivity and Consumption data and Extract it")
os.chdir("..")
exec(open('4vpu_extract.py'.encode('utf-8')).read())

print("Spectral Clustering to obtain clusters of meters corresponding to transformers")
os.chdir("..")
exec(open('5spectral_cluster_multiview_regular_merged2 - Confidence_Metric.py'.encode('utf-8')).read())

print("Computation of Accuracy and Generation of Complete Plot")
os.chdir("..")
exec(open('6spectral_cluster_accuracy_confidence_matrix.py'.encode('u

elapsed=(time.time() - t)
print('Total time for execution: %s seconds' %elapsed )
```





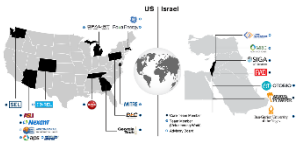
OUTPUT:
Total Number of Correctly Predicted Connections = 1514
Total Number of Incorrectly Predicted Connections = 70
Total Number of Connections = 1584
Total Accuracy [%]= Correct\Total * 100 = 95.5808
Total time for execution: 263.06036 seconds

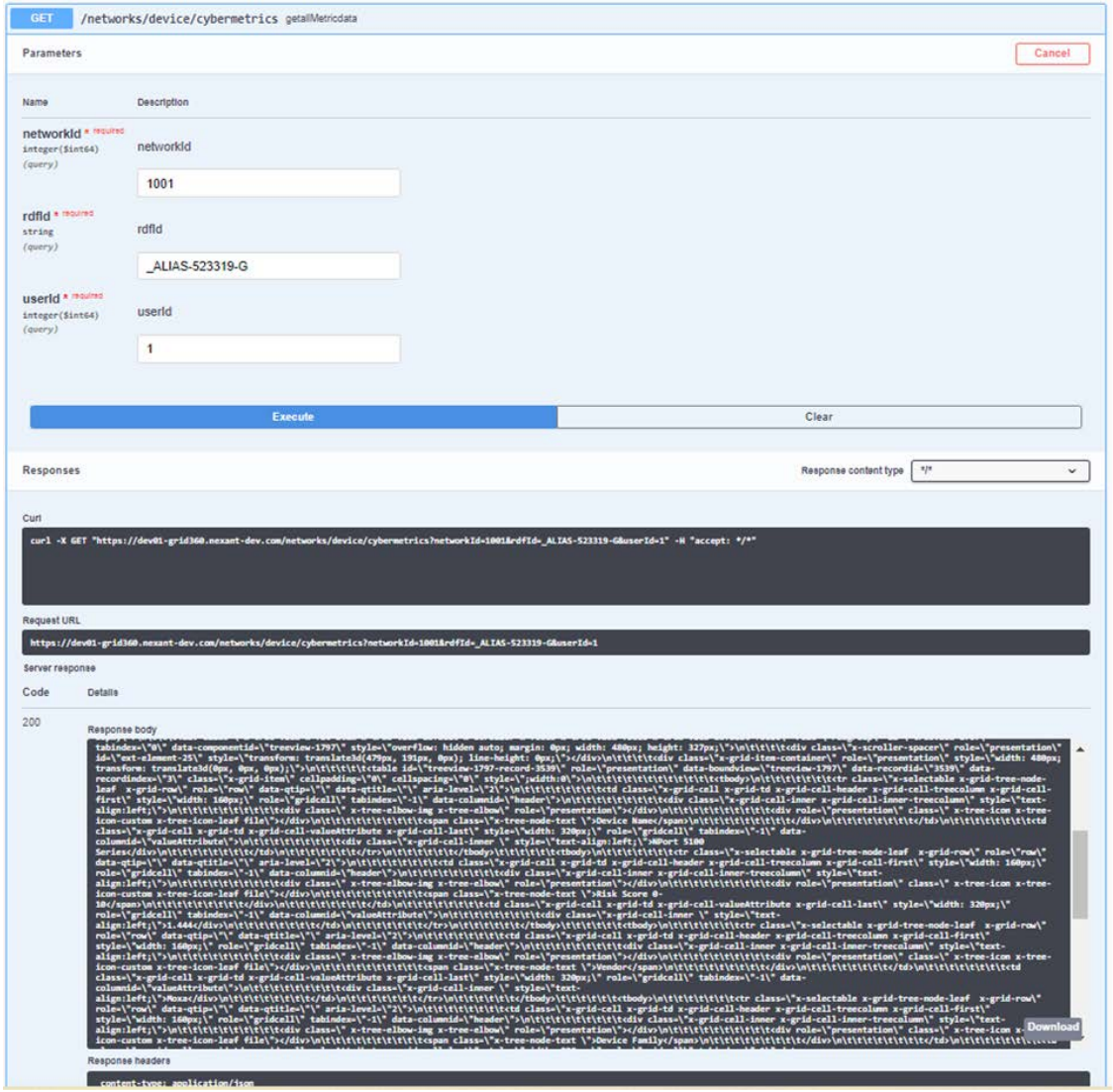
Commercialization - Topology Processor Visualization

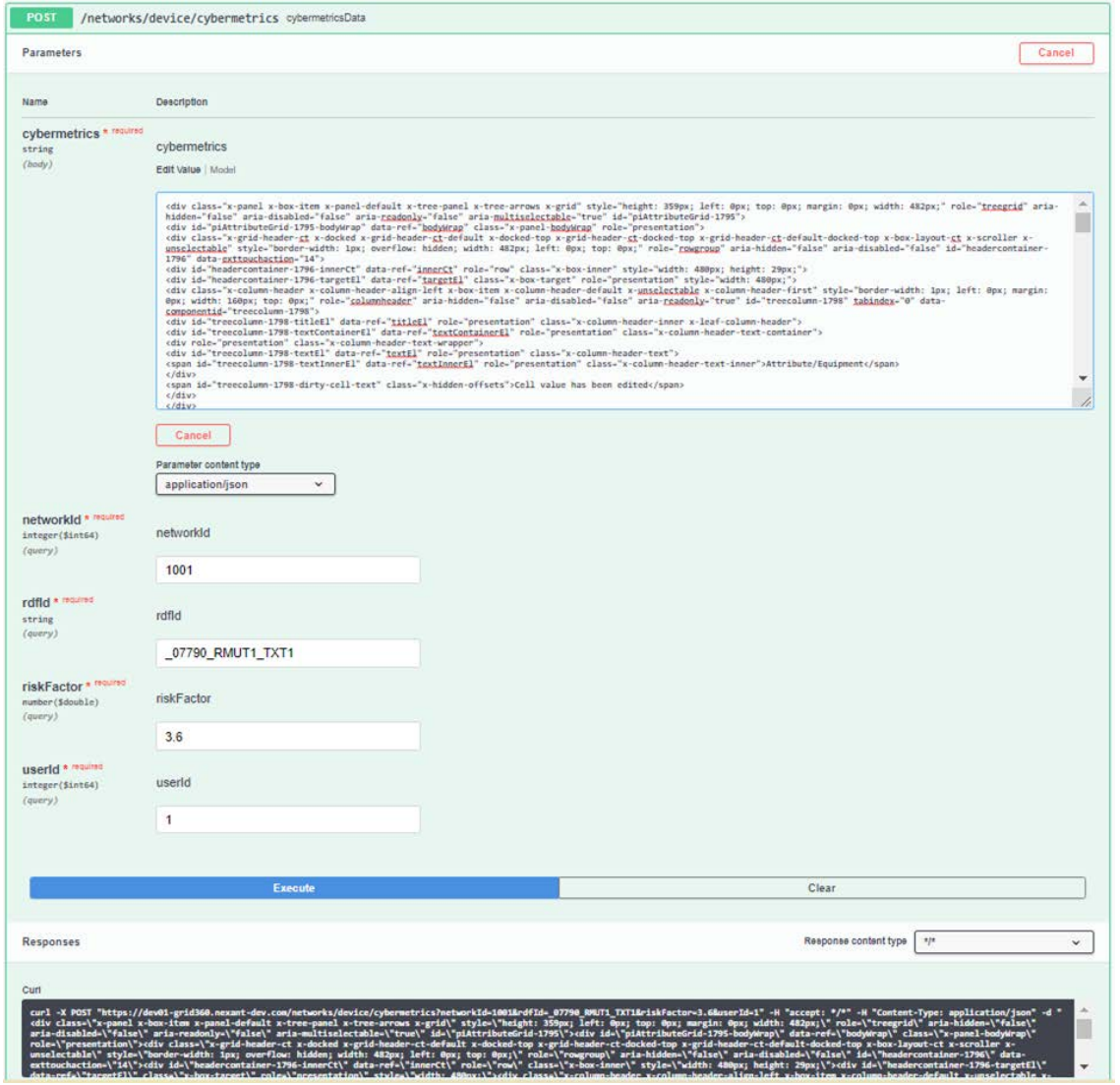


Commercialization - Cyber Metrics API

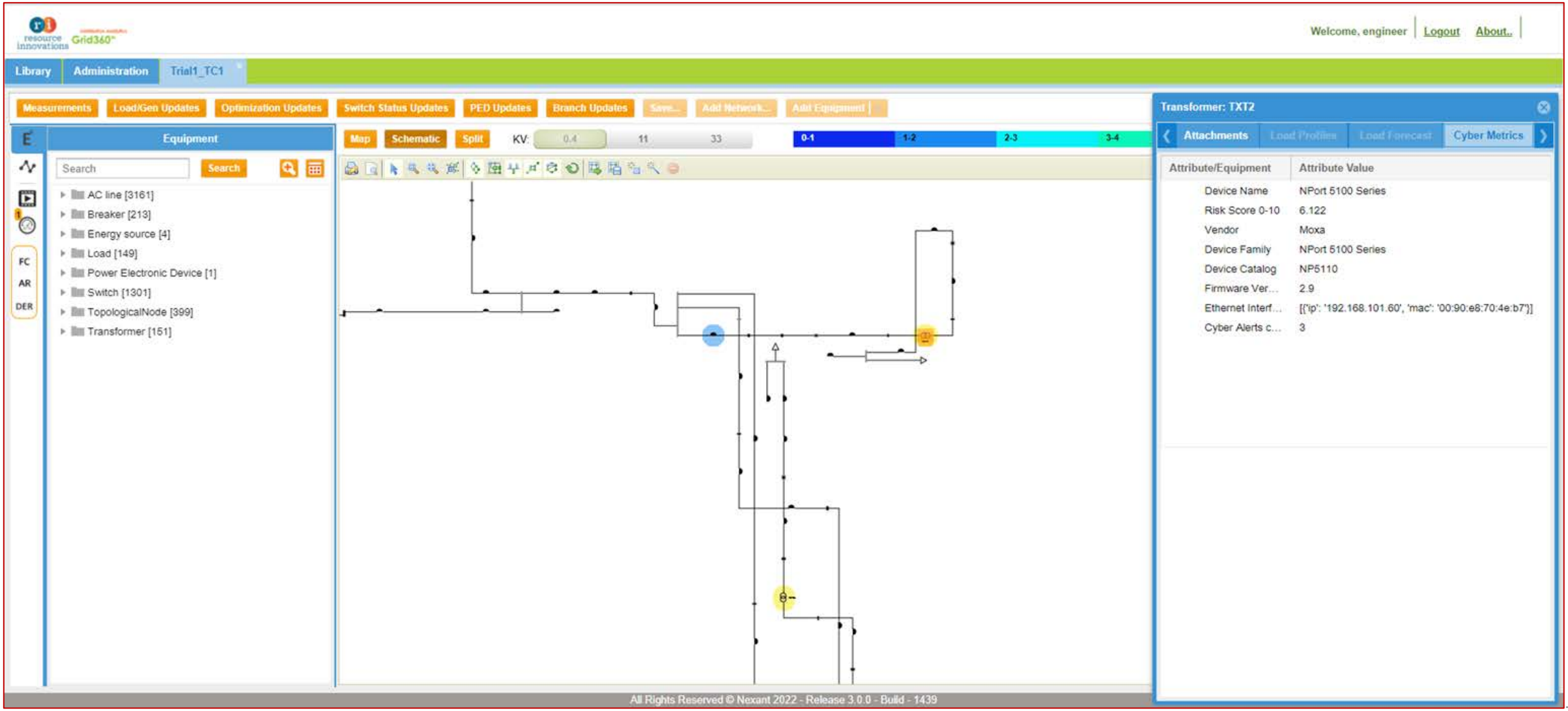
Grid360 APIs



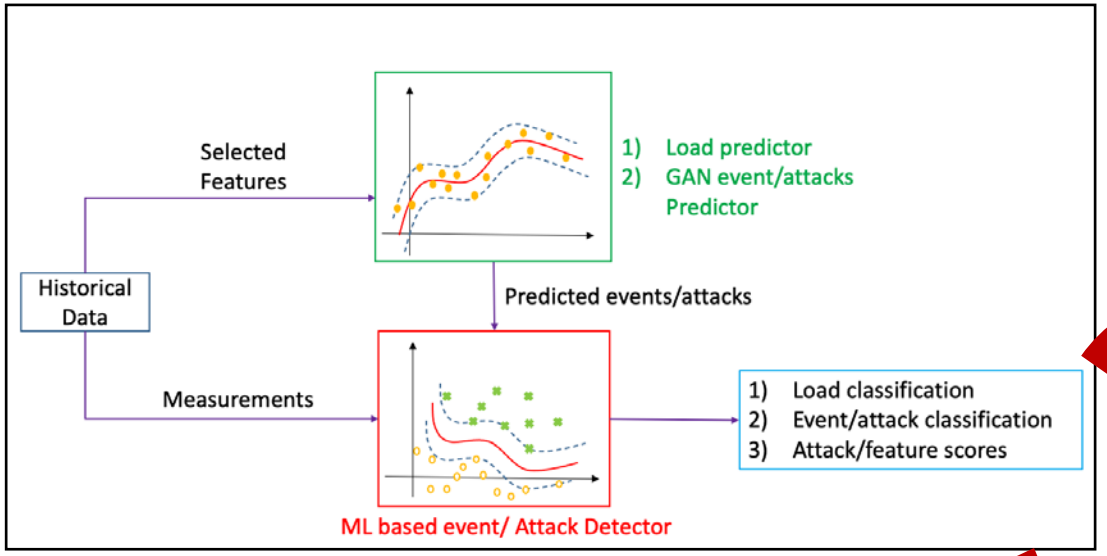




Commercialization - Cyber Metrics Visualization

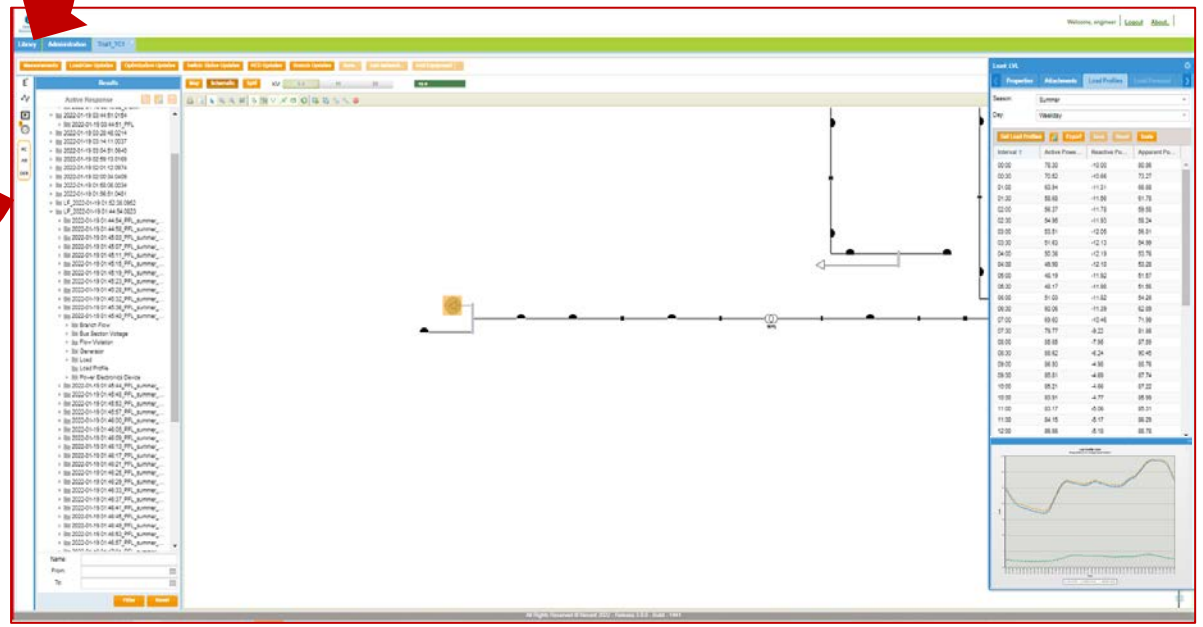


Commercialization – From Detection to Anomaly Visualization

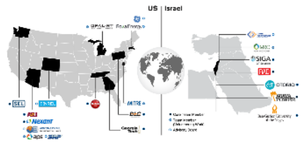


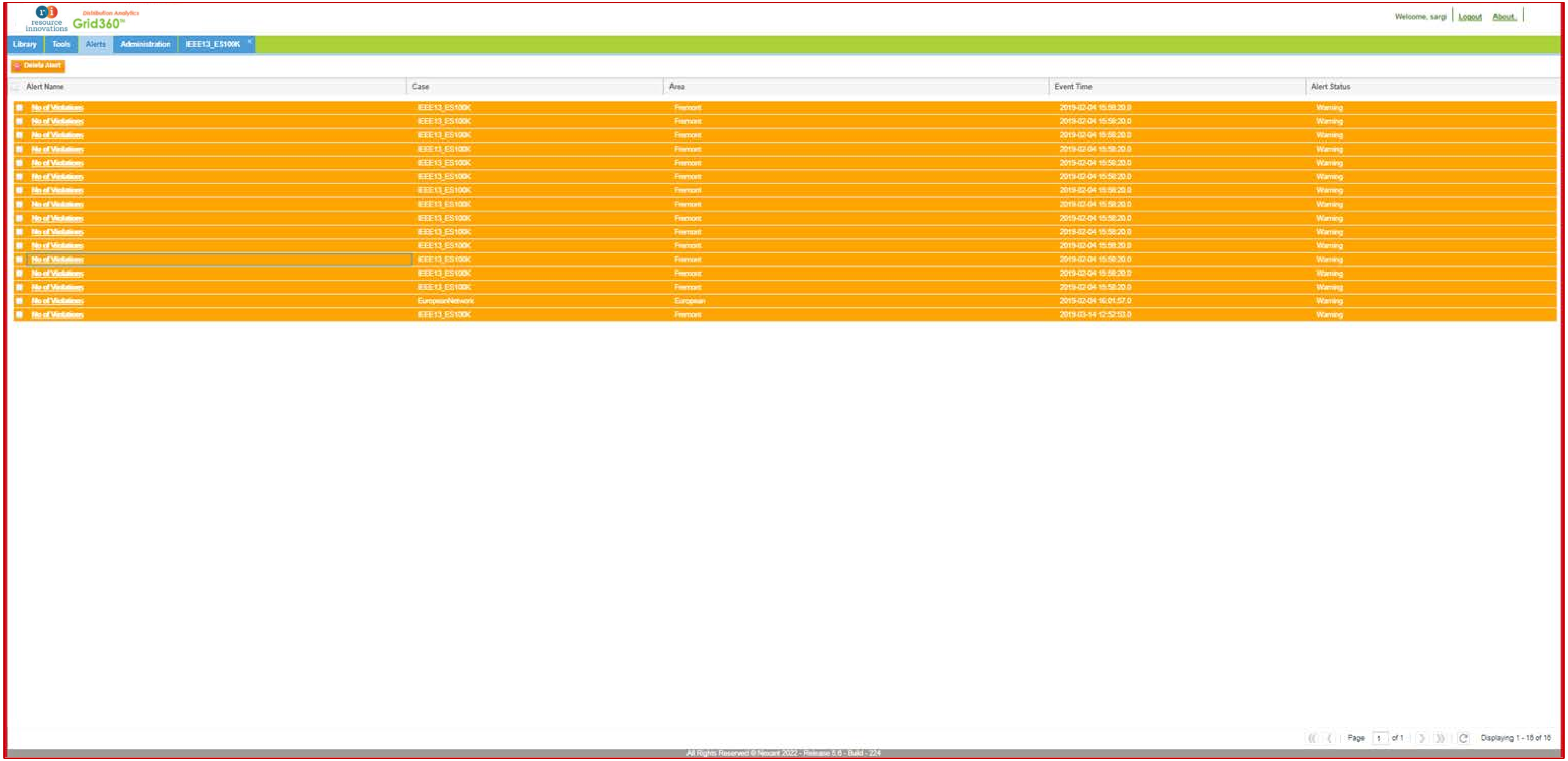
Intelligent and interpretable attack/event detector

RI Grid360: Load Anomaly Visualization

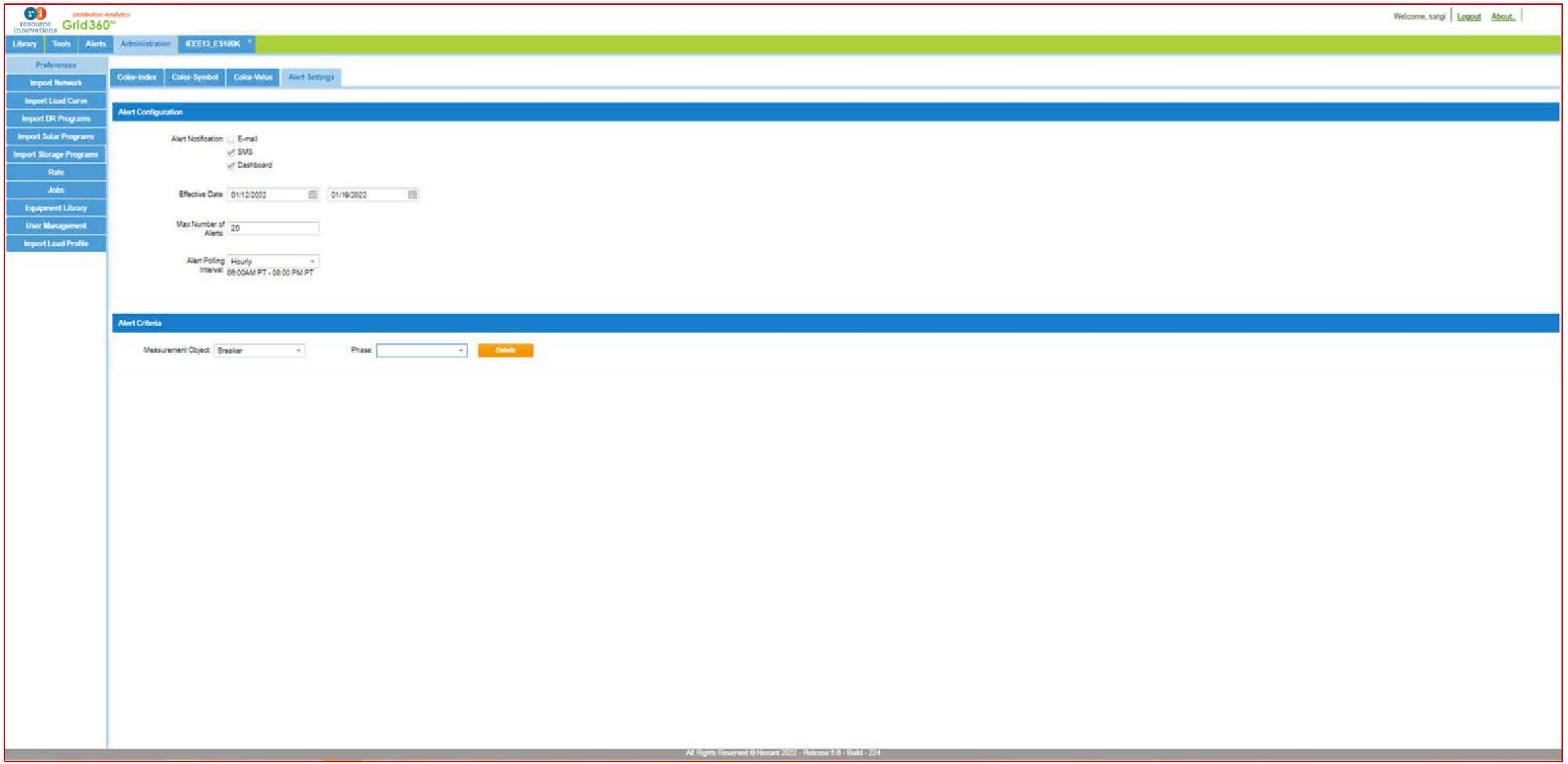


Commercialization - Alert Dashboard

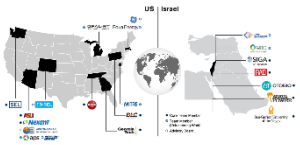


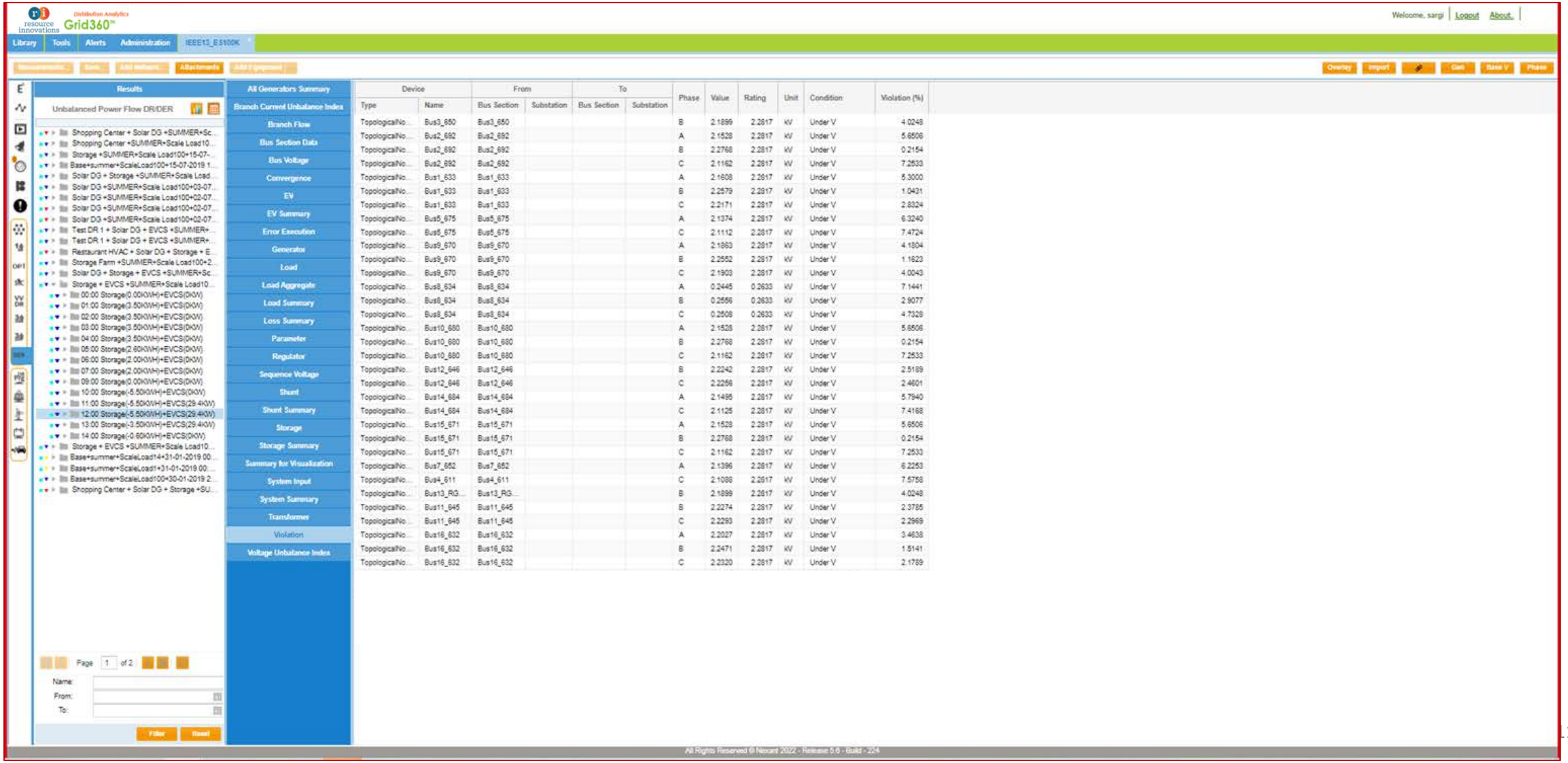


Commercialization - Alert Configuration



Commercialization - Violation Reports





Device		From		To		Phase	Value	Rating	Unit	Condition	Violation (%)
Type	Name	Bus Section	Substation	Bus Section	Substation						
TopologicalNo...	Bus3_650	Bus3_650				B	2.1899	2.2617	kV	Under V	4.0248
TopologicalNo...	Bus2_692	Bus2_692				A	2.1528	2.2617	kV	Under V	5.6506
TopologicalNo...	Bus2_692	Bus2_692				B	2.2768	2.2617	kV	Under V	0.2154
TopologicalNo...	Bus2_692	Bus2_692				C	2.1162	2.2617	kV	Under V	7.2533
TopologicalNo...	Bus1_633	Bus1_633				A	2.1608	2.2617	kV	Under V	5.3000
TopologicalNo...	Bus1_633	Bus1_633				B	2.2579	2.2617	kV	Under V	1.0431
TopologicalNo...	Bus1_633	Bus1_633				C	2.2171	2.2617	kV	Under V	2.8324
TopologicalNo...	Bus5_675	Bus5_675				A	2.1374	2.2617	kV	Under V	6.3240
TopologicalNo...	Bus5_675	Bus5_675				C	2.1112	2.2617	kV	Under V	7.4724
TopologicalNo...	Bus9_670	Bus9_670				A	2.1863	2.2617	kV	Under V	4.1504
TopologicalNo...	Bus9_670	Bus9_670				B	2.2552	2.2617	kV	Under V	1.1623
TopologicalNo...	Bus9_670	Bus9_670				C	2.1903	2.2617	kV	Under V	4.0043
TopologicalNo...	Bus8_634	Bus8_634				A	0.2445	0.2633	kV	Under V	7.1441
TopologicalNo...	Bus8_634	Bus8_634				B	0.2556	0.2633	kV	Under V	2.9077
TopologicalNo...	Bus8_634	Bus8_634				C	0.2508	0.2633	kV	Under V	4.7328
TopologicalNo...	Bus10_680	Bus10_680				A	2.1528	2.2617	kV	Under V	5.6506
TopologicalNo...	Bus10_680	Bus10_680				B	2.2768	2.2617	kV	Under V	0.2154
TopologicalNo...	Bus10_680	Bus10_680				C	2.1162	2.2617	kV	Under V	7.2533
TopologicalNo...	Bus12_646	Bus12_646				B	2.2242	2.2617	kV	Under V	2.5189
TopologicalNo...	Bus12_646	Bus12_646				C	2.2256	2.2617	kV	Under V	2.4601
TopologicalNo...	Bus14_684	Bus14_684				A	2.1486	2.2617	kV	Under V	5.7940
TopologicalNo...	Bus14_684	Bus14_684				C	2.1125	2.2617	kV	Under V	7.4168
TopologicalNo...	Bus15_671	Bus15_671				A	2.1528	2.2617	kV	Under V	5.6506
TopologicalNo...	Bus15_671	Bus15_671				B	2.2768	2.2617	kV	Under V	0.2154
TopologicalNo...	Bus15_671	Bus15_671				C	2.1162	2.2617	kV	Under V	7.2533
TopologicalNo...	Bus7_652	Bus7_652				A	2.1396	2.2617	kV	Under V	6.2253
TopologicalNo...	Bus4_611	Bus4_611				C	2.1088	2.2617	kV	Under V	7.5758
TopologicalNo...	Bus13_RG...	Bus13_RG...				B	2.1899	2.2617	kV	Under V	4.0248
TopologicalNo...	Bus11_645	Bus11_645				B	2.2274	2.2617	kV	Under V	2.3785
TopologicalNo...	Bus11_645	Bus11_645				C	2.2293	2.2617	kV	Under V	2.2969
TopologicalNo...	Bus16_632	Bus16_632				A	2.2027	2.2617	kV	Under V	3.4638
TopologicalNo...	Bus16_632	Bus16_632				B	2.2471	2.2617	kV	Under V	1.5141
TopologicalNo...	Bus16_632	Bus16_632				C	2.2320	2.2617	kV	Under V	2.1789

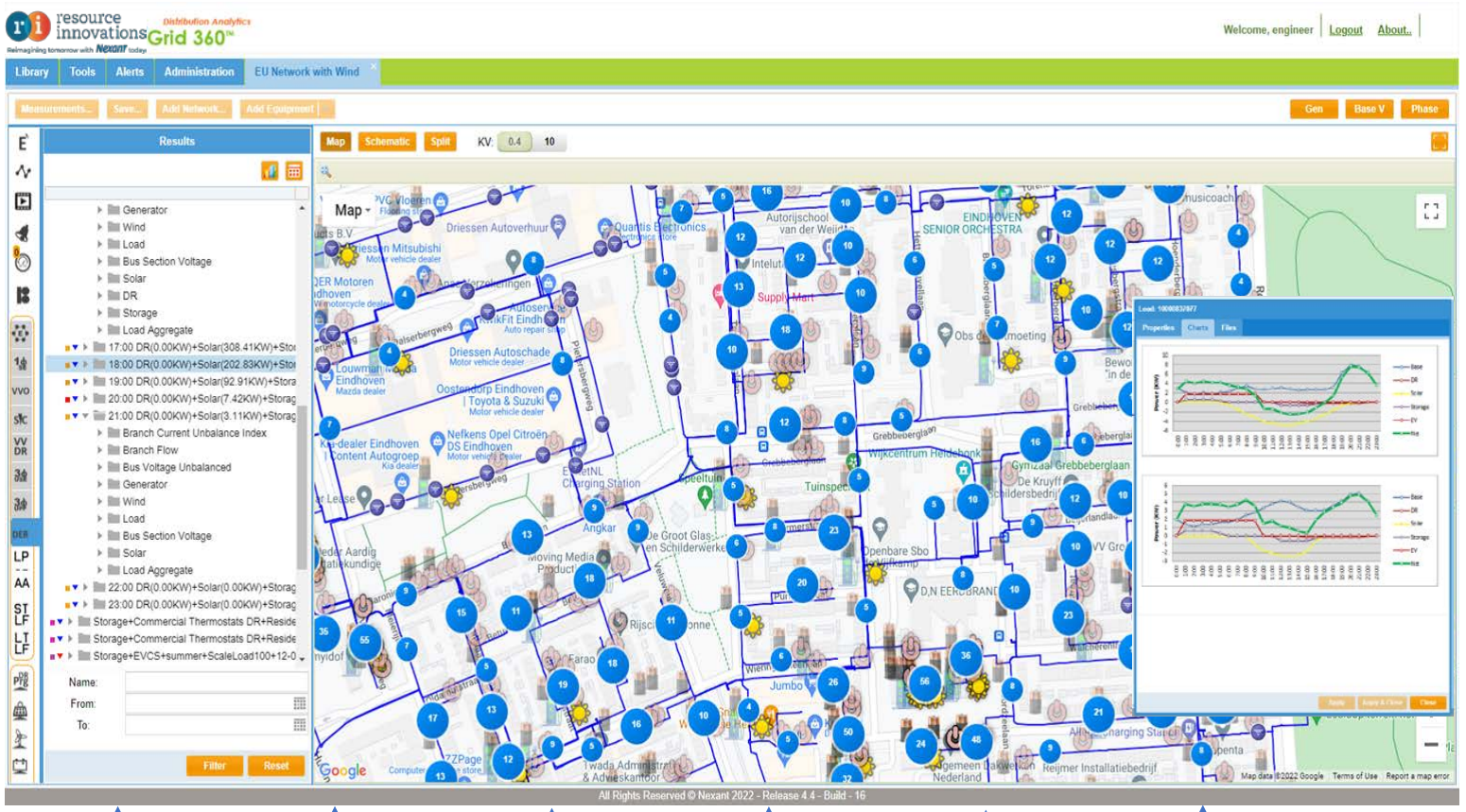
Commercialization - Software Deployment

Primary Markets:

1. Energy Management Systems (EMS)
2. Distribution Management Systems (DMS)
3. Supervisory Control and Data Acquisition (SCADA)
4. Programmable Logic Controller (PLC)
5. Industrial Control Systems (ICS)/Cyber-Physical Systems (CPS)
6. IoT devices

Integration/add on of new technology without need for wholesale replacement of systems/devices

Licensing mechanism is preferred



Malware Threat Mitigation

False Data Injection

Multilayer Anomaly Detection

AI based Intrusion Detection

Self-healing and Auto-Remediatin

State Estimation

Topology Processor

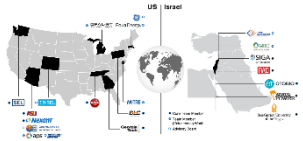
Forecasting

Optimal Power Flow

Contingncy Analysis

Fault Analysis

Commercialization - Industry Advisory Board

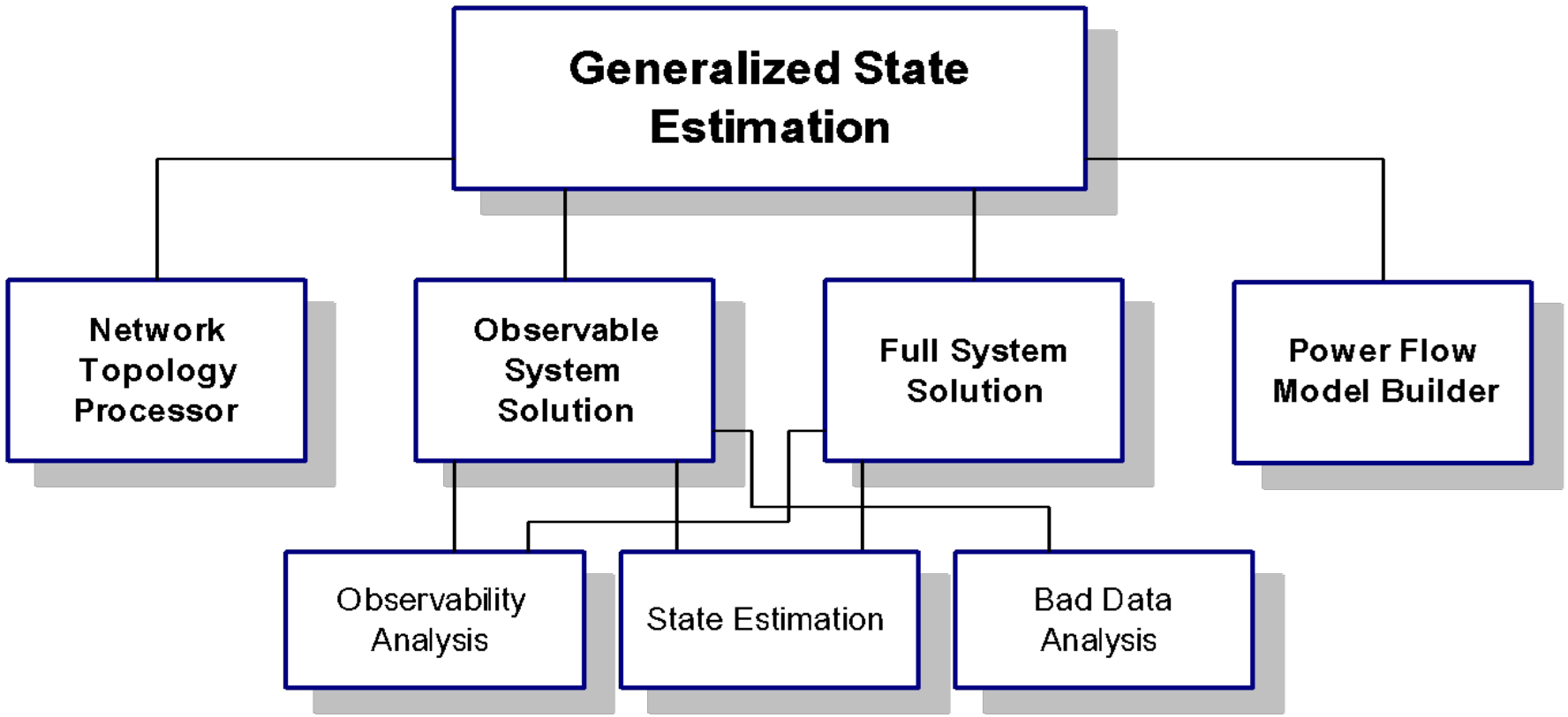


Form Industry Advisory Board

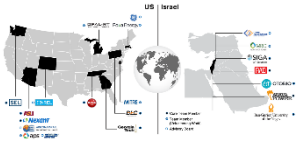
Board member organizations from previous collaboration of Resource Innovations with ASU: ComED, Entergy, Oncor, PSEG, Salt River Project, San Diego Gas & Electric Company, Southern California Edison, Southern Company, UK Power Networks

Future Industry Advisory Board will include Arava Power, Duquesne Light Company , Salt River Project, and Arizona Public Service plus many other utility companies

State Estimation - Overview



State Estimation - Example



Ask a roomful of people: “What time is it?”

“Around noon”

“12:01”

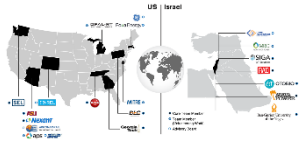
“12:00:01”

“12:00”

“12:00:02”

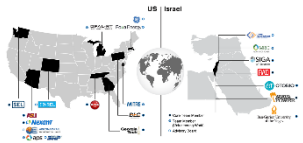
“12:03”

State Estimation - Generalized Bad Data Analysis



- **Recognizes the interaction between status & analog measurement errors**
  - Avoids camouflaging of topology errors as multiple analog measurement errors – does not assume correct topology
- **Performs estimation using a mixed model**
  - Parts of the network are represented at a physical level using explicit bus-section/switching-device modeling
- **Estimates analog states & breaker statuses simultaneously**
  - Supports largest weighted & normalized residual methods – an efficiency / accuracy tradeoff
- **Measurement redundancy is of paramount importance**

State Estimation - Measurement Error Identification



SCADA Checks
- Rejection of bad data by source SCADA system

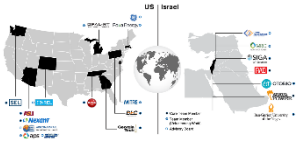
Gross Error Checks
- Rejection of data outside limits

Plausibility Checks
- Rejection of suspect data based on known data

Bad Data Analysis
- Weighted Residual Test and Normalized Residual Test (default)

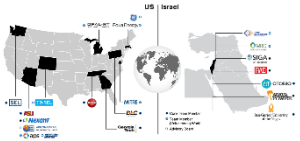
Final Solution

State Estimation - Bad Data Analysis Special Features

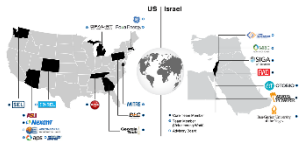


- **Detection & identification**
  - Weighted residuals
  - Normalized residuals
- **State estimation solution during bad data analysis**
  - Linear (non-iterative)
  - Non-linear (iterative)
- **Cycling with state estimation solution after bad data analysis**
- **Automatic & multi-level Bad Data Analysis (Screening Pockets and Zoomed Windows)**
  - Screening – Performs rigorous analysis on identified “bad data pockets”
  - Zooming – Remodels pockets for Bad Data Analysis at bus-section/switching-device level and “zooms in” if topology errors are suspected
    - Handles any expansion, contraction, creation & merging of electrical & observable islands
    - Provides effective pinpointing of bad data locations

State Estimation - Localized Modeling Special Features



- **Switch & bus injection pseudo-measurements are subject to bad data analysis**
  - Pseudo-measurements are used to augment available realtime measurements
  - Pseudo-measurements are typically calculated using short-term load forecasts or historical data
- **Gross errors do not propagate extensively**
- **Searching for bad data in the locality of the problem is efficient, particularly for large networks**
- **Local bad data analysis involves “windowing” and “pocketing”**
  - Pockets and windows can change, overlap or merge on the fly



Thank You!

Questions?