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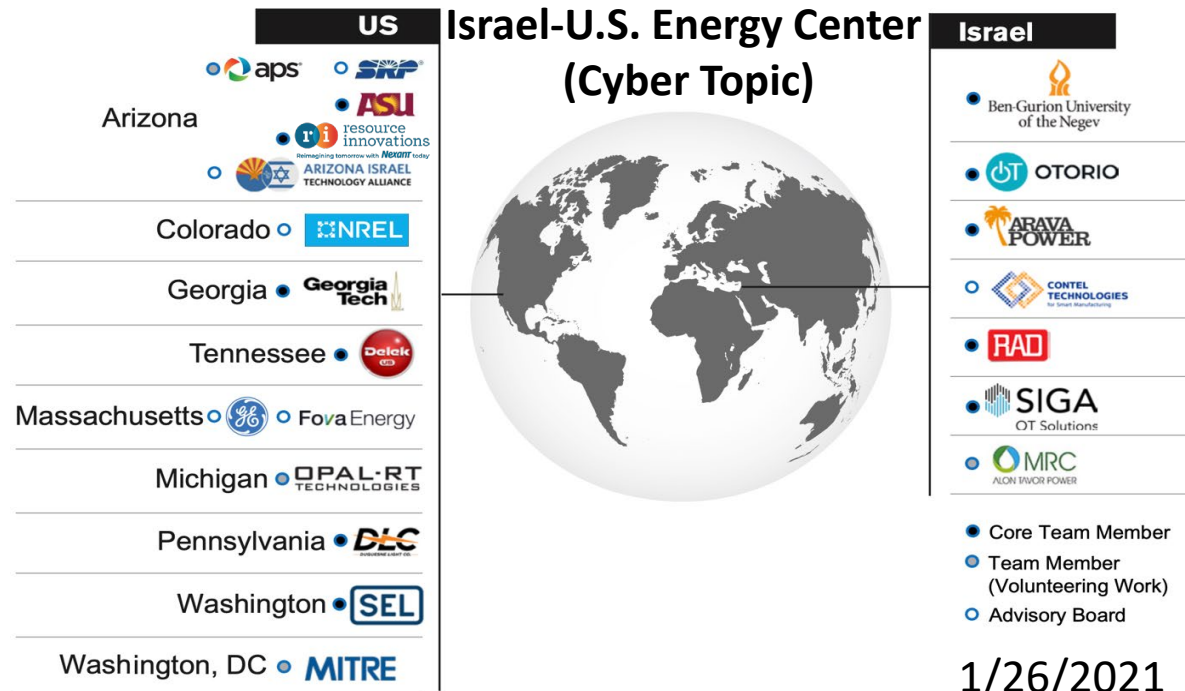 Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Israel-U.S. Energy Center (Cyber Topic)

**Task 1: Realization of Advanced Energy Management Applications in T&D**

**John Dirkman, PE**

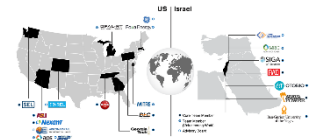Prepared for

**Itai Ganzer** and **Ofer Goldhirsh**
Israel Innovation Authority

**Avi Shavit** and **Eynan Lichterman**
Israel Ministry of Energy

1/26/2021

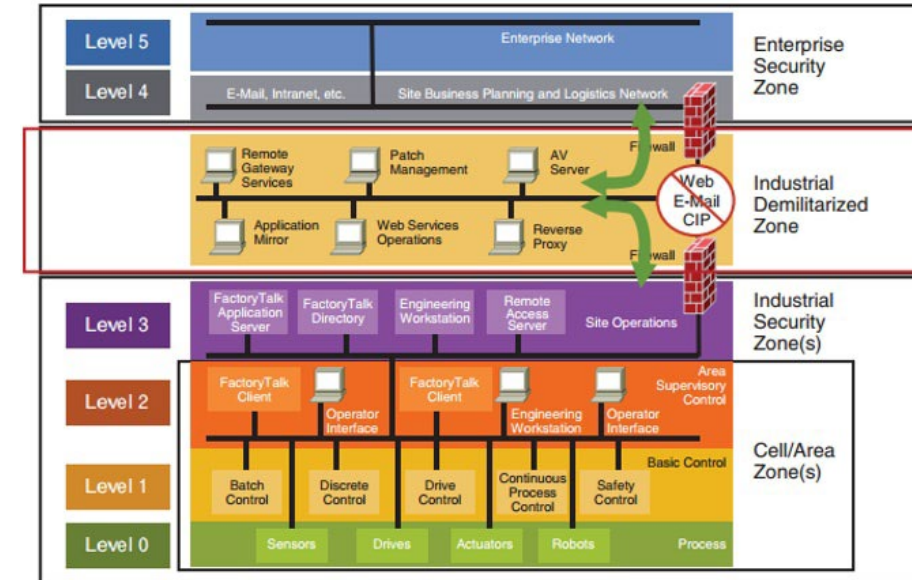# Commercialization - Presentations



Sukarno Mertoguno (Georgia Tech), John Geiger (RAD), Adam Hahn (MITRE), Rami Puzis (BGU), Ying-Cheng Lai (ASU), Shiri Freund Koren (BIRD Foundation), Andrea Yonah (BIRD Foundation)

# Commercialization Tasks

- Assemble digital twins in Grid360
  - distribution/transmission network, solar arrays, refineries, communications network
  - DLC, APS, SRP, Arava, Delek
  - Provided Grid360 logins to ASU team for state estimation research
- Assemble cybersecurity lab
  - Sensors, Meters, PLCs, RTUs, HMI, Firewalls, Historians, Management Systems, etc.
  - Zones: Corporate, DMZ, Operations
- Team Education - T&D dynamics and threat vectors
- Team Education - commercialization approaches
  - Convert academic work to commercialized product
    - User experience: data input, processing, output, visualization
    - Use of third-party tools
    - Integration with other applications - APIs
    - Testing
    - Installation and User Guides, Training
  - Commercialization Plan: Go-to-market and business growth strategy
    - what is the product, who are the target customers, customer value proposition, market potential, competitive advantages, IP strategy, promotion, management, metrics, and financial performance
- Lean Canvas - determines which tasks have greatest potential for commercialization
- Establish Industry Advisory Board, first meeting in September, meetings about every six months

# The Lean Canvas

## Problem

Top 3 problems

## Solution

Top 3 features

## Unique Value Prop.

Single, clear and compelling message that states why you are different and worth buying

## Unfair Advantage

E.g. can't be easily copied or bought

## Customer Segments

Target Customers

## Existing Alternatives

List how these problems are solved today.

## Key Metrics

Key activities you measure

## High-Level Concept

List your X for Y analogy
(e.g. YouTube = Flickr for videos)

## Channels

Path to customers

## Early Adopters

List the characteristics of your ideal initial customers.

## Cost Structure

List your fixed and variable costs:
- Customer acquisition costs
- Distribution costs
- Hosting
- People
- Technology
- Etc.

## Revenue Streams

List your sources of revenue:
- Revenue Model
- Life Time Value
- Revenue
- Gross Margin

# Commercialization - Software Deployment
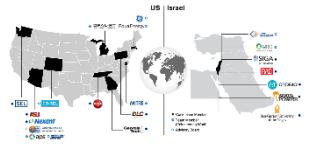
Add developed software as "engines" inside of Grid360 and other vendor systems

Create commercial grade engines to be embedded in Energy Management Systems (EMS), Distribution Management Systems (DMS), and Supervisory Control and Data Acquisition (SCADA) systems, similar to Resource Innovations' current work with Hitachi/ABB, GE, Toshiba, and Smarter Grid Solutions
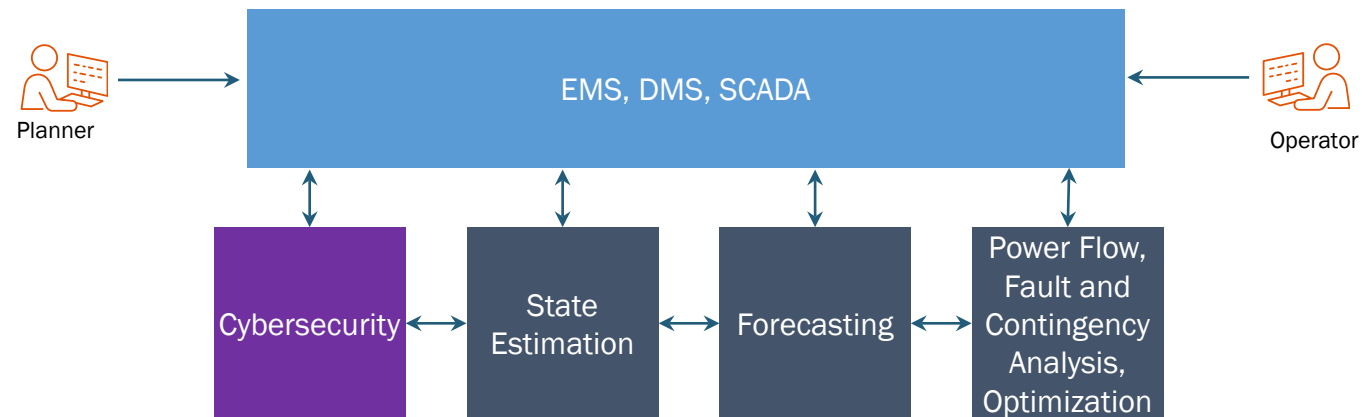
# Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-based Centralized Defence and Edge Resilience



Likely best candidates for commercialization

**Theme 1: Cyber-Physical System (CPS) Data Preparation**

**Project 1**: Physical Processes as Cybersecurity Assets
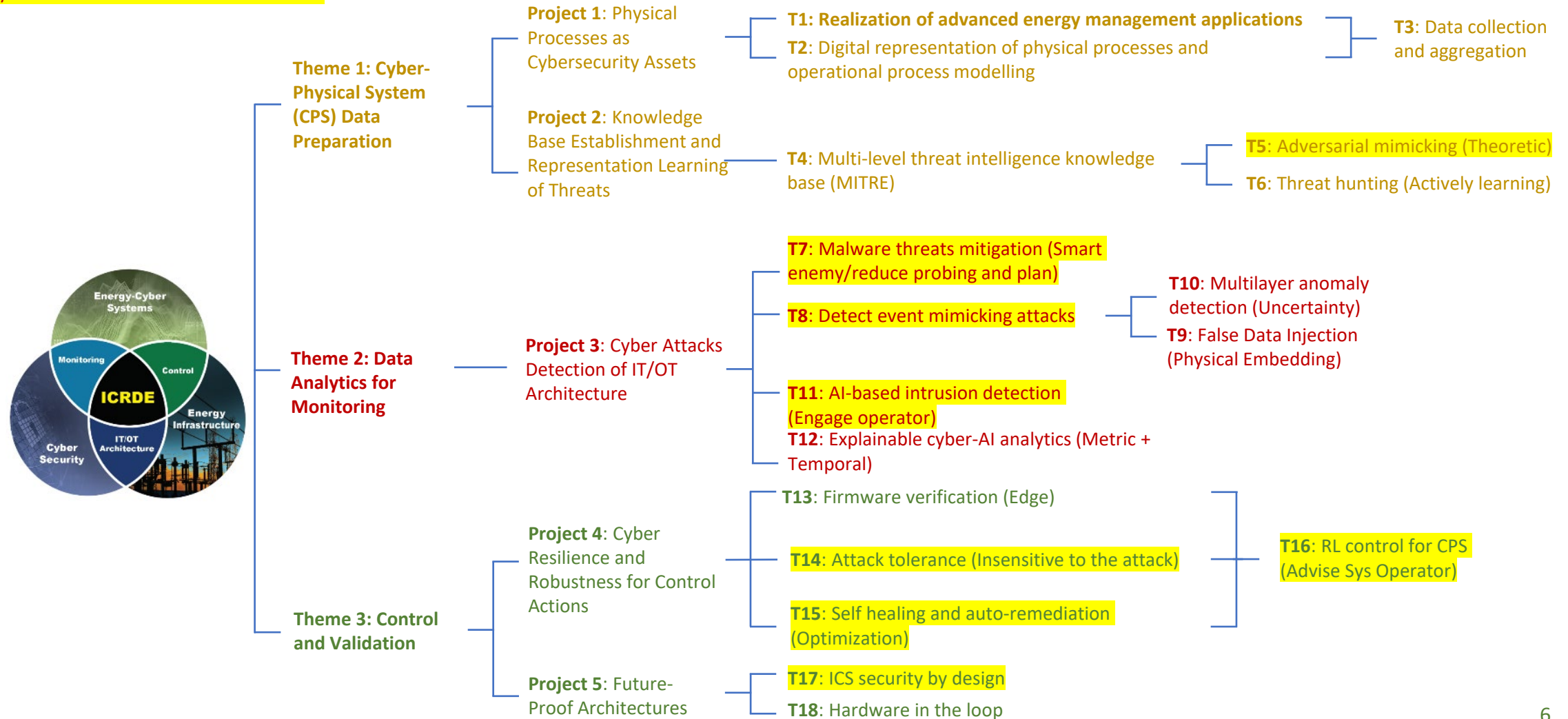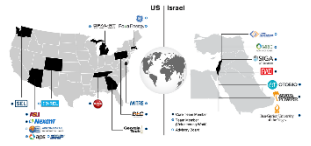
**T1: Realization of advanced energy management applications**

**T2**: Digital representation of physical processes and operational process modelling

**T3**: Data collection and aggregation

**Project 2**: Knowledge Base Establishment and Representation Learning of Threats

**T4**: Multi-level threat intelligence knowledge base (MITRE)

**T5**: Adversarial mimicking (Theoretic)

**T6**: Threat hunting (Actively learning)

**Theme 2: Data Analytics for Monitoring**

**Project 3**: Cyber Attacks Detection of IT/OT Architecture

**T7**: Malware threats mitigation (Smart enemy/reduce probing and plan)

**T8**: Detect event mimicking attacks

**T10**: Multilayer anomaly detection (Uncertainty)

**T9**: False Data Injection (Physical Embedding)

**T11**: AI-based intrusion detection (Engage operator)

**T12**: Explainable cyber-AI analytics (Metric + Temporal)

**Theme 3: Control and Validation**

**Project 4**: Cyber Resilience and Robustness for Control Actions

**T13**: Firmware verification (Edge)

**T14**: Attack tolerance (Insensitive to the attack)

**T16**: RL control for CPS (Advise Sys Operator)

**T15**: Self healing and auto-remediation (Optimization)

**Project 5**: Future-Proof Architectures

**T17**: ICS security by design

**T18**: Hardware in the loop

6

# Commercialization - Industry Advisory Board

Form Industry Advisory Board, first meeting in September

BIRD Cybersecurity Industry Advisory Board will include Arava Power, Arizona Public Service, Delek US, Duquesne Light Company, Salt River Project, as well as other organizations:

| Name | Title | Organization |
|------|-------|--------------|
| Bill Brandt | Director ASU LightWorks, Strategic Integration | ASU |
| Ed Budde | Regional Technical Manager SW Region | SEL |
| Sherry Jacob | Senior Manager O&G/Utility | Accenture |

I would like additional assistance recruiting Industry Advisory Board members.

# Commercialization - Approaches
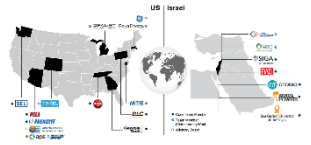
## Technical approach

Six 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), and (6) IoT devices

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

## Commercialization approach

Licensing mechanism is preferred

## Market segments

EMS/DMS/SCADA: IOU T&D utilities, municipal utilities and cooperatives in North America, T&D utilities in rest of the world

PLC/ICS/CPS/IoT: many potential applications

## Key commercial partners, customers/advisors

Form Industry Advisory Board (IAB)

Leverage eco-system of utilities, vendors, and system integrators

Composition of IAB will be utility personnel, vendors, system integrators, and academics

90 minute meetings approximately every six months

IAB will provide feedback/validation of our proposed approach and market strategy

Executed successfully for DOE ARPA-E Sensor Enabled Modeling of Future Distribution Systems with DER and other projects

Email jdirkman@resource-innovations.com to join
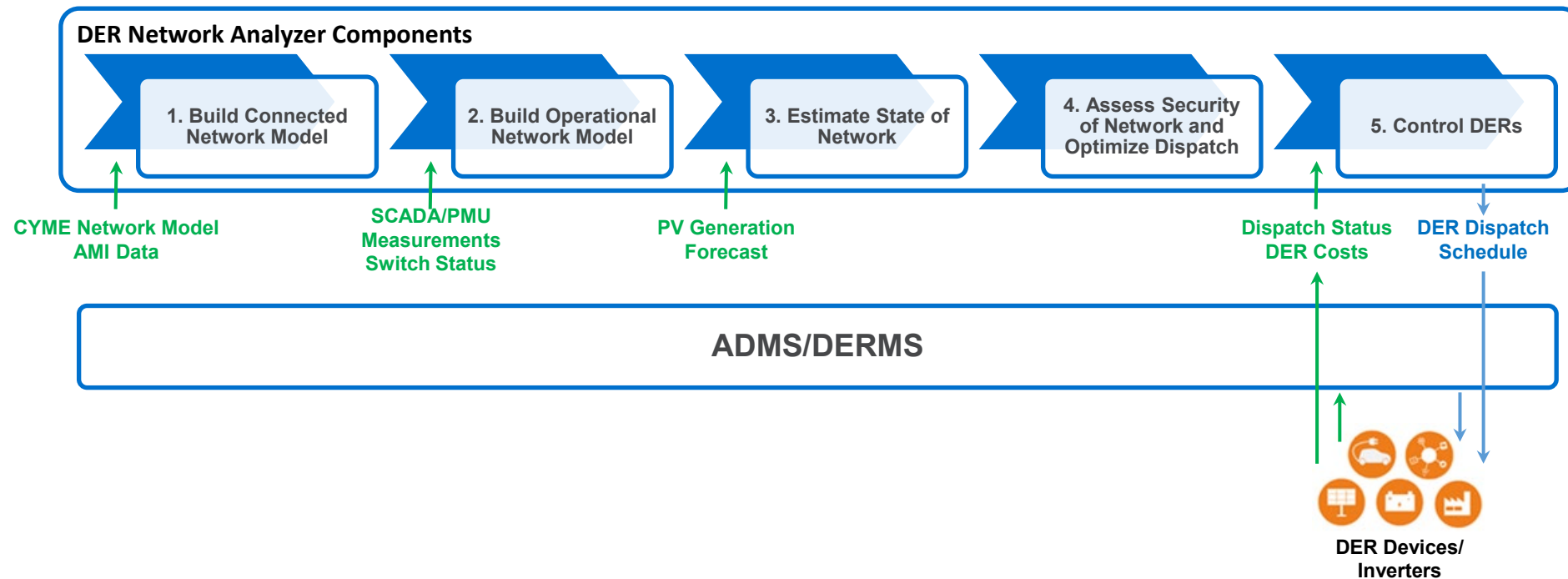
## Upcoming commercial activities

Promotion of technology and preliminary outreach to potential customers

Publication of results obtained during project - journals, white papers, conferences, etc.
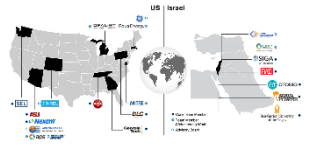
# DER Network Analyzer Commercialization

DER Network Analyzer components function in parallel with ADMS/DERMS



**DER Network Analyzer Components**

1. Build Connected Network Model → 2. Build Operational Network Model → 3. Estimate State of Network → 4. Assess Security of Network and Optimize Dispatch → 5. Control DERs

CYME Network Model AMI Data | SCADA/PMU Measurements Switch Status | PV Generation Forecast | Dispatch Status DER Costs | DER Dispatch Schedule

**ADMS/DERMS**

DER Devices/ Inverters

1. Compiled code from ASU, installed on Resource Innovations servers
2. Worked with ASU to create Installation Guides and User Guides to include data input, output, visualization
3. Worked with APS to set up servers, install and use developed code
4. Worked with Industry Advisory Board to determine best candidates for commercialization

```
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())
```

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 - Cyber Metrics Visualization

# Commercialization - Cyber Metrics API