

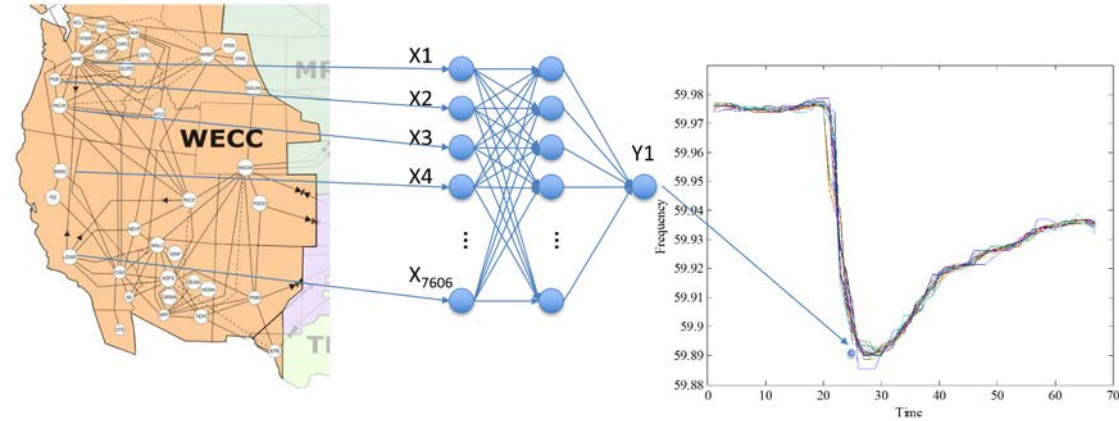
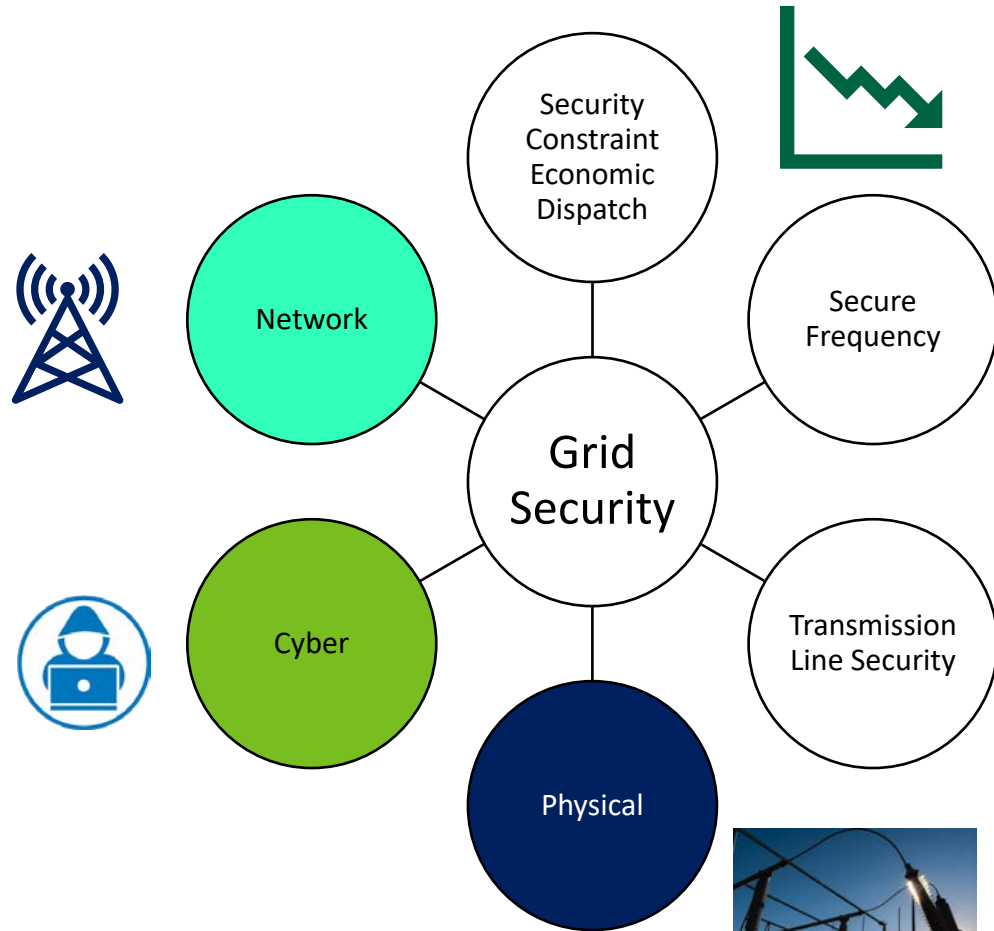


OT Operational Anomaly Detection (OAD) T&D + DER

2023 IEEE Power & Energy Society General Meeting

Seong Choi, Engineering Lead
National Renewable Energy Laboratory

What does 'security' mean in the electric grid?



- In the electric industry, 'grid security' relates to
- **Grid operating condition**: balancing generation and load
 - **Cyber**: data
 - **Network**: data relay
 - Physical: equipment to support the power delivery, including protection

Today's Coverage:
T&D Grid operation & Cyber



Source: NREL Flatiron Substation

Limitation of the Purdue Model

Level 3: Control Center

FEP/SCADA/EMS
Network Application/WAMS

Level 2: Station - Facility operation

- HMI/SCADA
- Historian/Engineering Workstation

Level 1: Bay - Control & protection

- RTU/PLC/DCS
- IED/Relay/Meter

Level 0: Process - Field

- Sensor
- Actuator
- CT/PT

Safety Zone

- Fence
- CCTV

1

Manufacturing (Widget) vs. Operating (Service)

- The Purdue model is developed for the manufacturing industry to integrate enterprise and control systems
- The power grid is to operate/deliver electricity from generation to load. Not like oil, water or gas, electricity cannot be stored at the interconnection level which requires operators to become critical to balance generation and load.

2

Power Flow: Unidirectional vs. Bi-Directional

- The Purdue model is unidirectional from design to production
- The power grid becomes bi-directional due to renewable. Bi-directional power flow makes each layer flattened to directly communicate with other layers
- Lower layers can send data to a cloud and receive a command from the cloud, not go through layers

3

Asset: Physical vs. Virtual

- Layers become blurred with Virtual SCADA or Virtual Relay
- With virtualized servers or firewalls, logical grouping blurs layers

4

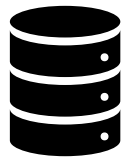
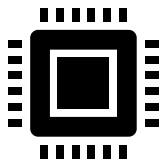
Visibility: Utility own data vs. Consumer sharable data.

- Consumers or vendors share their data in Cloud services where utilities do not own or control.

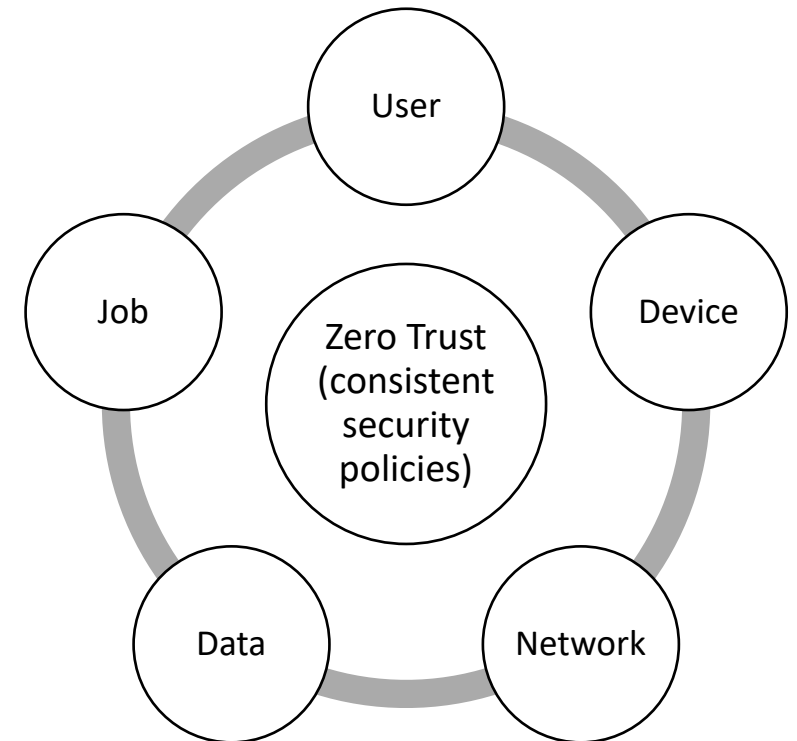
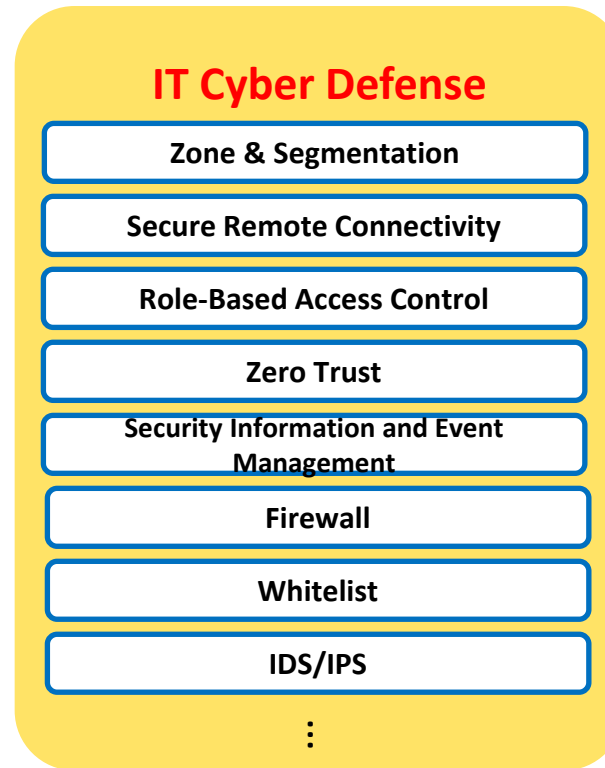


**OT Challenge: Purdue model is egress/ingress approach
If authenticated, lateral move is allowed.**

Purdue Model based IT Cyber Defense + Zero Trust: “Trust, But Verify”



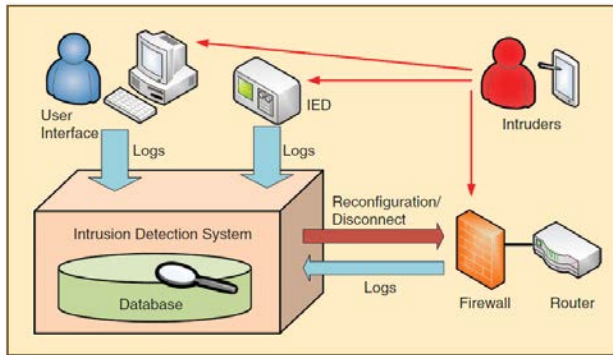
CPU, Memory or Network Anomaly Detection



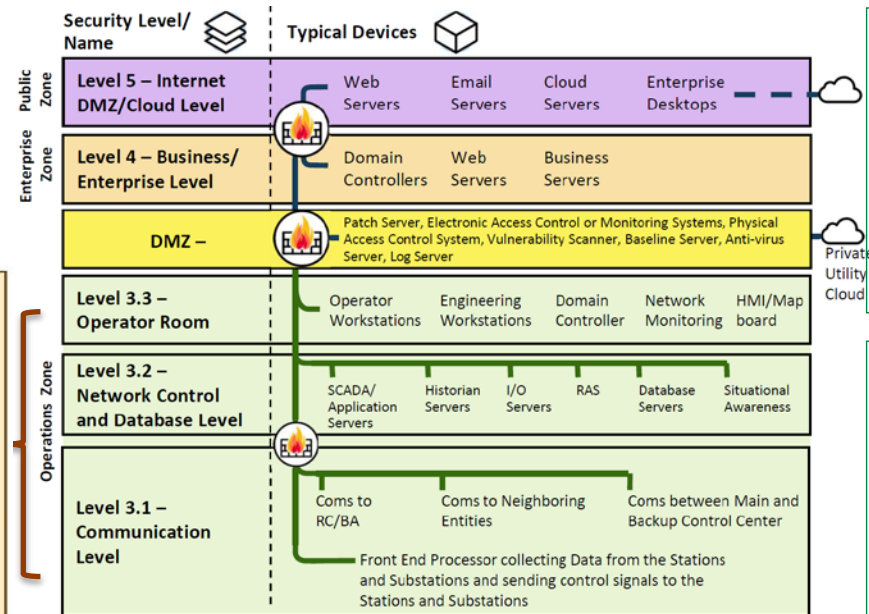
OT Challenge: If trusted and verified, should I accept data as it is?

How to protect from insider threats or disguised employees?

Is the inside action **hostile** to the crown jewels you want to protect?



Chen-Ching Liu, Intruders in the Grid



DOE CESER, Reference Architectures as a Means of Influencing Electric Energy Operational Technology/Industrial Control System Security Outcomes

Phishing or Cyberattack victims

- Engineers
- DER aggregators
- VPP operators

Supply Chain Attack victims

- RTU data
- IED
- PLC

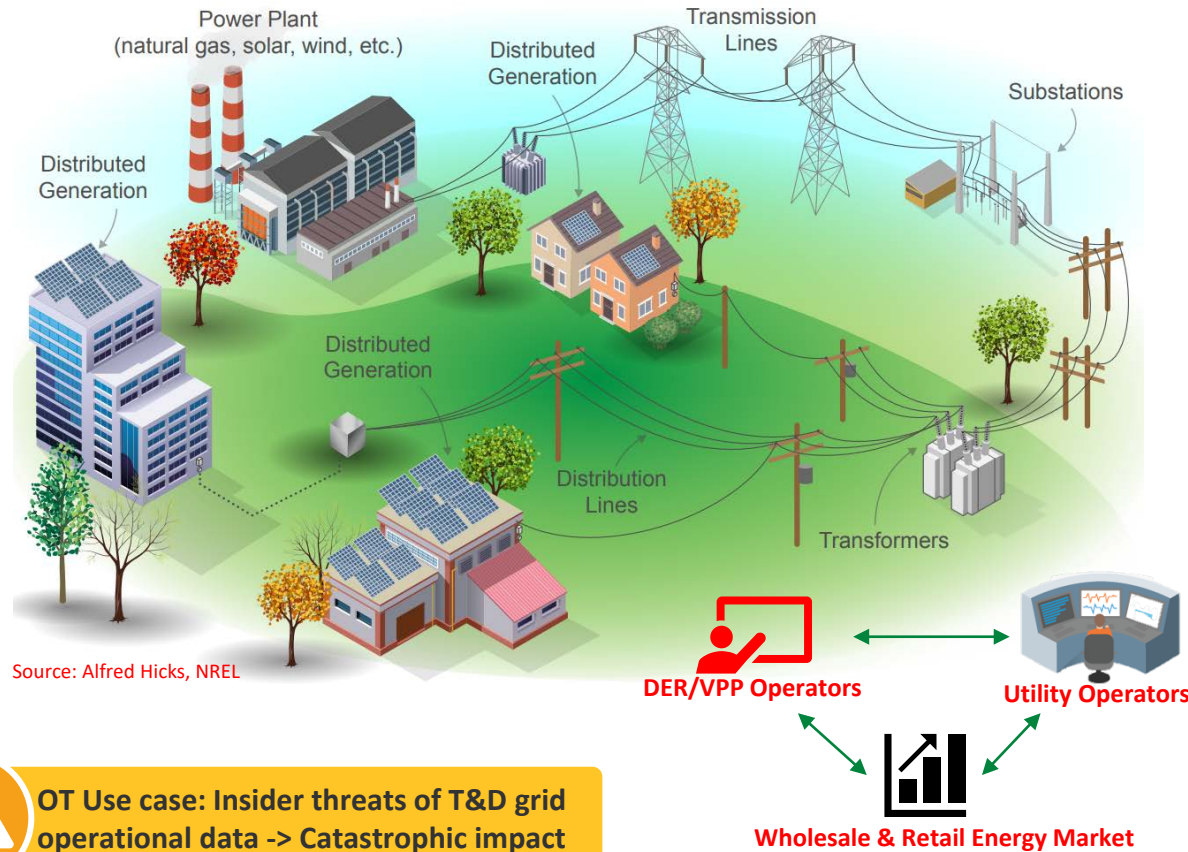
Impacts: Manipulation of Control & View



OT Challenge: Am I seeing the right data to operate?
If the data is not right, then a catastrophic impact is inevitable

DOE Cybersecurity Goal

Ensure Cybersecurity Attacks Do Not Catastrophically Impact the Energy Sector



Insider Threats



Drone Attack



Physical Attack



Zero-Day Cyberattack



Phishing or Cyberattack

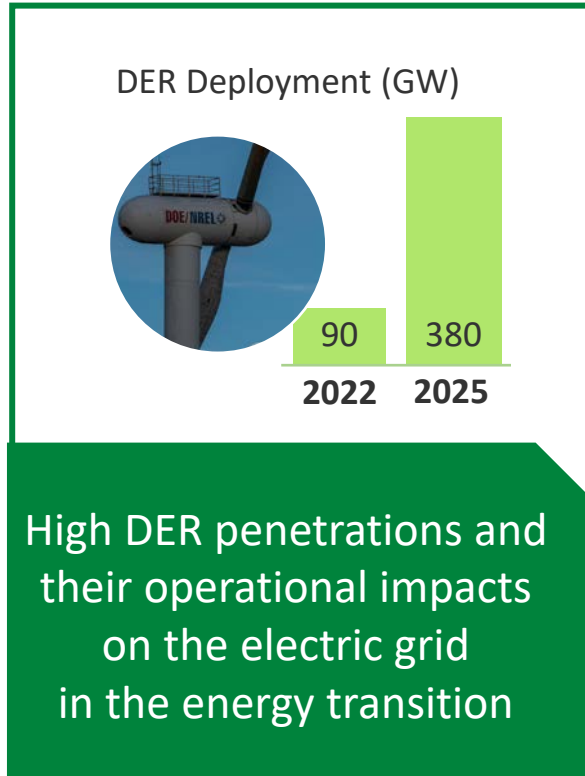


Supply Chain Attack



OT Use case: Insider threats of T&D grid operational data -> Catastrophic impact

Operational Technology OAD Problem Statement

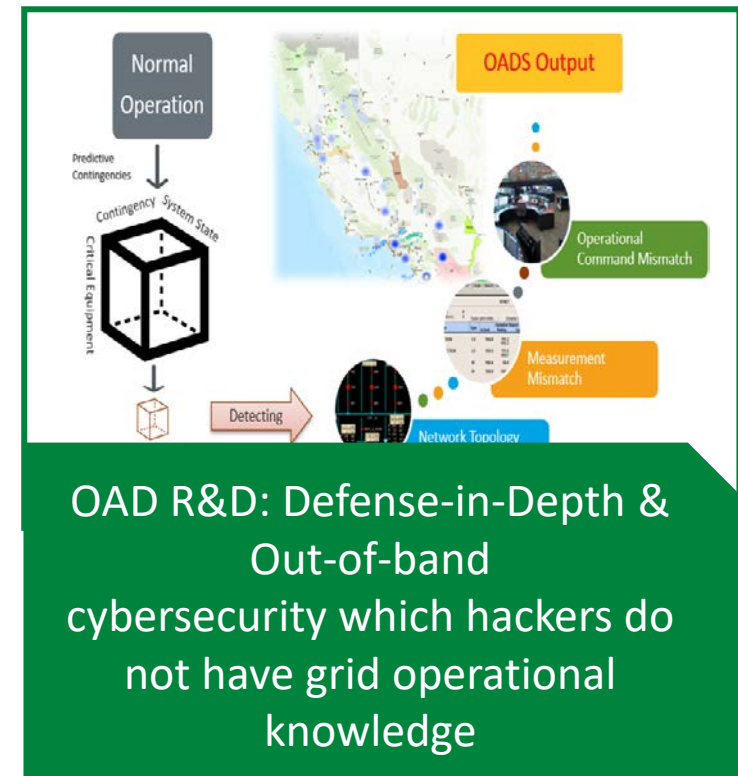


Challenge

Security Level/Name	Typical Device Examples	Function
Level 5 – Internet /Cloud Level	Domain Name System Server, Public Cloud Servers	External Communication
Level 4 – Business/Enterprise Level	DMZ – Web Servers, Email Servers, Remote Access Server	Internal Business Communication
Level 3 – Control Center Level	DMZ – Historian, Backup Director, Patch Server, Remote Access/Operator Workstations, Database Servers, I/O Servers, Domain Controller, SCADA/ Application Servers	Internal Operatic Communication
Level 2 – Facility Level	DMZ – Historian, Backup Director, Patch Server, Remote Access/RTU / Gateways, Local HMIs, Engineering Workstations	Process Data Cor Control, Asset M
Level 1 – Subsystem Level	Protection, Subsystem Controllers, IEDs	Data Acquisition, Process Control

Current Purdue model-based anomaly detection is not sufficient to orchestrate EMS-ADMS-DERMS-BTM (grid of grids)

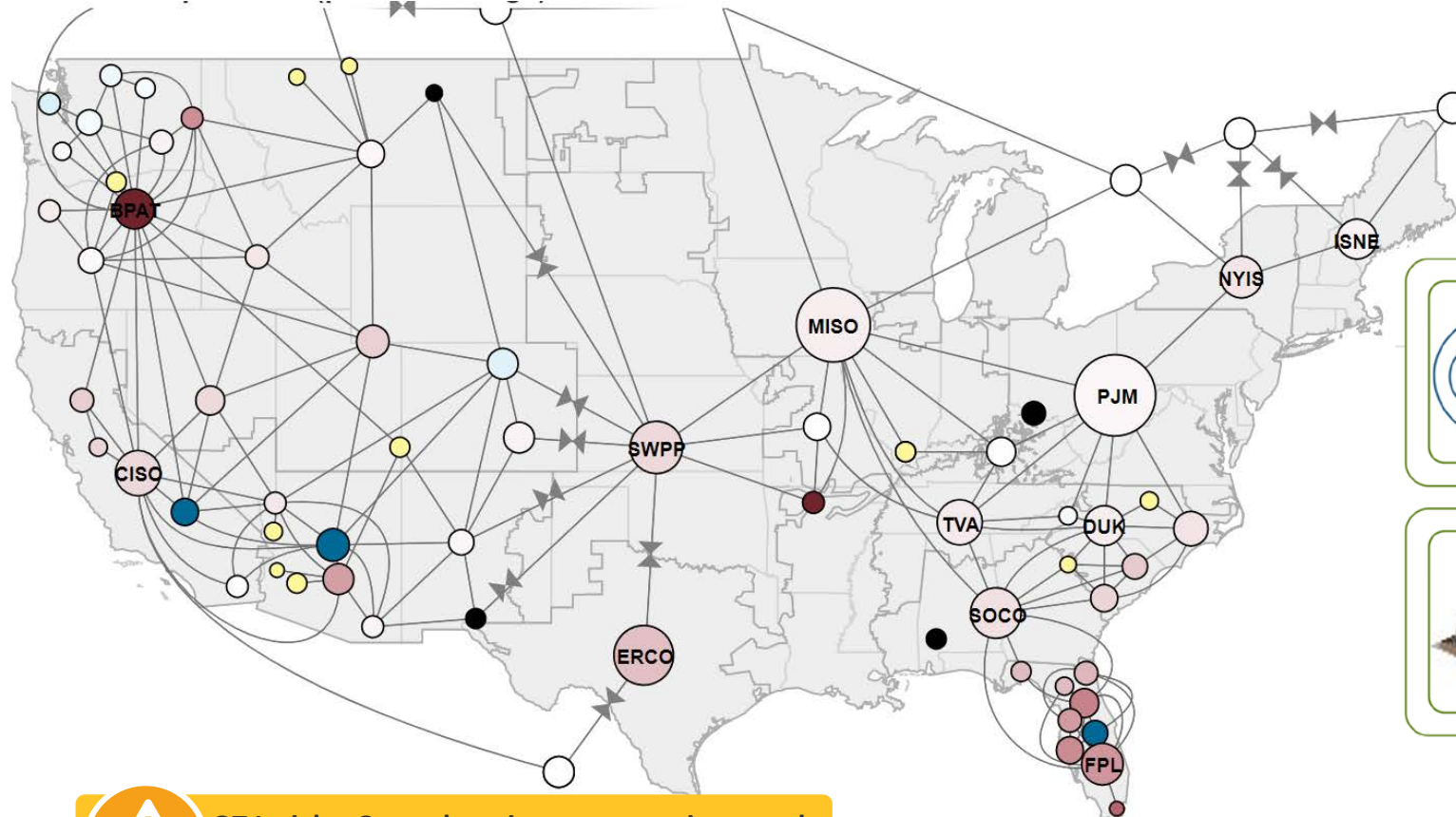
Gap



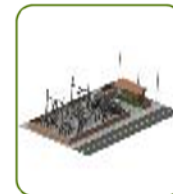
Recommendation

Catastrophic impact: Which data to manipulate

Data from substation connect to the Critical Transmission Corridor or from Generation



11,900 Utility Scale Power Plants (>1MW)



55,000 Transmission Substations



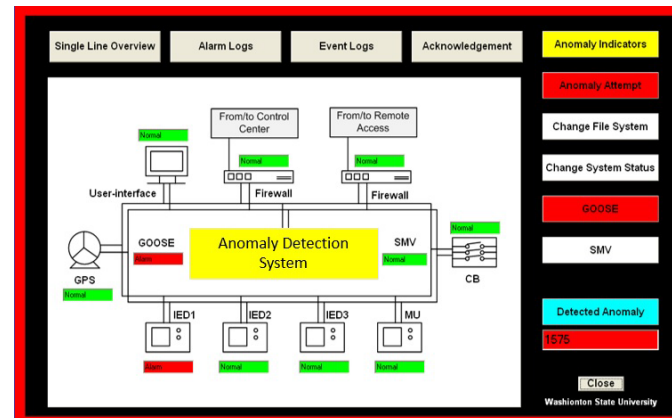
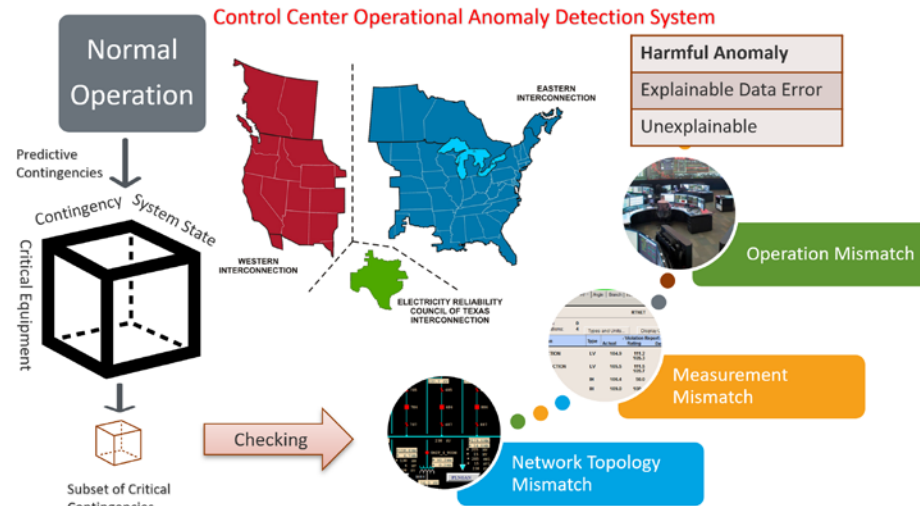
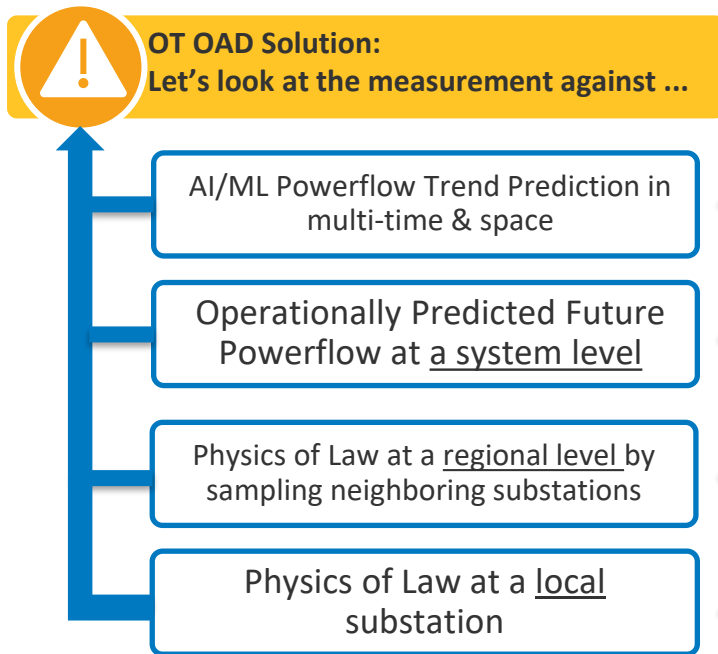
OT Insight: One substation or generation attack is not enough to cause catastrophic impact

Source: EIA, Hourly Electric Grid Monitor

OT Approaches to Deal With Insider Threats: Compliment to IT Cybersecurity & Zero Trust

Pay less attention to what people say and **more attention** to what they **do**.

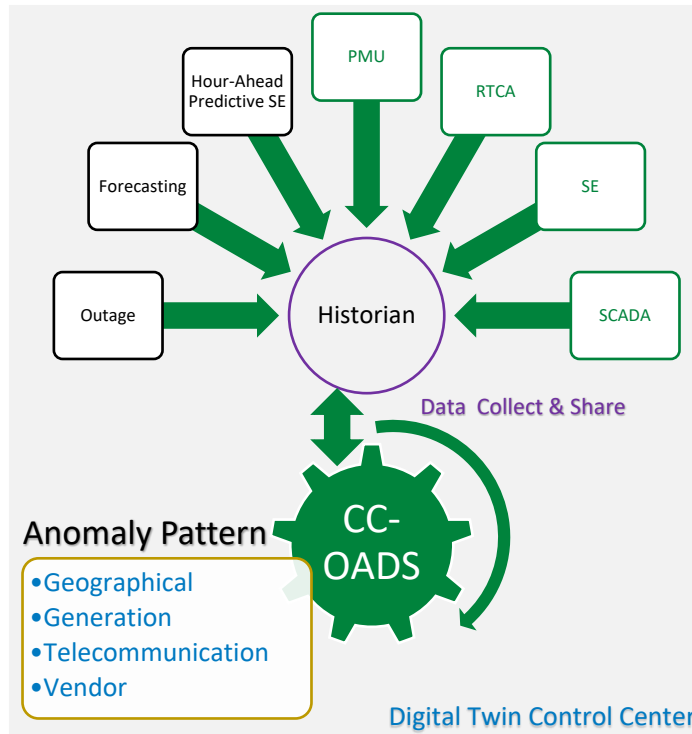
Andrew Carnegie



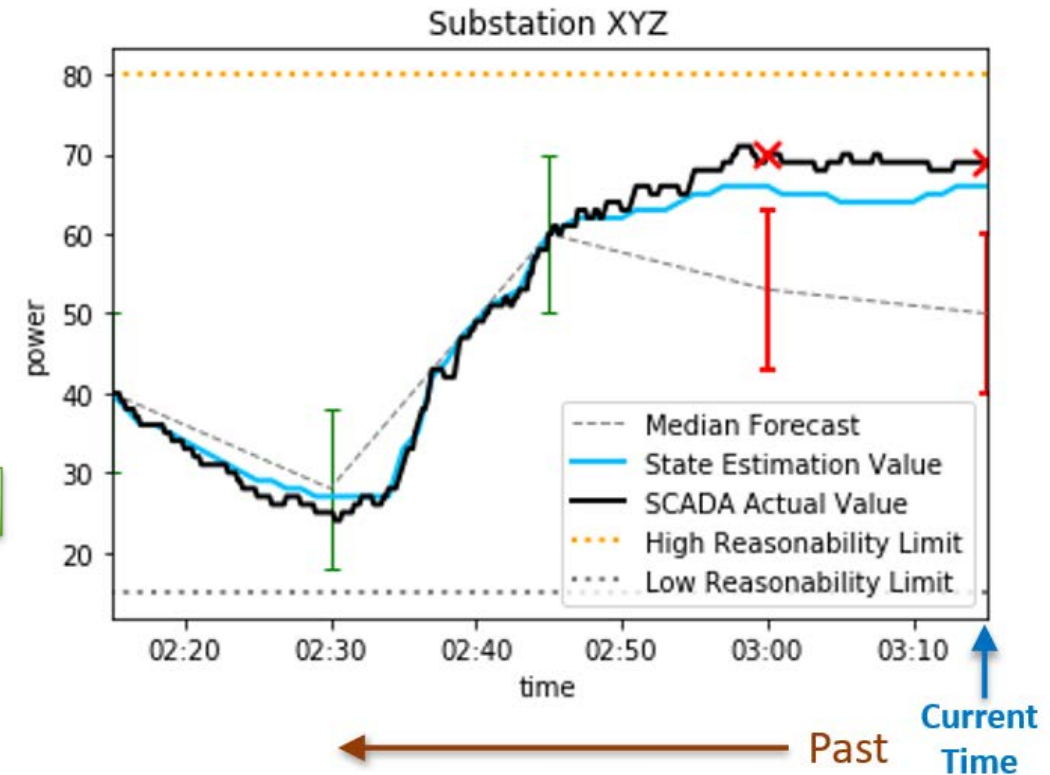
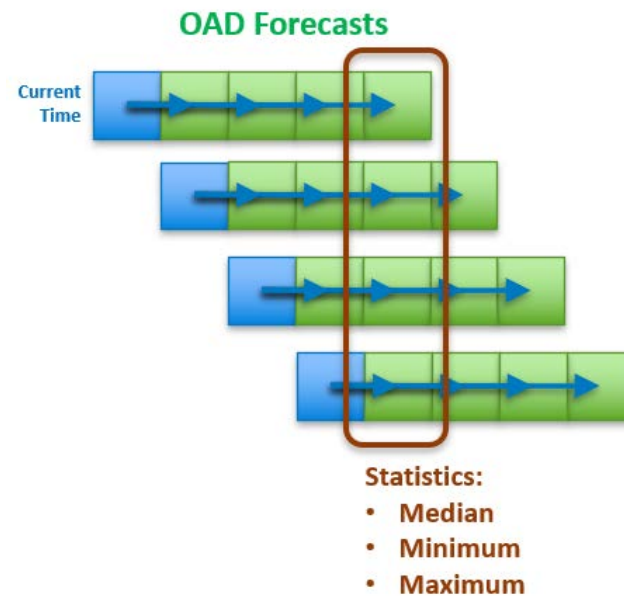
Chen-Ching Liu, Cyber security of a power grid: State-of-the-art


Ensemble State Prediction Model

Current Network Topology, Forecasting, and Outage



Control Center Operation Anomaly Detection



 OT OAD Advantage:
Hackers do not know look ahead analysis

OT Measurement + Cyber Check

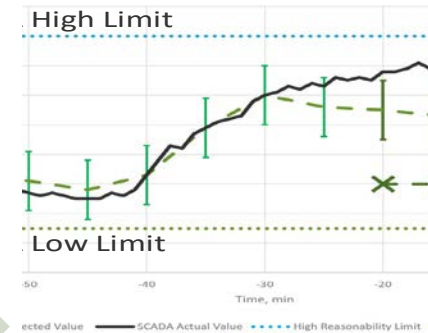
Local, Regional & System Level

- State Estimator + Real-Time Contingency Analysis
- State Prediction with future-hour forecasted data

Channel	Residual Pattern	Risk Level Suggestion		
1		0	1	2
2		0	1	2
3		0	1	2
4		0	1	2

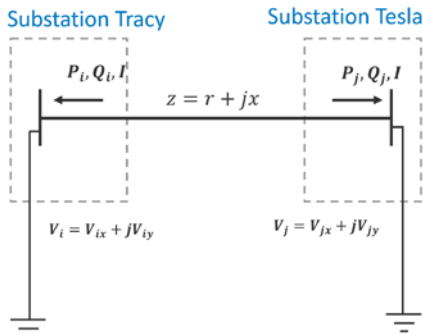
AI/ML Powerflow Trend Prediction in multi-time & space

Operationally Predicted Future Powerflow at a system level



Physics of Law at a regional level by sampling neighboring substations

Physics of Law at a local substation



- DNP3 Protocol Packet Analysis
- Kirchhoff's and Ohm's Laws

Circuit Law	OADS RULES
KCL	$ \sum I_{exit} - \sum I_{enter} \leq k_{cern1} i_i + k_{cern} i_n $
KVL	$ v_1 + \dots + v_n \leq k_{vern1} v_i + k_{vern} v_n $
Ohm's Law	$ v_j - v_k - i_{jk}Z_{line} \leq \text{MAX}\{k_{verj} v_j , k_{verk} v_k , k_{cerjk} i_{jk}Z_{line} \}$



OT OAD Solution: Out-of-the-band check

OT Cyber Defense

Asset Inventory and Device Authorization

Protocol Anomaly Detection

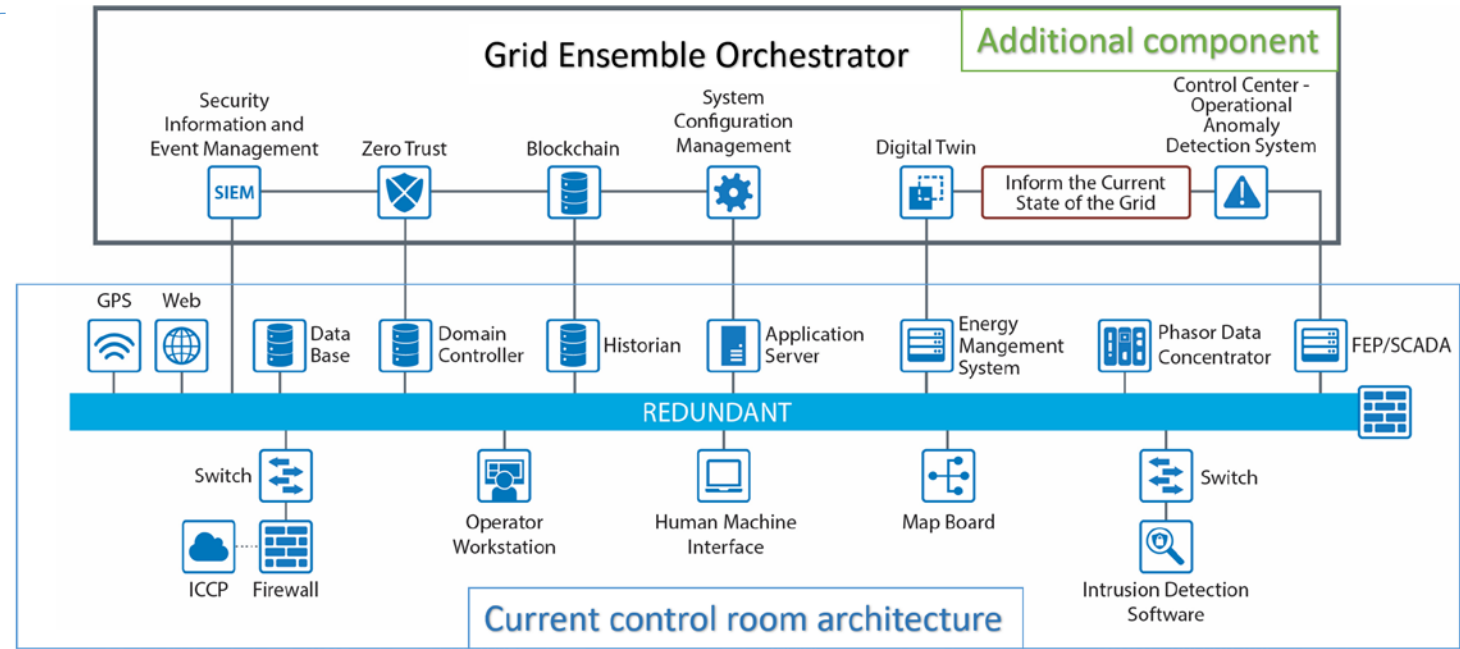
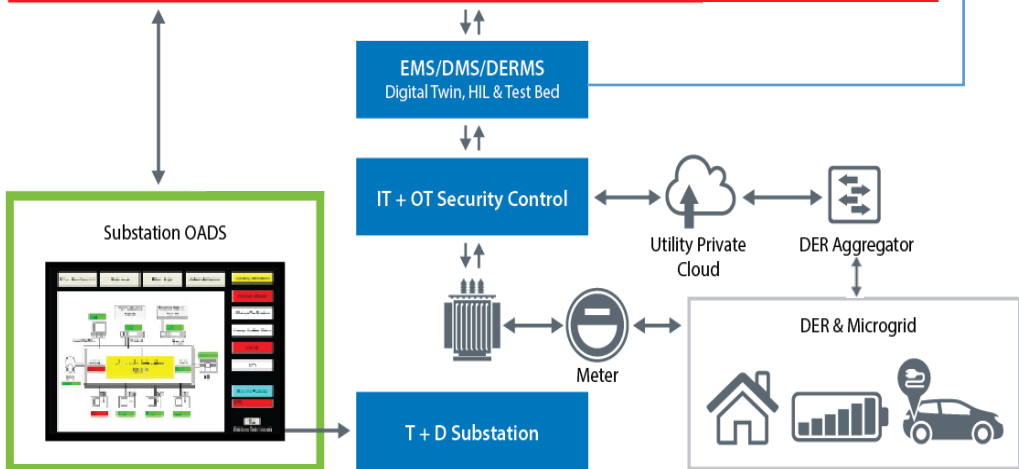
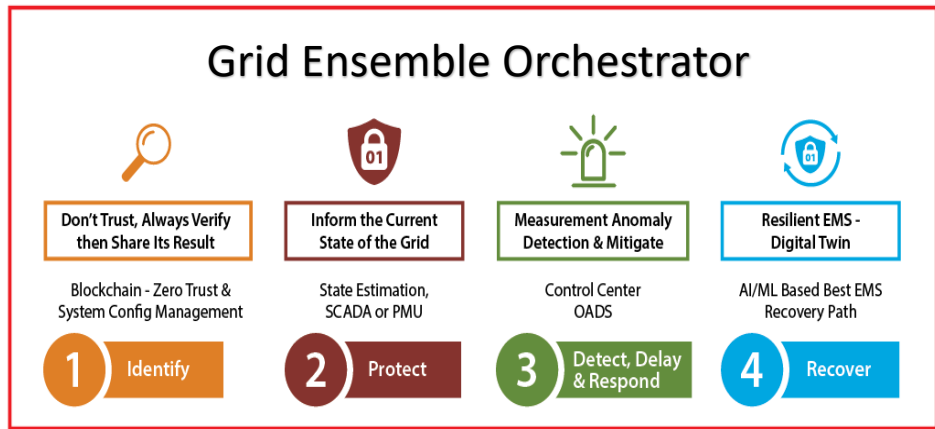
OT Network Monitoring and Anomaly Detection

Protocol Threshold Check

OT Measurement Signature-Based AI/ML Anomaly Detection

⋮

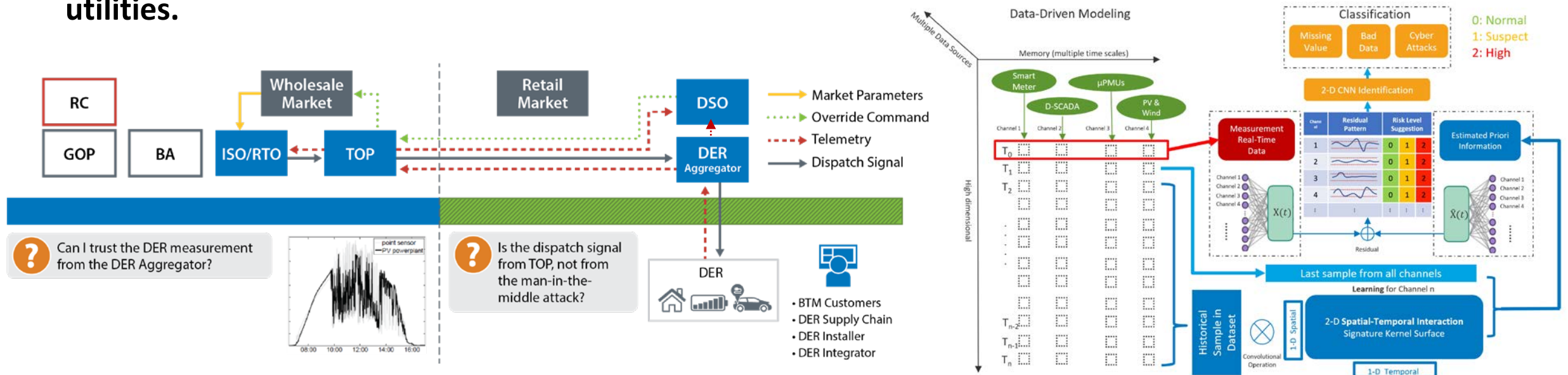
Grid Ensemble Orchestrator



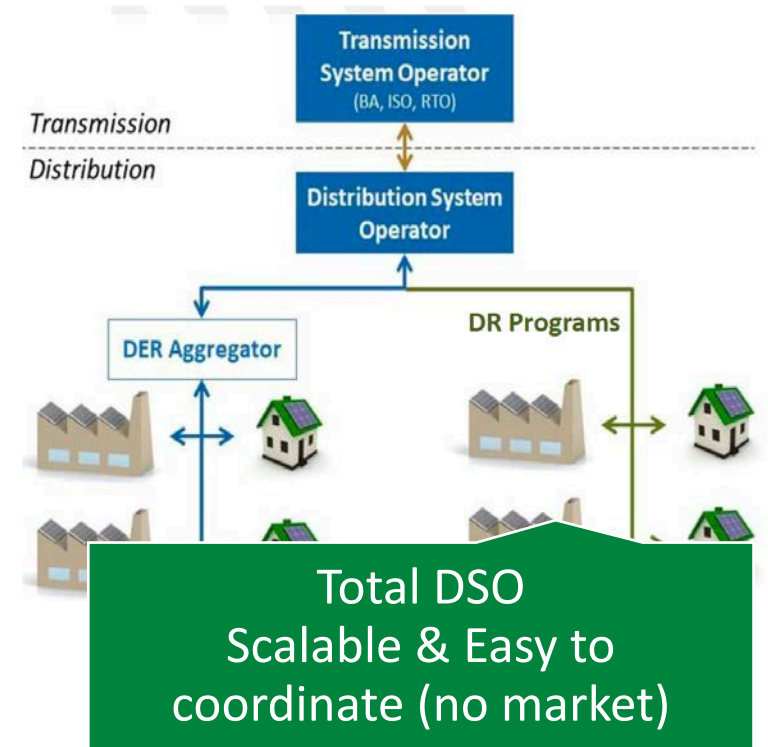
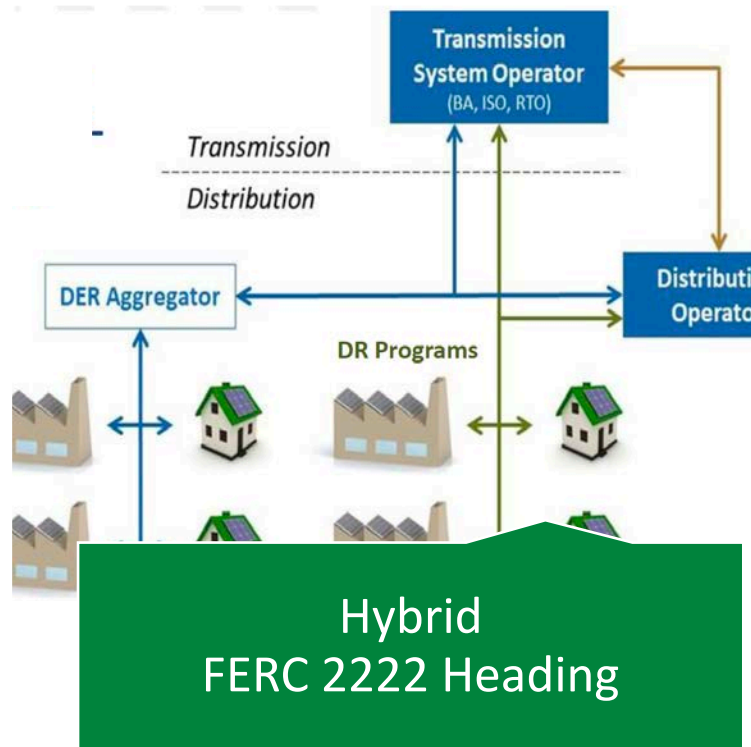
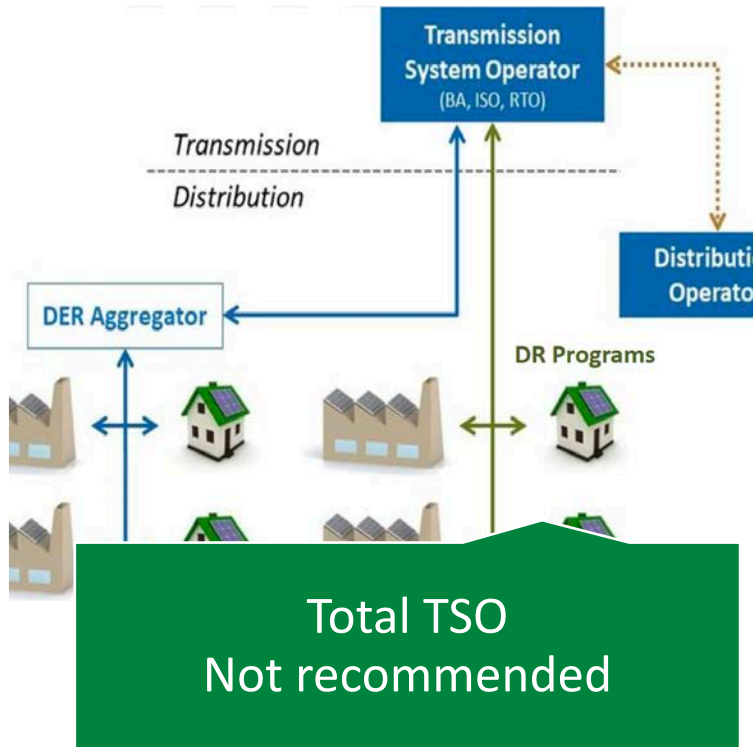
Extending OT OAD to DER Layer?

Call for AI/ML Anomaly Detection in DER

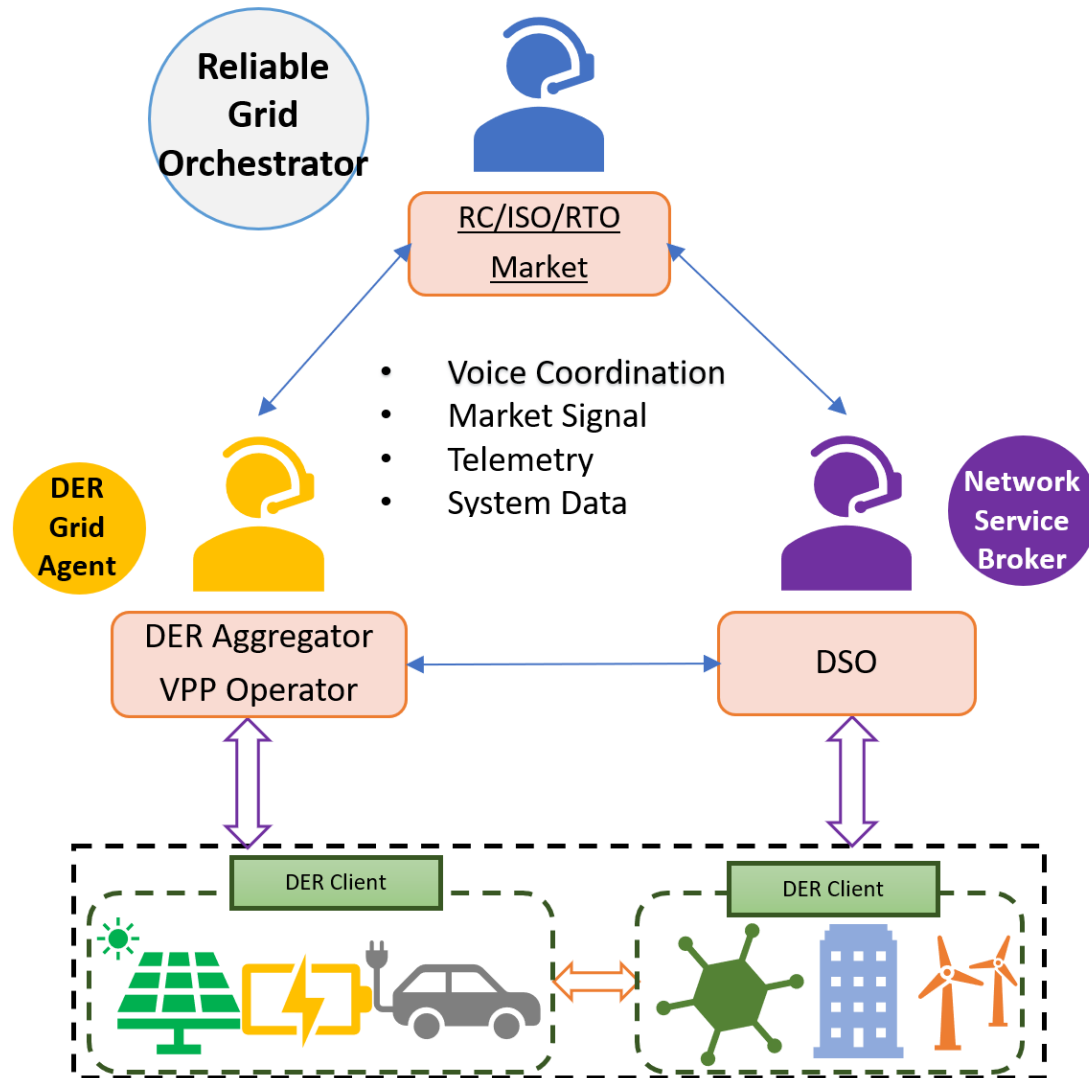
1. OT OAD proposed look-ahead predictive state estimation, which is not available in most ADMS network applications.
2. False positive: Probabilistic load and generation forecast will cause false positive alarms most of the time.
3. Scalability concern: Increasing penetration levels of DER inverters
4. Visibility concern: Exponential growth of IoT devices impacting load pattern, which is not visible to the utilities.



Future TSO-DSO-DER Interaction Options



DER Multi-Agent Orchestrator Architecture



- Orchestrator manages brokers
- Reassigns brokers.

Cyber Orch.

- Brokers manage agents
- Notify role update
- Peer-to-peer brokers.

Cyber Broker

- Possible roles:
- Threat sharing
 - Continuous monitoring
 - Trust evaluation
 - Risk evaluation
 - Micro-segmentation
 - Encryption
 - Risk-aware access control.

Cyber Agent


IT + OT Convergence with Power Knowledge



IT cybersecurity inspects network traffic/data packets

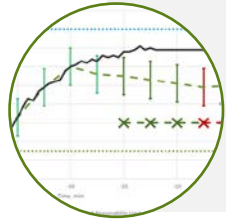
+



 OT OAD Goal: Enhance IT & OT Convergence by leveraging cyber-physical power knowledge

What Are the OT OAD Benefits to the Utility Industry?

Conclusions



Verify operationally acceptable measurements at substations.

- OAD provides operationally acceptable measurements at substations.
- OAD flags measurements do not follow the physics of law at substations.



Safety



Verify operationally acceptable measurement at a control center.

- OAD provides operationally acceptable network topology.
- OAD provides early flags of suspicious substation measurements at the front-end processing.



Reliability

NREL ECM Team Members



Seong Choi (PI)
Project Overseer and Architect



Jiazi Zhang
Scenario Development



Venkateswara Reddy Motakatla
Anomaly Detection Algorithm
Development



Hongfei Sun
AI/ML Data Scientist



Joshua Comden
ECM UI Development



Michael Parker
Project Management



Thank you!

Seong.Choi@nrel.gov
Jiazi.Zhang@nrel.gov

NREL/PR-5D00-86275