Artificial Intelligence for Energy Systems Cybersecurity

September 29, 2021

Richard Macwan

Senior Researcher – Power System Cybersecurity

Cybersecurity Science and Simulation Group

Ryan King

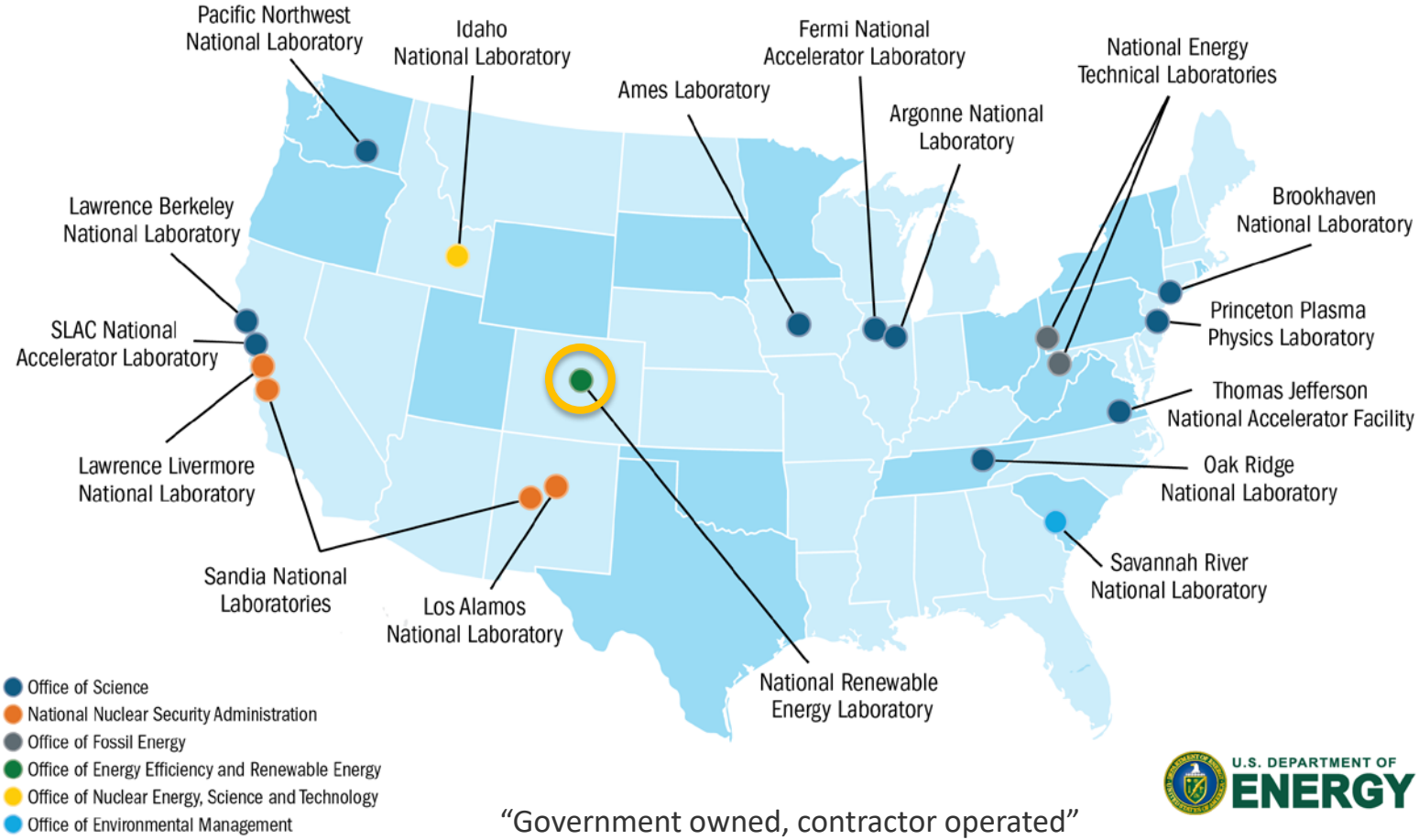
Senior Scientist

Complex Systems Simulation and Optimization

Overview

1. Introduction
2. Cybersecurity challenges and opportunities
3. AI for Cybersecurity
4. Ongoing AI Research at NREL
5. Cyber Range for AI Research
6. Challenges Leveraging AI for Cybersecurity

17 U.S. Department of Energy National Laboratories



"Government owned, contractor operated"

U.S. DEPARTMENT OF ENERGY

NREL at-a-Glance

2,926

Workforce, including

219 postdoctoral researchers

60 graduate students

81 undergraduate students

World-class

facilities, renowned technology experts

More than 900

Partnerships

with industry, academia, and government

Campus

operates as a living laboratory

NREL Science Drives Innovation

Renewable Power

Solar

Wind

Water

Geothermal

Sustainable Transportation

Bioenergy

Vehicle Technologies

Hydrogen

Energy Efficiency

Buildings

Advanced Manufacturing

Government Energy Management

Energy Systems Integration

Grid Integration

Hybrid Systems

Energy Security and Resilience

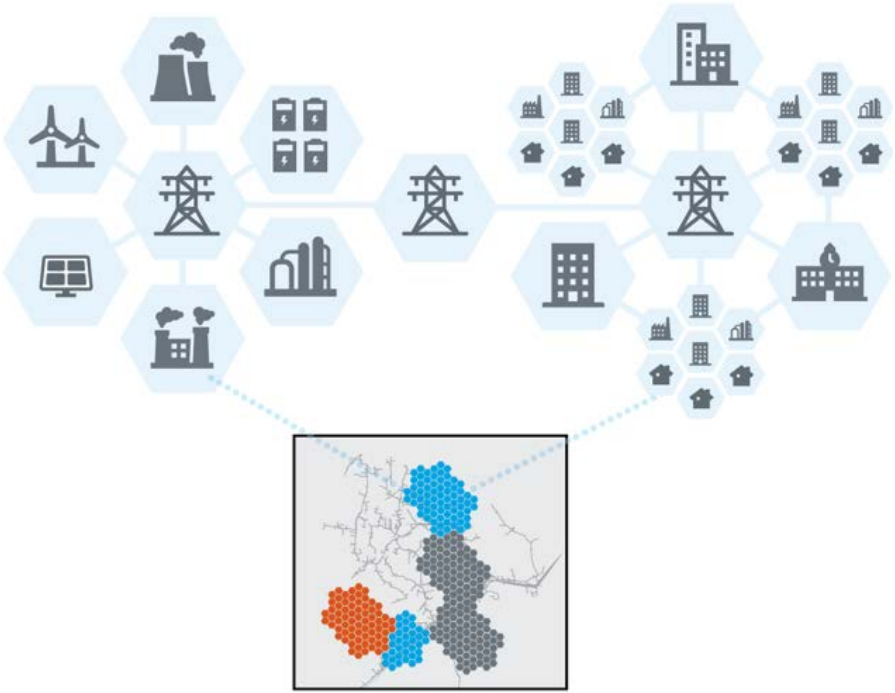
Cybersecurity Challenges and AI Research Opportunities

Future Grid Challenges

Features of future grid		Cybersecurity challenges
Distributed Authority	→	Distributed attack surface
Interconnected Communications	→	Many attacker pivot options
Hierarchal and Coordinated Operation	→	Cascading impacts and failures
Autonomous Operation	→	Trust in autonomous decisions
Scale of number of devices	→	Larger attack surface
Diversity of vendors and devices	→	Supply chain risks

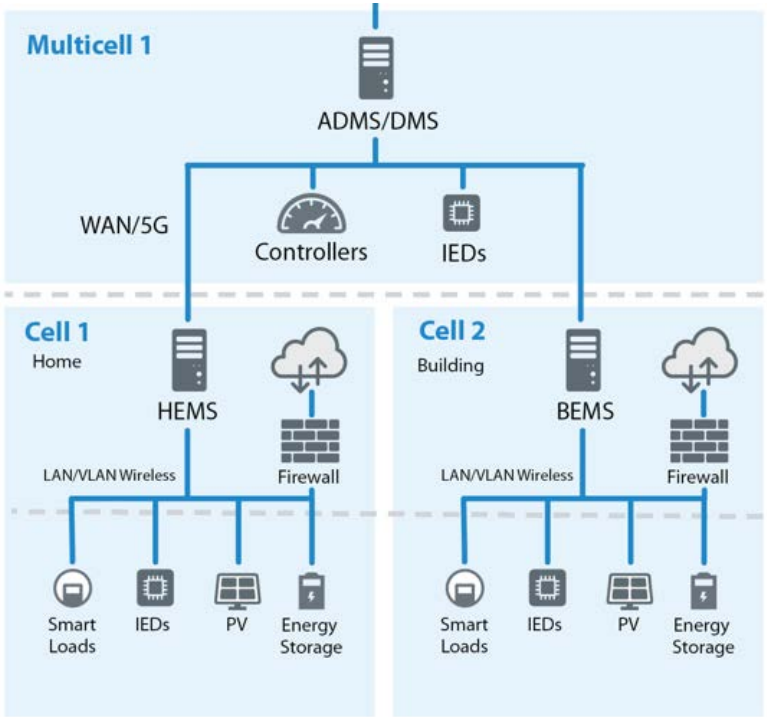
AI Research Opportunities

- **Distributed Attack Surface:**
  - AI for threat correlation across entities and geographies
- **Multiple Attack Entry Points:**
  - Hybrid Intrusion Detection for Energy System
- **Scale of number of devices:**
  - AI for attack anticipation using large datasets



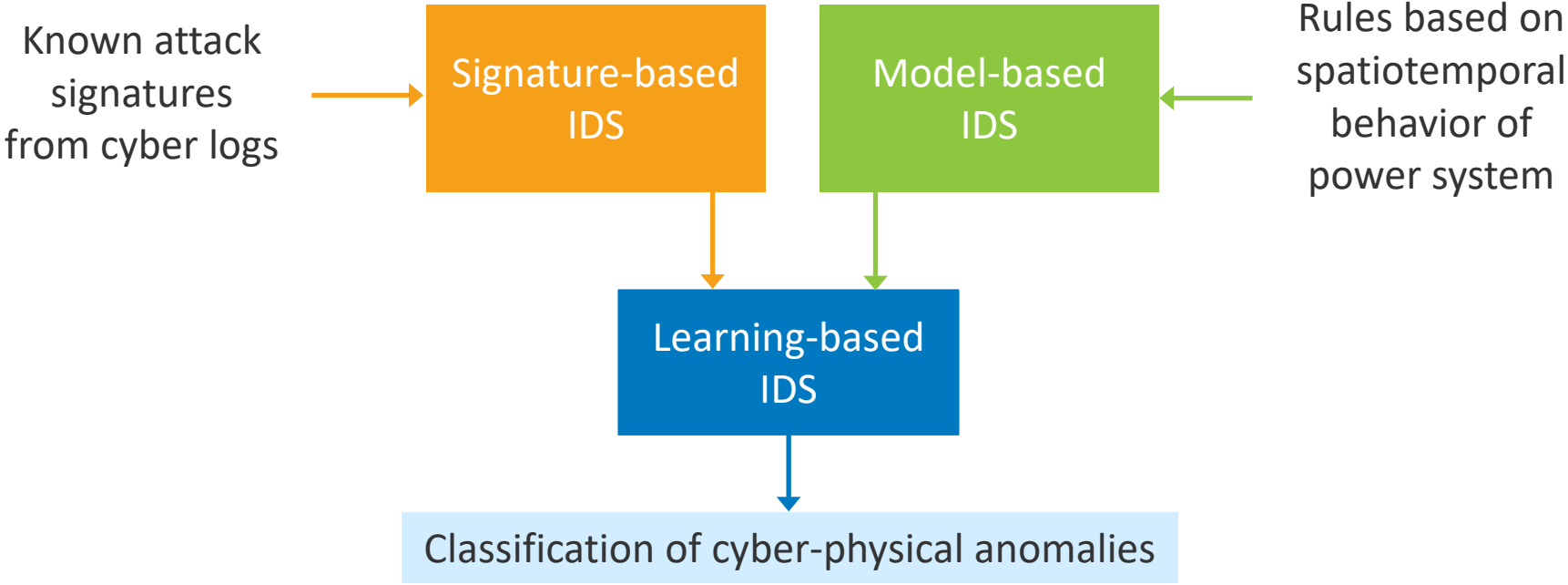
AI Research Opportunities

- **Cascading Impacts and Failures:**
  - Physics informed machine learning for attack detection at control layer
- **Supply Chain:**
  - AI for characterizing device behavior and trust scores
- **Autonomous Decision Making:**
  - Online real-time learning in adversarial environments



AI for Cybersecurity

Hybrid Intrusion Detection for Energy System



Hybrid Intrusion Detection for Energy System

Attack Vectors

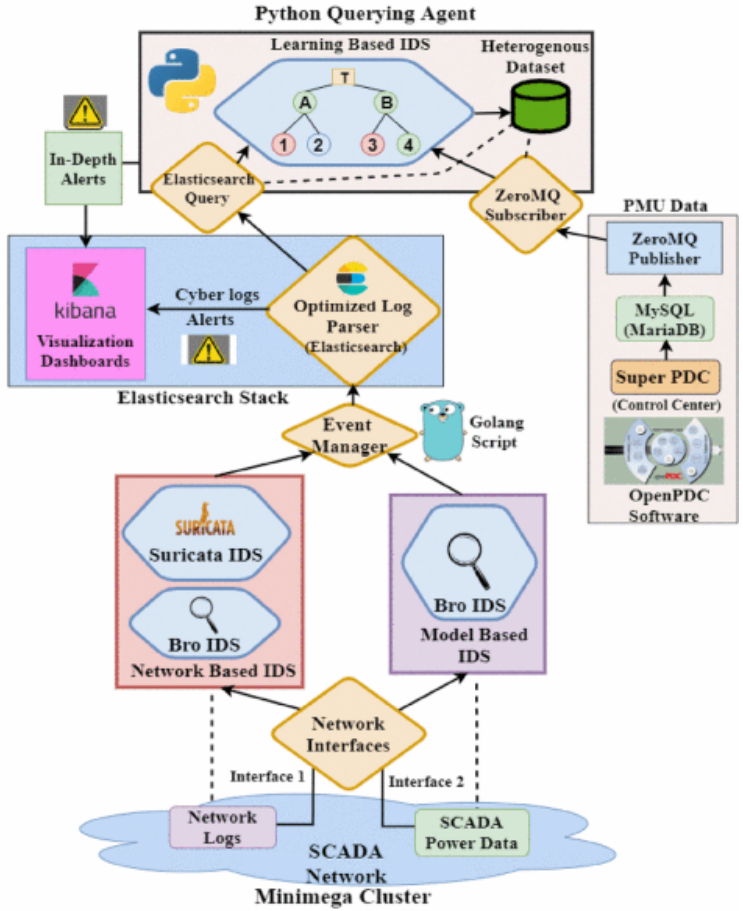
IT based attacks

- Network scanning
- Denial of Service
- IP spoofing

OT based attacks

- Malicious tripping (MITM)
- Pulse attack
- Ramp attack

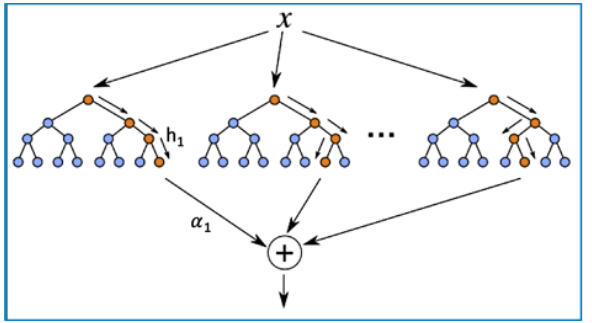
IDSs	IT Attacks	OT Attacks	Line Faults
Network-based IDS	100%	×	×
Model-based IDS	×	98.624%	×
Hybrid IDS (Network+Model+Learning)	100%	98.624%	97.9%



V. K. Singh, E. Vaughan, J. Rivera and A. Hasandka, "HIDES: Hybrid Intrusion Detector for Energy Systems," 2020 IEEE Texas Power and Energy Conference (TPEC), 2020, pp. 1-6, doi: 10.1109/TPEC48276.2020.9042544.

DDoS Attack Detection on SDN

- Well-tuned gradient-boosted decision tree for automated detection of DoS and DDoS attacks
- Optimal machine learning classifiers with general protocol case algorithm accuracy > 97%



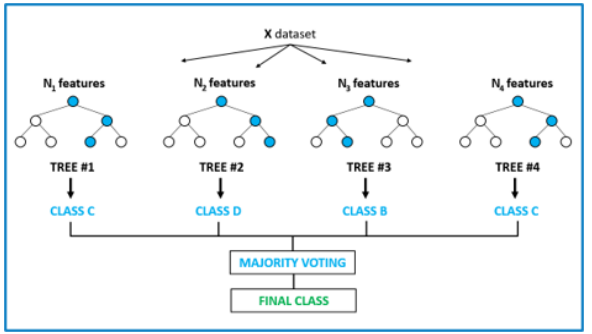


Table 5: *RF vs. XGB Performance Comparison.*

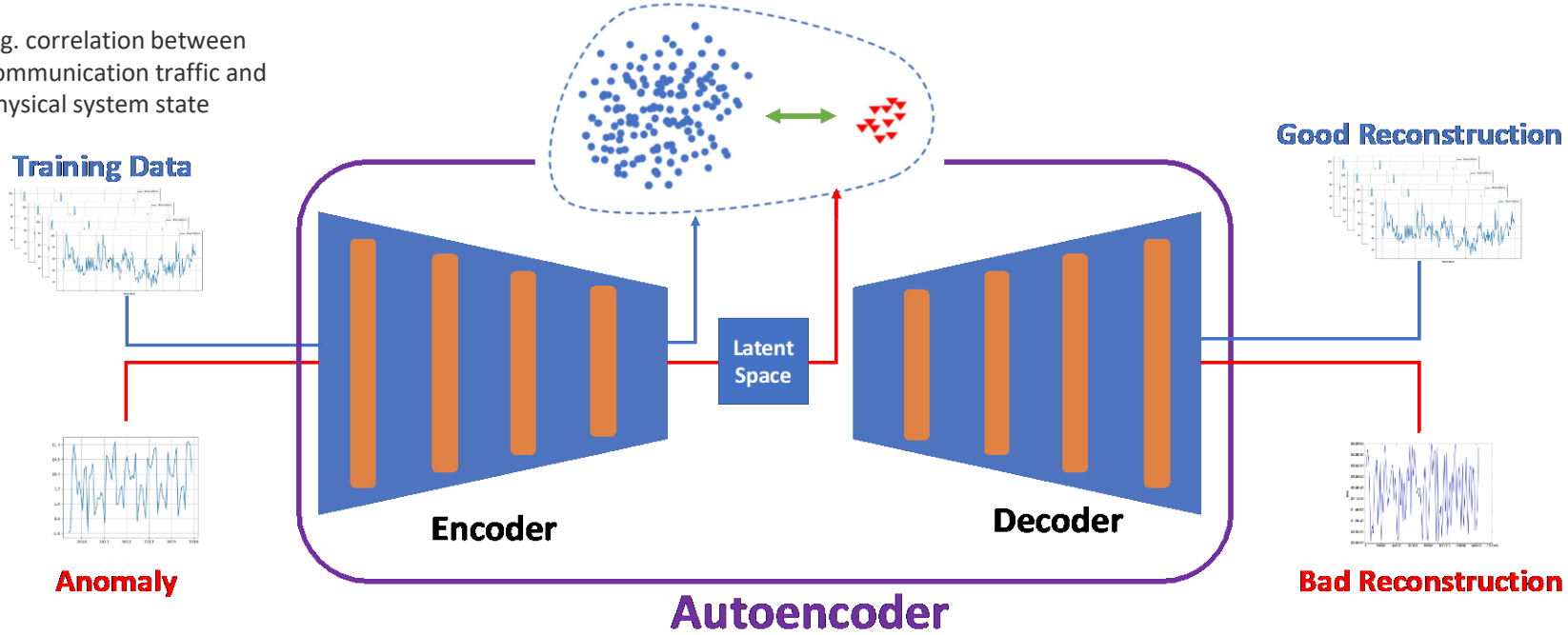
Algorithm	Accuracy	Precision	Recall	ROC AUC
Random Forest	97.15 ± 0.04	95.57 ± 0.07	97.17 ± 0.08	0.99
XGBoost	**97.66**	**95.33**	**98.81**	**0.99**

S. Corsetti, A. Purkayastha, A. Hasandka, and M. Samon, "Automatic DDoS Attack Detection on SDNs," The 2021 International Conference on Security and Management, 2021

Ongoing AI Research at NREL

Autoencoders for Anomaly Detection

e.g. correlation between communication traffic and physical system state



Autoencoders provide two means of anomaly detection: latent space distance measurement and reconstruction errors

NREL has experience using autoencoders to detect physical system anomalies, for example in wind plant flow physics

Reinforcement Learning for Distribution System Resilience

- Deep reinforcement learning (DRL) solves a critical load restoration (CLR) problem in distribution system following major outages or attacks.
- DRL controller restores load despite uncertainty in generation ability, network or user actions.
- DRL controller is less susceptible to generation forecast errors than model predictive control (MPC).

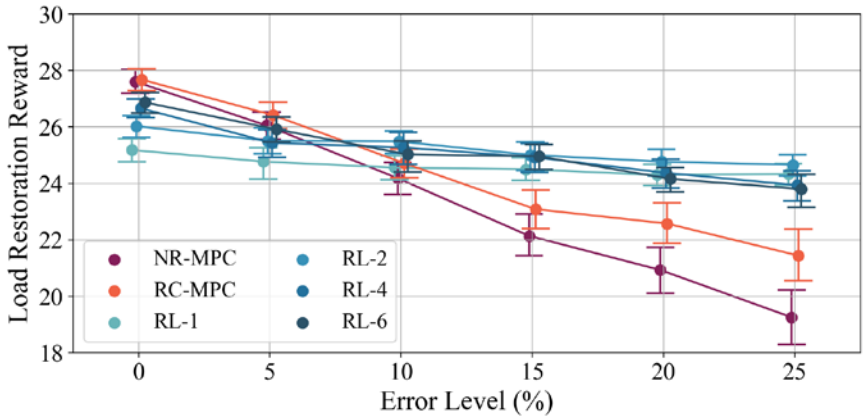
Restoration reward

Load shedding penalty

$$\underset{\mathbf{p}_t^{\mathcal{G}},\boldsymbol{\alpha}_t^{\mathcal{G}},\mathbf{p}_t,\mathbf{q}_t \forall t\in\mathcal{T}}{\text{maximize}} \quad \sum_{t\in\mathcal{T}}(r_t^{CLR}+v_t) \qquad \begin{cases} r_t^{CLR} \coloneqq \mathbf{z}^\top \mathbf{p}_t - \mathbf{z}^\top \text{diag}\{\boldsymbol{\epsilon}\}[\mathbf{p}_{t-1}-\mathbf{p}_t]^+ \\ v_t \coloneqq -\lambda \mathbf{1}_{N_b}^\top \text{diag}\{\delta \mathbf{v_t}\}\delta \mathbf{v_t}, \quad \delta \mathbf{v_t} = [\mathbf{v_t}-\overline{\mathbf{v}}]^+ + [\underline{\mathbf{v}}-\mathbf{v_t}]^+ \end{cases}$$

Subject to: Constraints related to DERs and loads control feasibility, power flow, etc.

$(\forall t \in \mathcal{T})$ For renewable DERs $\forall r \in \mathcal{R}$: $p_t^r \in [0, \overline{p_t^r}]$, and forecasts $\overline{p_t^r}$ is the source of uncertainty



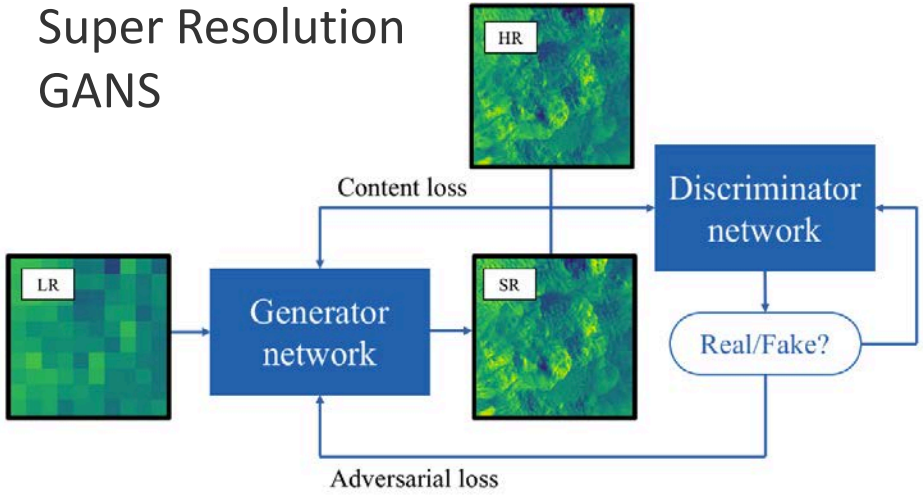
DRL controller vs MPC controller given different forecast horizons and error levels

Zhang, X., Eseye, A. T., Reynolds, M., Knueven, B., & Jones, W. (2021). Restoring Critical Loads in Resilient Distribution Systems Using a Curriculum Learned Controller (No. NREL/CP-2C00-78351). National Renewable Energy Lab.(NREL), Golden, CO (United States).

Adversarial Training

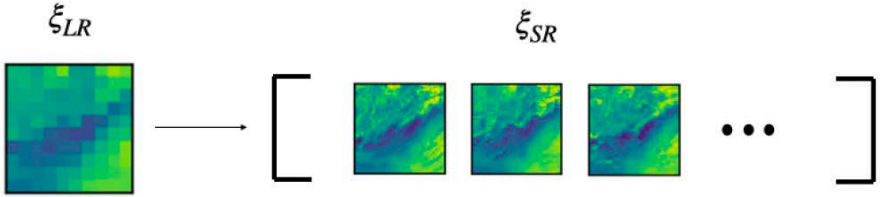
- Generative Adversarial Networks (GANS) train two competing neural networks: **generator** and **discriminator**
- Discriminator identifies fake/anomalous samples and generator produces new samples (fallback action/synthetic data)
- Adversarial attacks can use similar gradient information to identify weaknesses in NN's

Super Resolution GANS



Stengel, Glaws, Hettinger, and King, Proc. of the Natl Acad. Sciences, 2020

Conditional GANS



Hassanaly et al, under review in JCP, 2021.

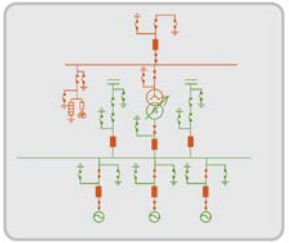
Cyber Range for AI Research

NREL's **Cyber Range** is a broadly capable hybrid private cloud solution for research involving operation and security for both telecommunication networks and physical systems.

With hardware-, controller-, and human-in-the-loop integration, NREL's Cyber Range offers a realistic, interactive dynamic environment and provides visualizations of the **digital and physical systems for real-time awareness, historical analysis, and future planning and operation**.

Distribution Utility Emulation Environment

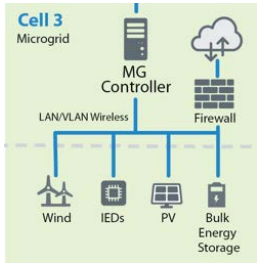
Distribution Utility
Electrical Nodes: 375K
No. of Customers: 134K
No. of Dist. Xmers: 11K

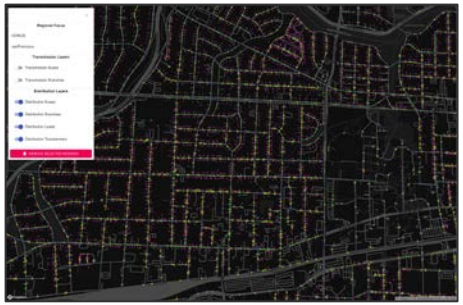


Control Center

Internet

AMI Aggregator





Utility WAN
VM

Substations and
Field Devices

AMI Environment

DER Comms Engine

GIS Visualization

OT Environment

Cyber Energy
Emulation Platform

Physical Evaluation of Future Cybersecurity Risk

EV and Building Control Testbed

Hydrogen Cycle Testbed

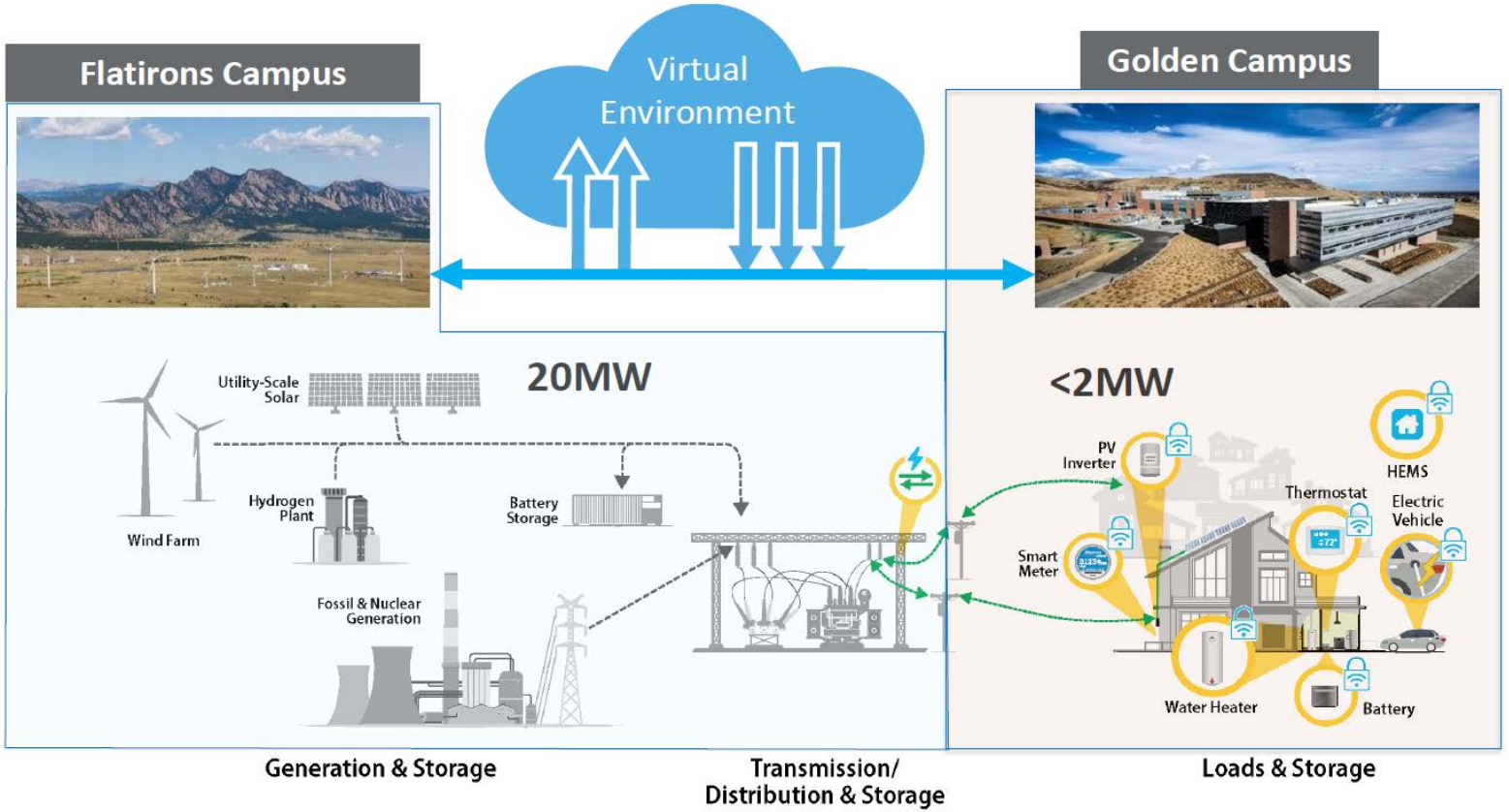
Extreme Testing Facility

Full Scale Wind-Solar-Storage

20-MW Controllable Grid

Distribution Management Testbed

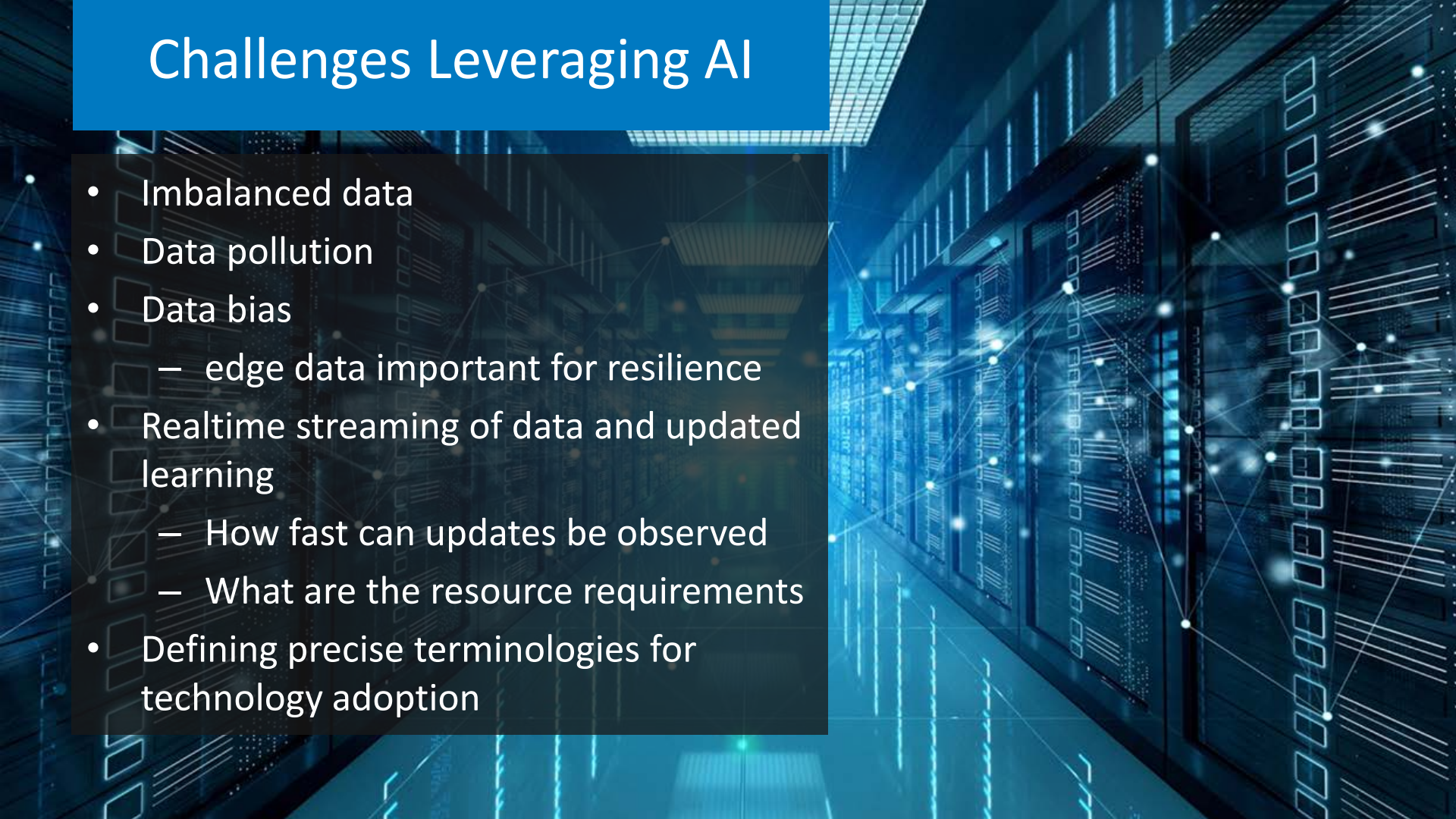
ARIES Research Platform – At-Scale



Challenges Leveraging AI

Challenges Leveraging AI

- Imbalanced data
- Data pollution
- Data bias
  - edge data important for resilience
- Realtime streaming of data and updated learning
  - How fast can updates be observed
  - What are the resource requirements
- Defining precise terminologies for technology adoption



Thank You!

Questions?

Richard.Macwan@NREL.gov

NREL/PR-5R00-81098

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the National Renewable Energy Laboratory's Energy Security and Resilience Center. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.