INL/MIS-23-75276-Revision-0

All Hazards Approach to Grid Modernization

October 2023

Megan Jordan Culler

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-23-75276-Revision-0

All Hazards Approach to Grid Modernization

Megan Jordan Culler

October 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517, DE-AC07-05ID14517

October 31, 2023

Megan Culler
Infrastructure Security

All Hazards Approach to Grid Modernization

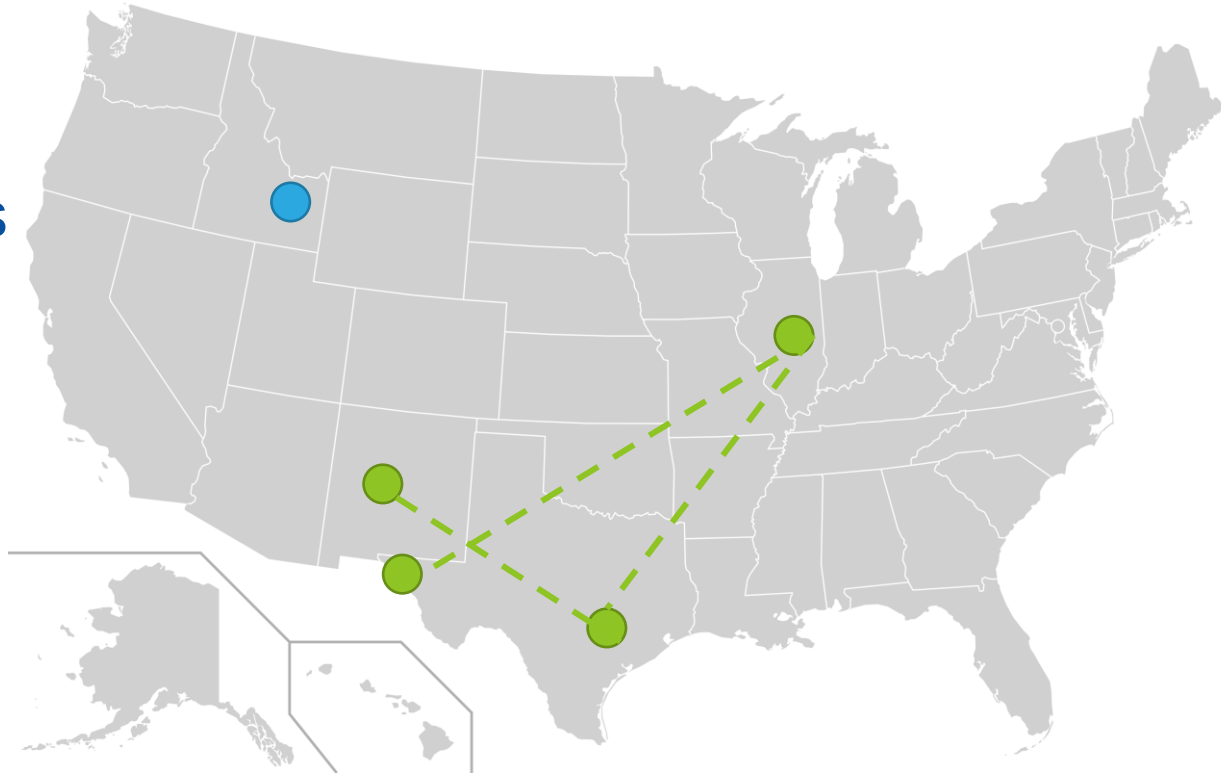
Click to edit subtitle

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

About Me

- Infrastructure Security Power Engineer
- Started as a Cybercore intern, then grad fellow
- Working remotely from El Paso, TX
- Newest hobby: Schutzhund dog sports



Resilience Hazards

The Record.
Recorded Future News

Leadership Cybercrime Nation-state People T

IMAGE: UNSPLASH / AMERICAN PUBLIC POWER ASSOCIATION

Daryna Antoniuk
May 25th, 2023

News Malware

New Russia-linked malware can physically harm power grids, Mandiant reports

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY MERCH

ANDY GREENBERG SECURITY SEP 12, 2023 6:00 AM

China-Linked Hackers Breached a Power Grid—Again

Signs suggest the culprits worked within a notorious Chinese hacker group that may have also hacked Indian electric utilities years earlier.

Resilience Hazards

ST. MARTIN PARISH

Lafayette man charged with shooting transformer at St. Martinville substation

by: Scott Yoshonis
Posted: Jul 11, 2023 / 01:45 PM CDT
Updated: Jul 11, 2023 / 01:45 PM CDT

A Lafayette man was arrested after he allegedly shot an electric substation in St. Martinville.

IMAGE: UNSPLASH / AMERICAN PUBLIC POWER ASSOCIATION

Daryna Antoniuk
May 25th, 2023

News Malware

New Russia-linked malware can physically harm power grids, Mandiant reports

ANDY GREENBERG SECURITY SEP 12, 2023 6:00 AM

China-Linked Hackers Bre

Signs suggest the culprits worked within a notorious Chin

tilities years earlier.

AMERICA

Sniper Attack On Calif. Power Station Raises Terrorism Fears

February 5, 2014 · 12:40 PM ET
Heard on All Things Considered
By Mark Memmott

5-Minute Listen + PLAYLIST

Fred Greaves /Reuters/Landov

Resilience Hazards

ST. MARTIN PARISH

Lafayette man charged with shooting transformer at St. Martinville substation

by: Scott Yoshonis
Posted: Jul 11, 2023 / 01:45 PM CDT
Updated: Jul 11, 2023 / 01:45 PM CDT

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigations

Boards, Policy & Regulation | Energy | Regulatory Oversight | Governance | Gas

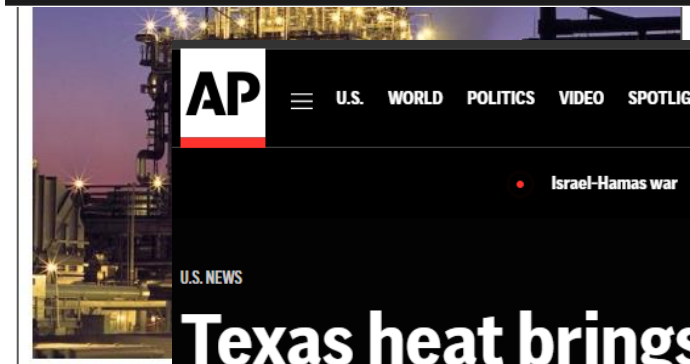
US energy regulator recommends revising reliability standards for extreme weather

Reuters

September 22, 2023 12:49 PM MDT · Updated a month ago

5-Minute Listen + PLAYLIST

Fred Greaves /Reuters/Landov



AP U.S. WORLD POLITICS VIDEO SPOTLIGHT ENTERTAINMENT SPORTS BUSINESS SCIENCE FACT CHECK CLIMATE HE

Israel-Hamas war Trump lawyer pleads guilty New Orleans 'superfog' China defense minister NCAA

U.S. NEWS

Texas heat brings the state's power grid closest it has been to outages since 2021 winter storm

IMAGE: UNSPLASH

Daryna Anto

May 25th, 2023

News Mal

tilities years earlier.

Resilience Hazards

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigations

Boards, Policy & Regulation | Energy | Regulatory Oversight | Governance | Gas

US energy regulator recommends revising reliability standards for extreme weather

Reuters

September 22, 2023 12:49 PM MDT · Updated a month ago

The New York Times

Electric Grids Are a Hidden Weak Spot in World's Climate Plans, Report Warns

Even as technologies like wind, solar and electric cars spread, nations are falling far behind in building the power lines needed to support them.

Share full article

The power grid in Cathedral City, California. Alex Welsh for The New York Times

ST. MARTIN PARISH

Lafayette shooting Martinvil

by: Scott Yoshonis
Posted: Jul 11, 2023 / 01:45 PM
Updated: Jul 11, 2023 / 01:45 P

5-Minute Listen + PLAYLIST

AP U.S. WORLD POLITICS VIDEO SPOTLIGHT ENTERTAINMENT SPORTS BUSINESS SCIENCE FACT CHECK CLIMATE

Israel-Hamas war Trump lawyer pleads guilty New Orleans 'superfog' China defense minister NCAA

BUSINESS

Electrical grids aren't keeping up with the green energy push. That could risk climate goals

AP

U.S. NEWS

Texa grid sinc

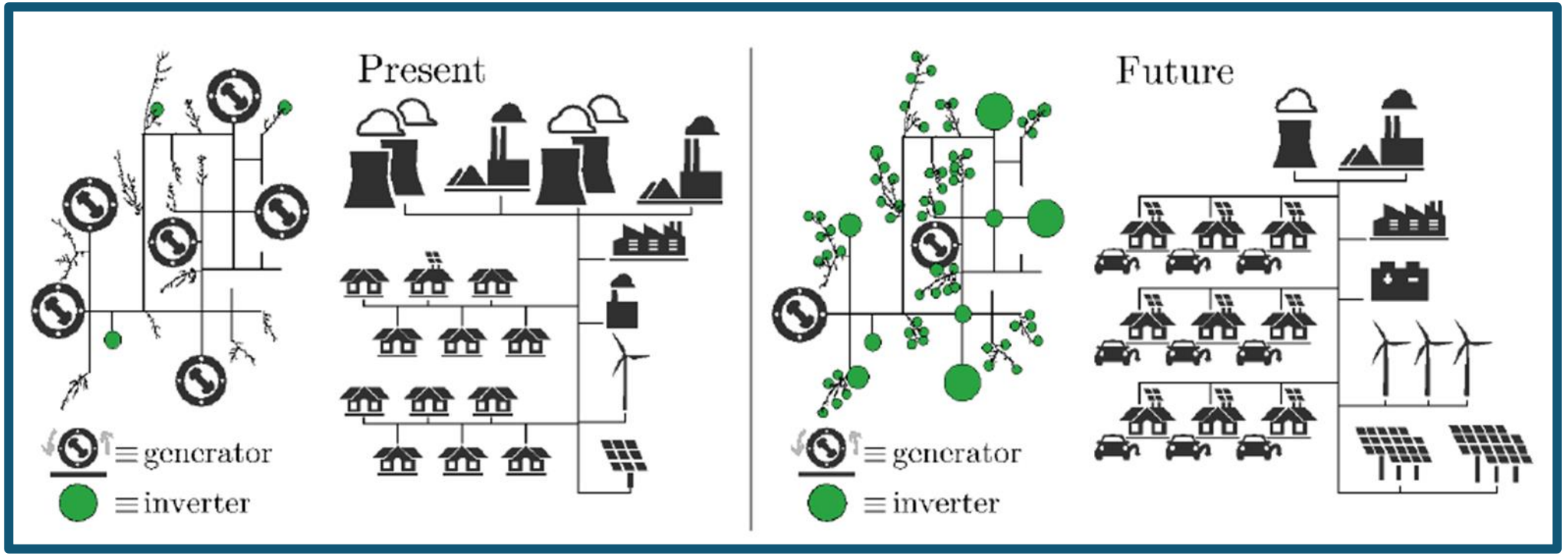
IMAGE: UNSPLASH

Daryna Anto
May 25th, 2023

News Mal

ars earlier.

Grid Modernization: Changing Generation Paradigms

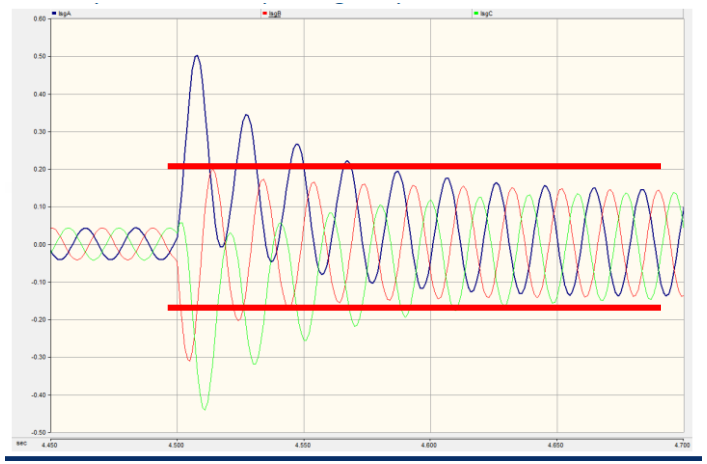


Remote, Large Scale
Thermal Systems
Nuclear, Coal, NG, Oil
Load Centers
Rotating Loads

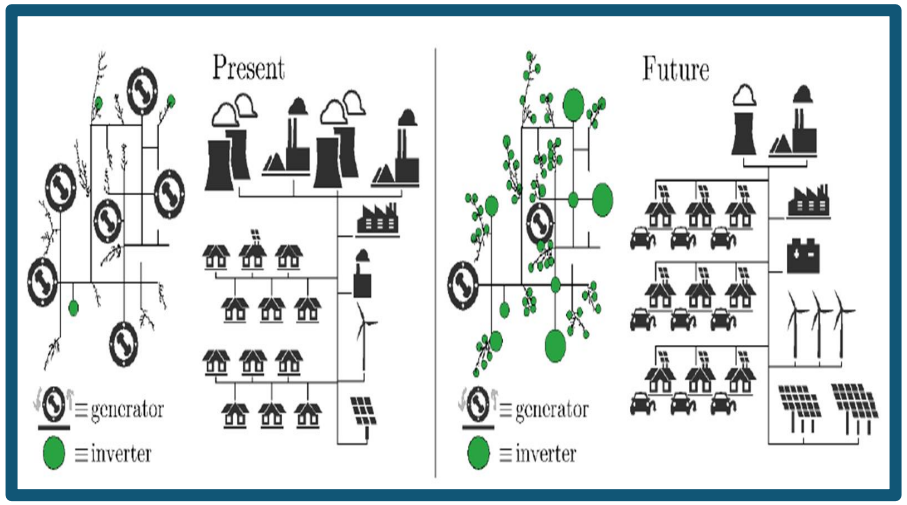
Distributed at many scales
Mostly Inverter Based
Renewable
Variable
Electrical Energy Storage
Smart Load
Bi-directional

Modernized Grid Requires New Operations

Grid or Power Systems operations today are based upon solution and methodologies tied the physics and electrical characteristics of synchronous generators, as we transition to a carbon free renewable grid, the physics and electrical characteristics of Inverter Based Resource (IBR) are not the same as synchronous generators, ultimately eroding effectiveness of existing methodologies.

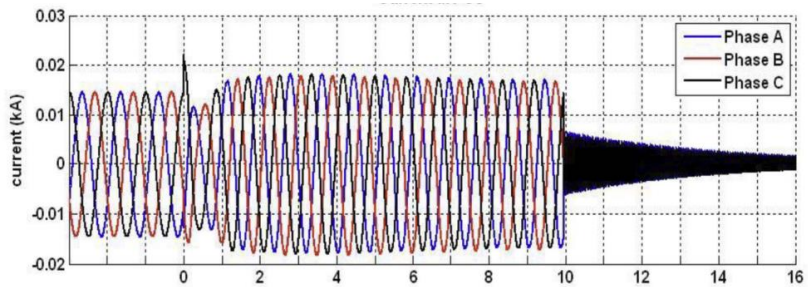


Fault current contribution by generators can be 6 to 10x



Challenge

Opportunity



Generic Model:

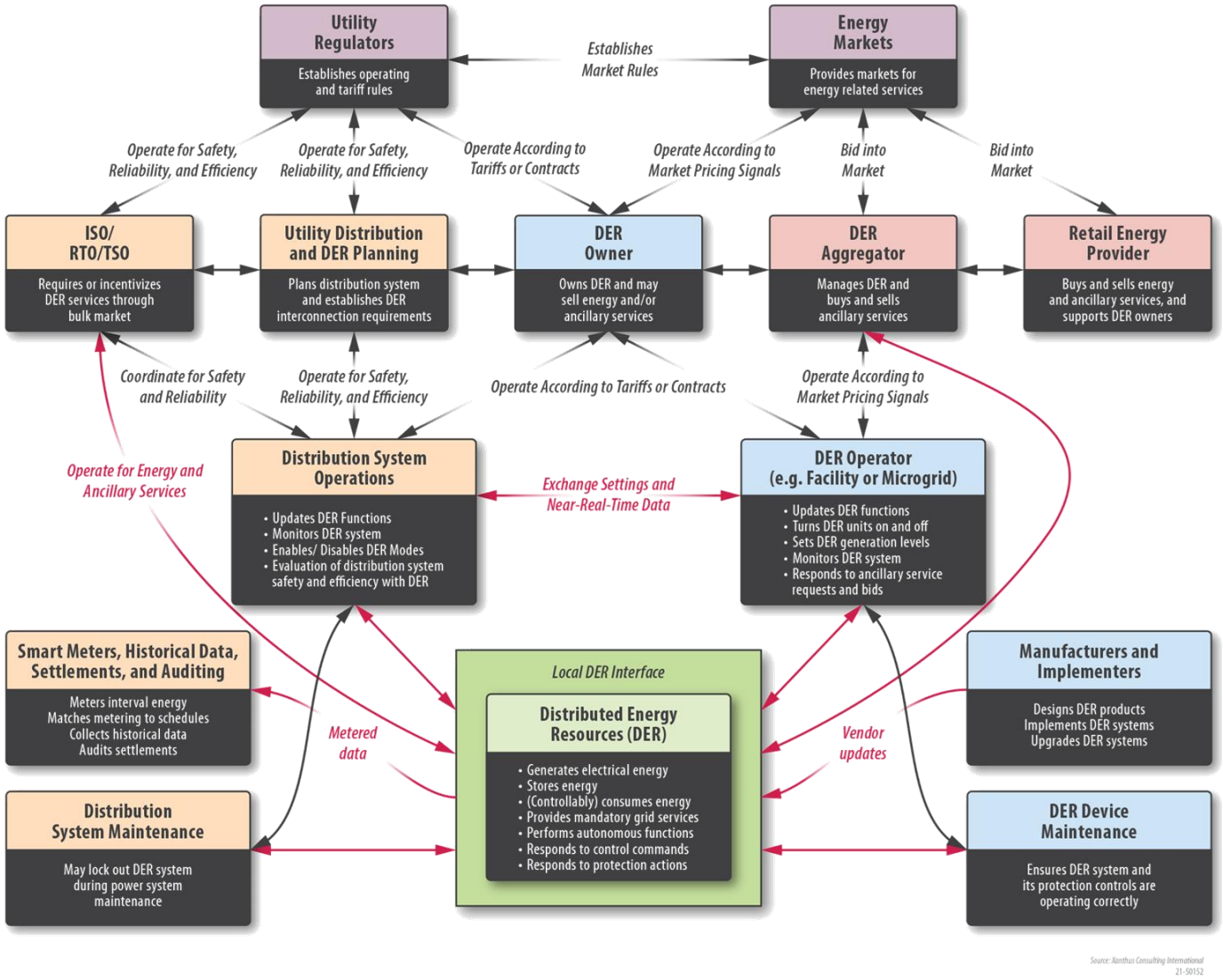
- Operate for 4 to 10 cycles after a fault incident even if the PCC voltage drops below 50%.
- The current is usually between 100% and 120% of the rated power of the inverter.
- The current contribution level is a function of the voltage at the terminal of the PV inverter (PCC) during a fault and thereby the type and location of the fault.

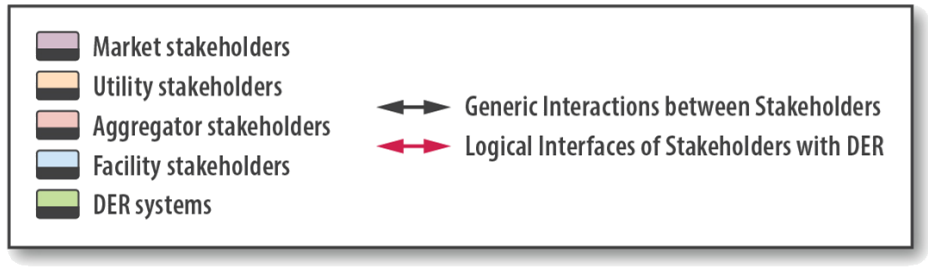
Fault current contribution by generators can be 1 to 1.2x

Sensing local and Act local
– today's protective relaying

Sensing Everywhere and Act local
– tomorrow's protective relaying

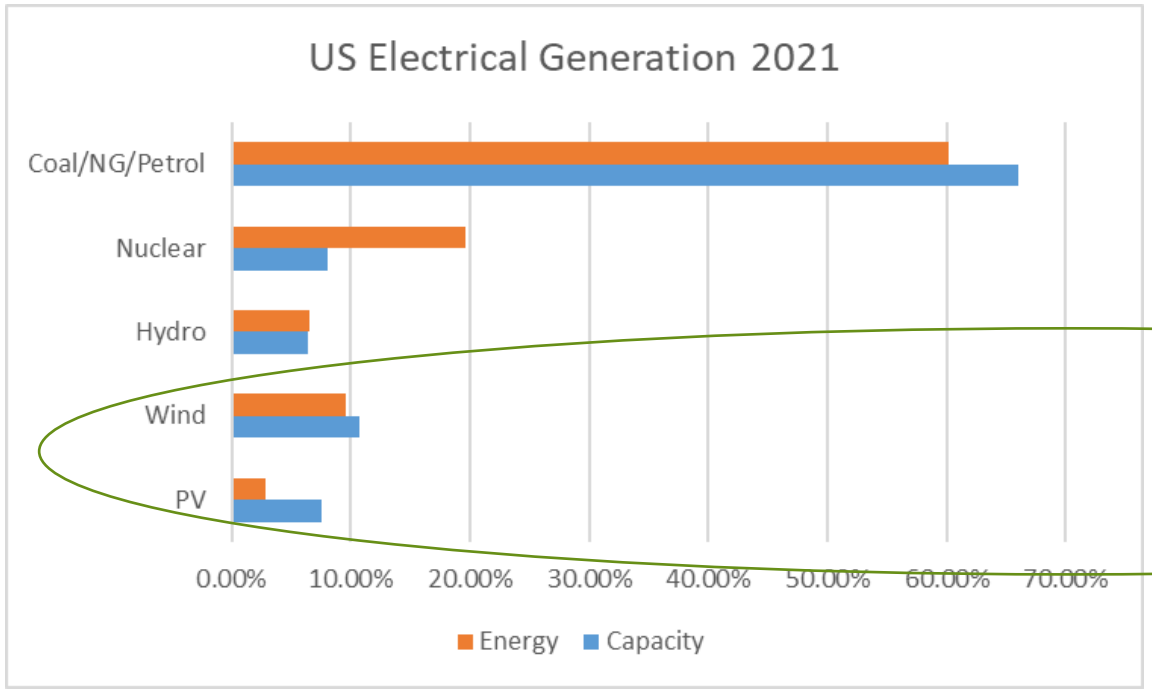
DER Stakeholders



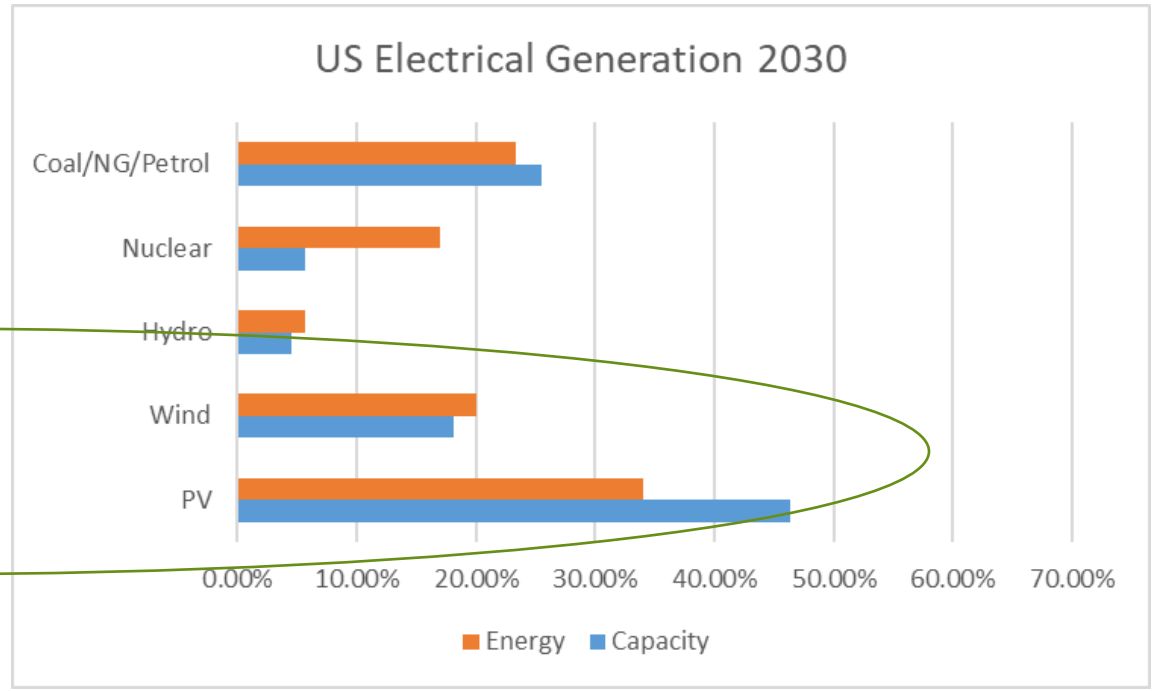


2021 to 2030* Capacity and Energy Production

EIA Energy and Capacity

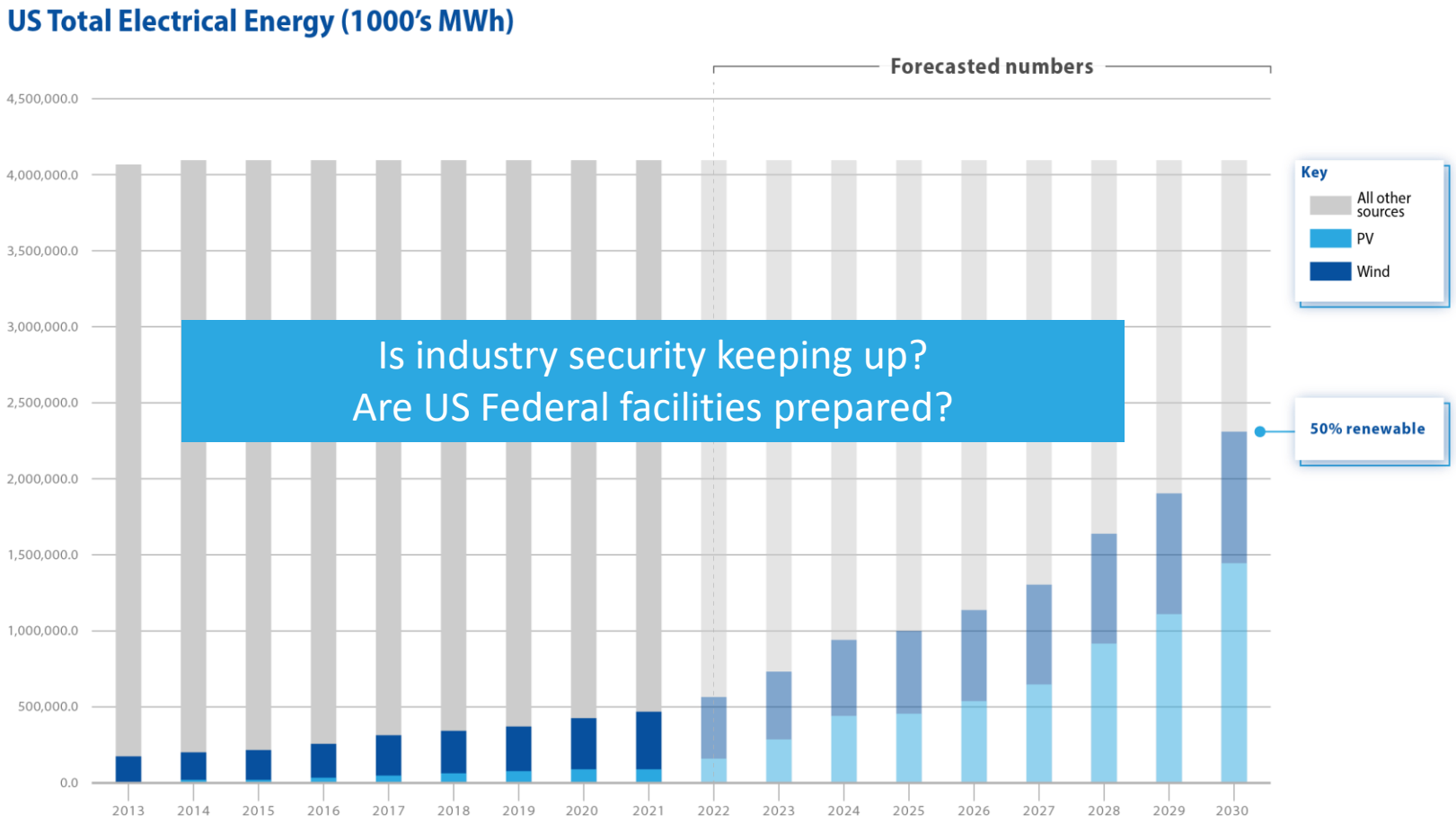


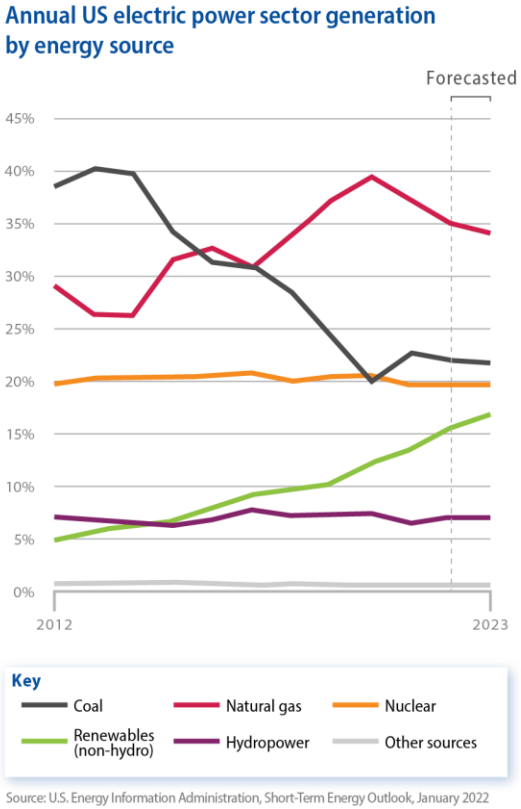
SETO and WETO Goals



* WETO 2030 Goals and Curve Fitting to SETO 2035 Goals, with Estimated 26 million EV's sold in 2030

To achieve high renewable energy targets of 50% by 2030, current trends will need to grow at a much higher rate.





Source: U.S. Energy Information Administration, Short-Term Energy Outlook, January 2022

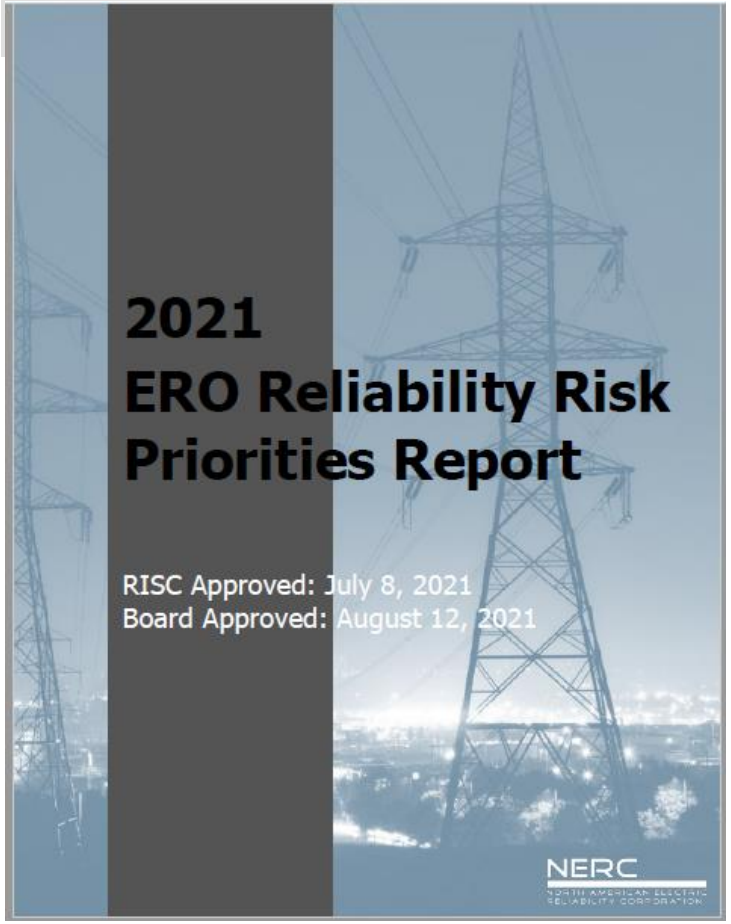
Future of DER

Changes in DER		Impact to cybersecurity
• Growth of stakeholders	→	• Increase in attack surface
• Growth of endpoints	→	• Increase in attack surface, vulnerabilities
• Electrification of loads	→	• Increase in potential impact
• Aggregation of DER	→	• Increase in potential impact
• Increasing regulation	→	• Standards more widespread
• Digitization of monitoring	→	• Explosion of data to process and store
• Digitization of control	→	• Need for resilience of critical functionality
• Distribution of control	→	• Management of roles and privileges
• Smarter inverters	→	• Increase in attack surface

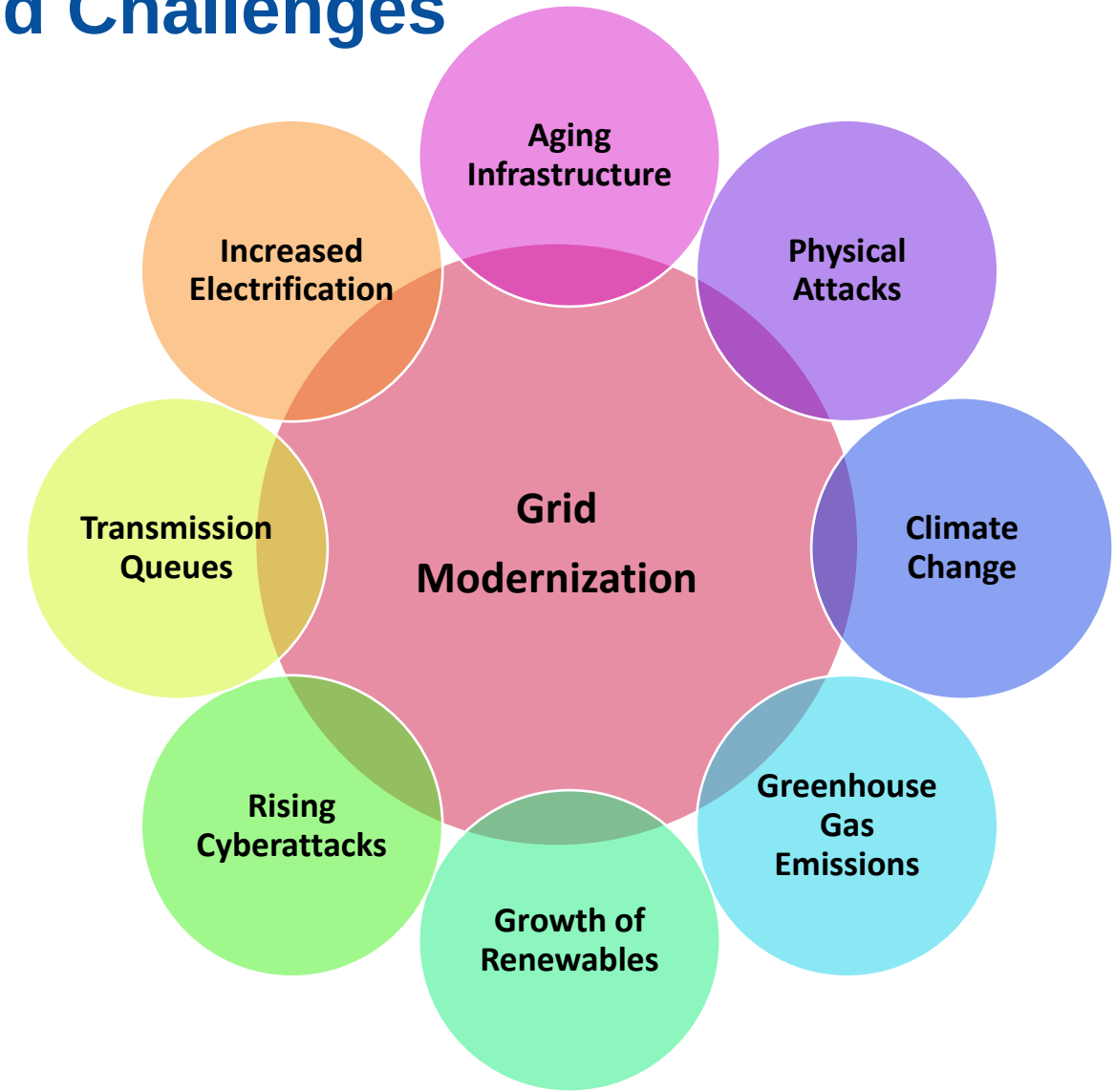
Risk for the Grid

Changing Resource Mix and Cybersecurity are the highest Ranked Risks

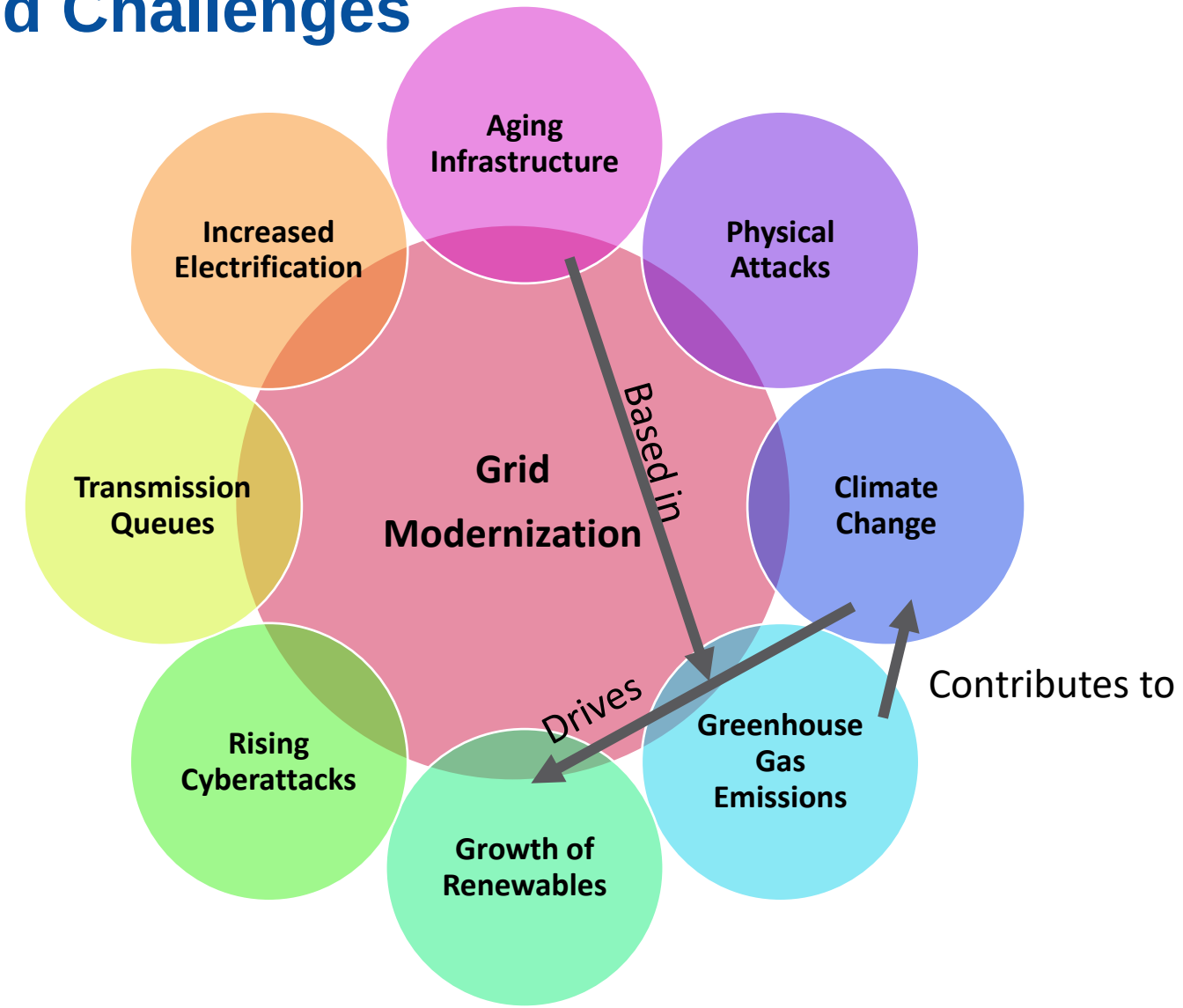
NERC Reliability - Risk



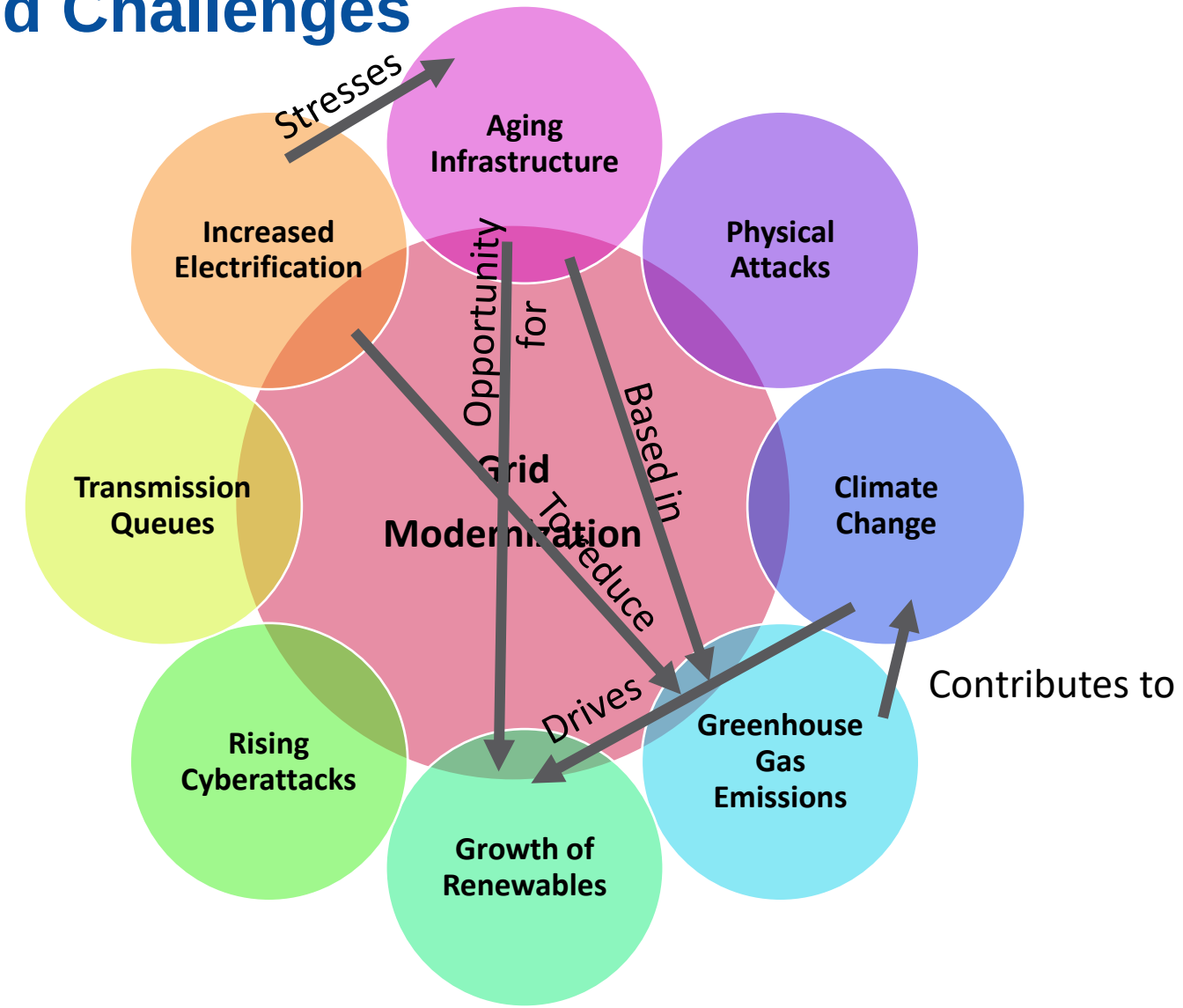
Interconnected Challenges



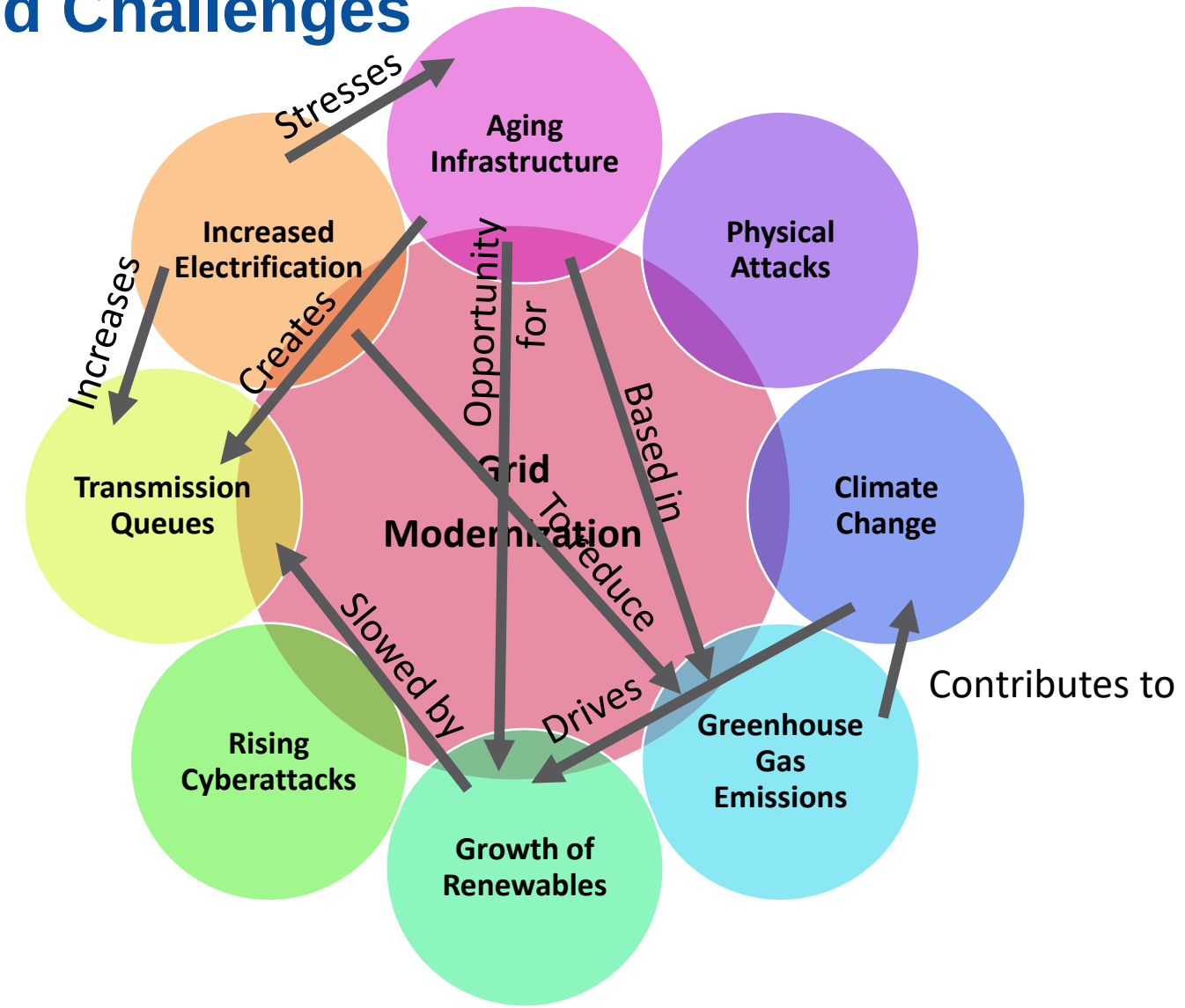
Interconnected Challenges



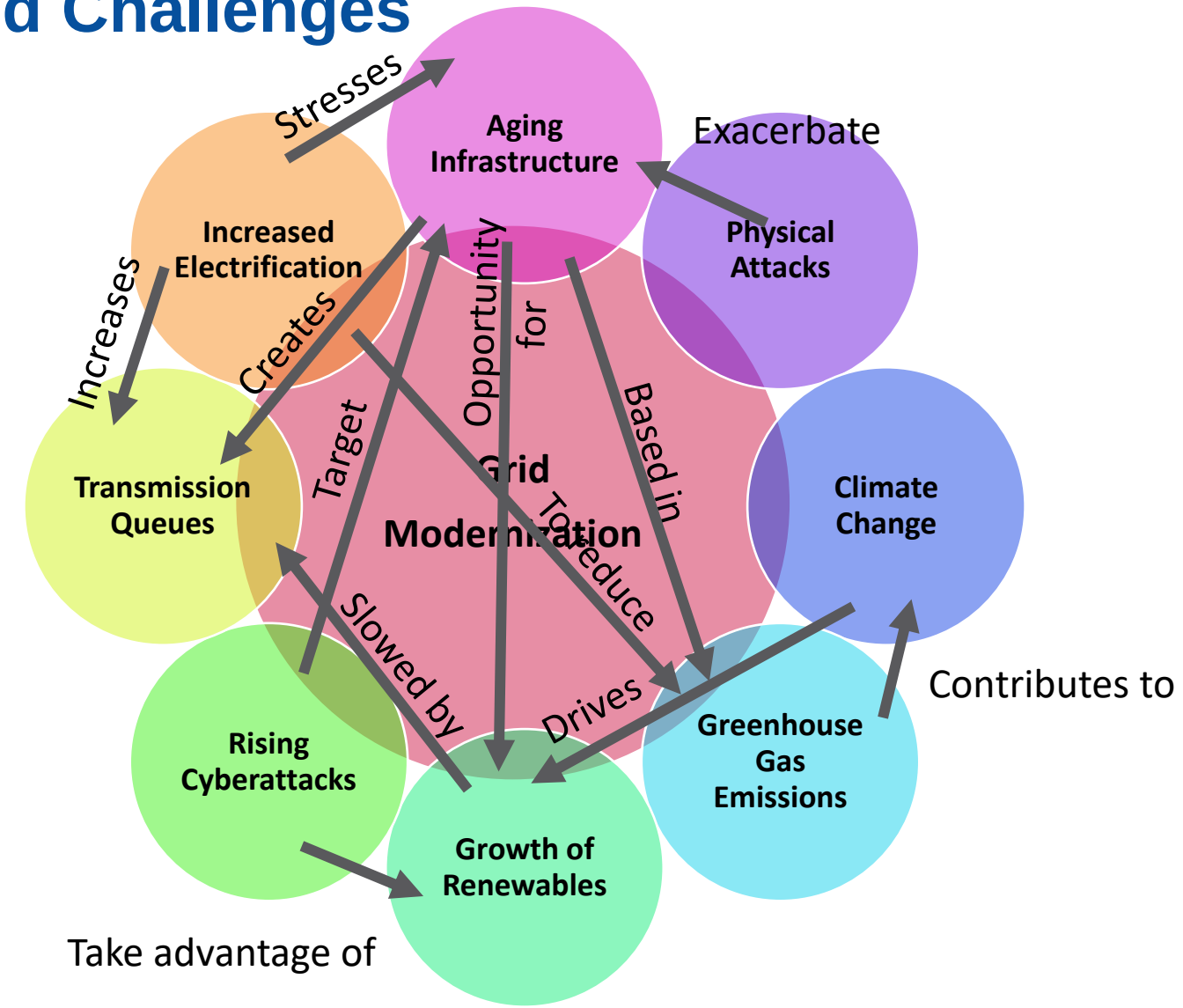
Interconnected Challenges



Interconnected Challenges



Interconnected Challenges



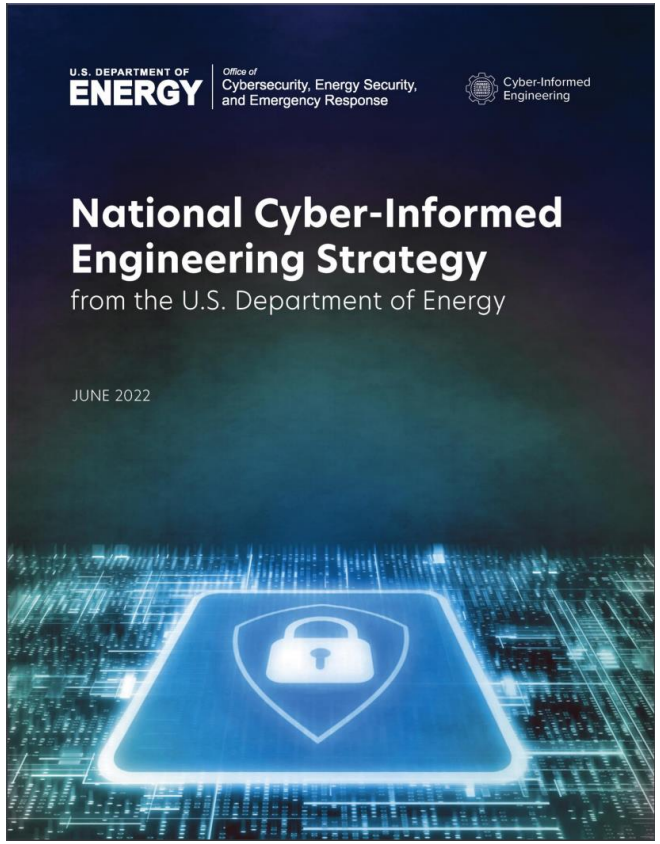
Risk-based Approach to Grid Modernization

Understand and prioritize the risks

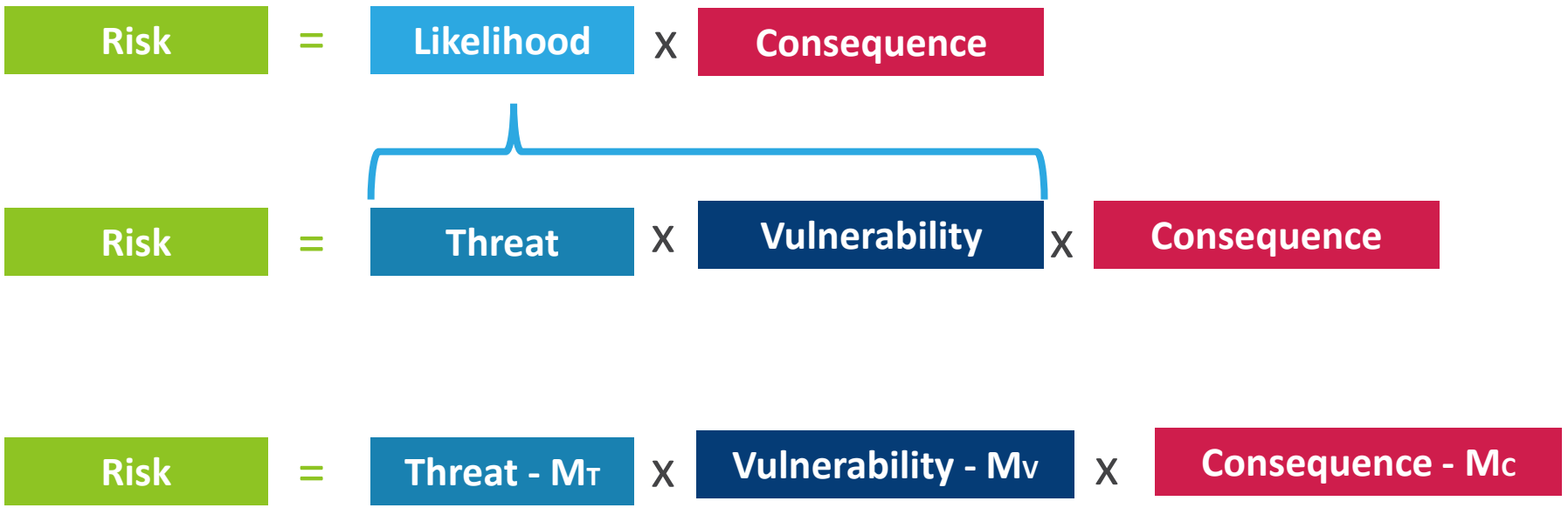
Rank disparate risks on a comparative scale

Risk mitigation by design

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5



Risk Management Architecture



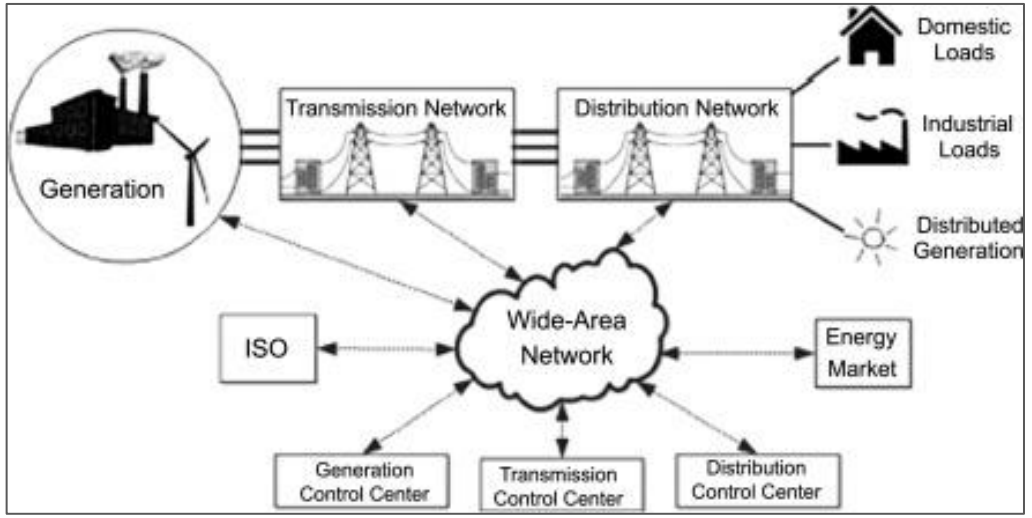
- Risk management comes from mitigating each element individually
- Resilience measures can apply to any element

Risk Management Architecture: Threats

Threat = **Intent** x **Capability** x **Opportunity**

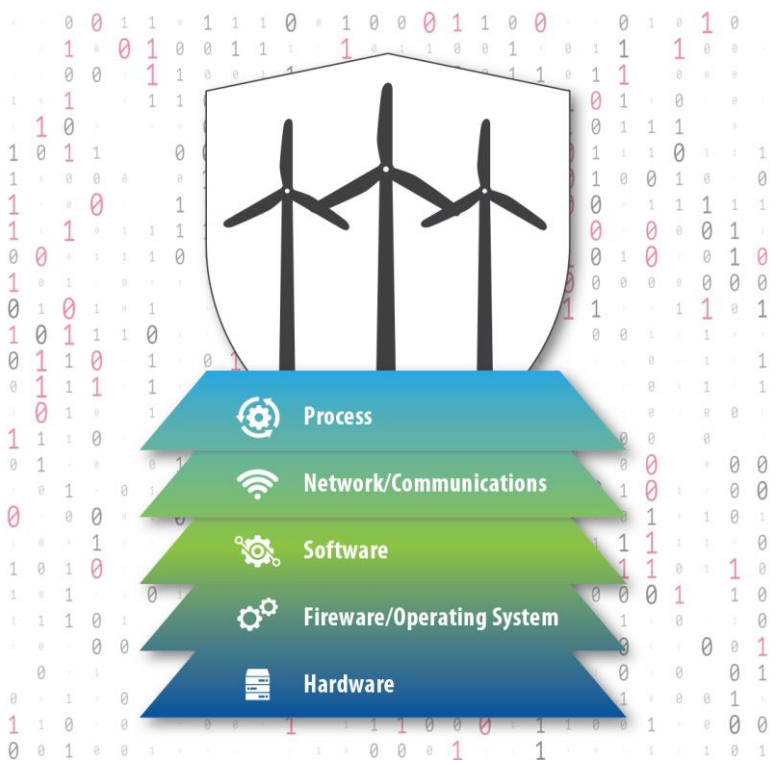
- **Intent:** may be intentional (driven by a particular objective) or unintentional
- **Capability:** skills and funding, intensity
- **Opportunity/Exposure:** Access to a target

Capability	Example
Hacker	Spower Firewall DoS attacker
Insider	3rd party stakeholders
Organized group	Ransomware organizations
Hostile nation-state or terrorist	Nation-state sponsored APT



Risk Management Architecture: Vulnerability / Susceptibility

- **Vulnerability:** a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions on a system
- **Susceptibility:** a liability to being influenced or harmed by a particular thing
- May be a flaw in either design or implementation
- Can occur at any layer of the system



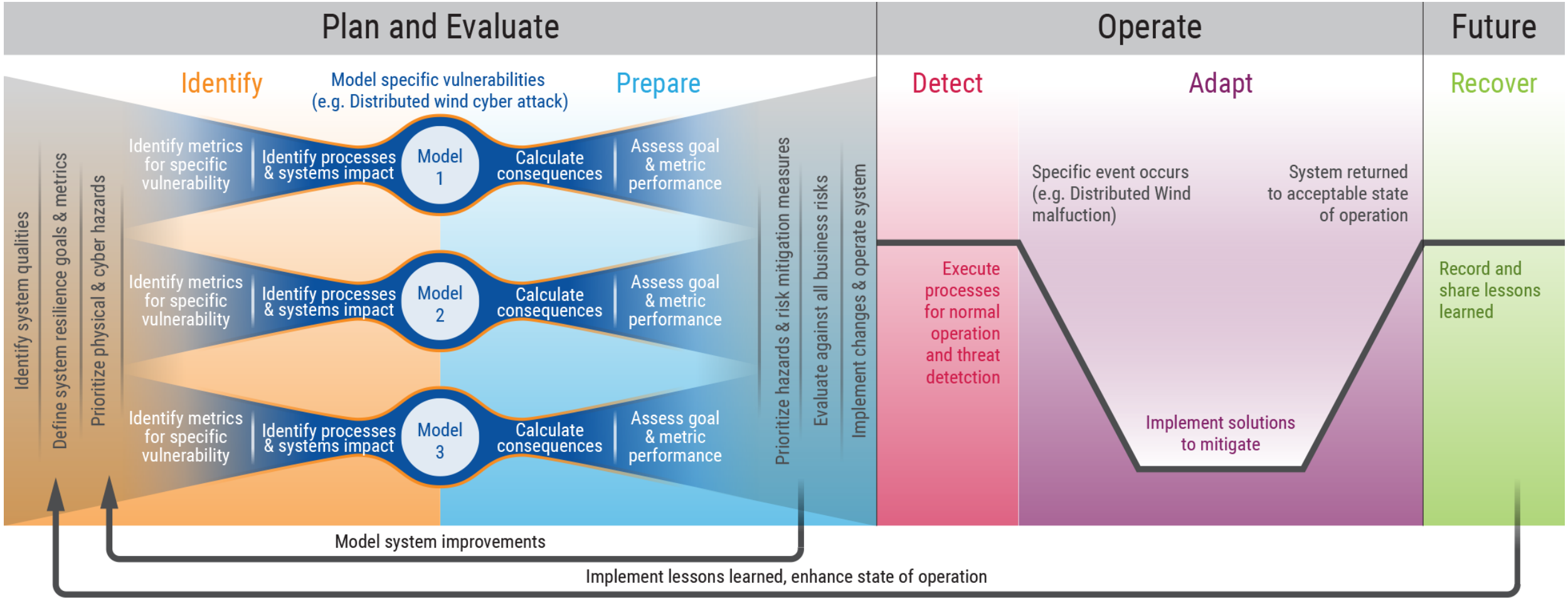
Risk Management Architecture: Consequences

Loss	Denial	Manipulation
• Loss of View • Loss of Control	• Denial of View • Denial of Control • Denial of Safety	• Manipulation of View • Manipulation of Control • Manipulation of Safety • Manipulation of sensors and instruments

Who Experiences the Consequence?

- Utility
- Manufacturer
- Integrator
- Owner/Operator
- Customer

Resilience Framework for Electric Energy Delivery Systems



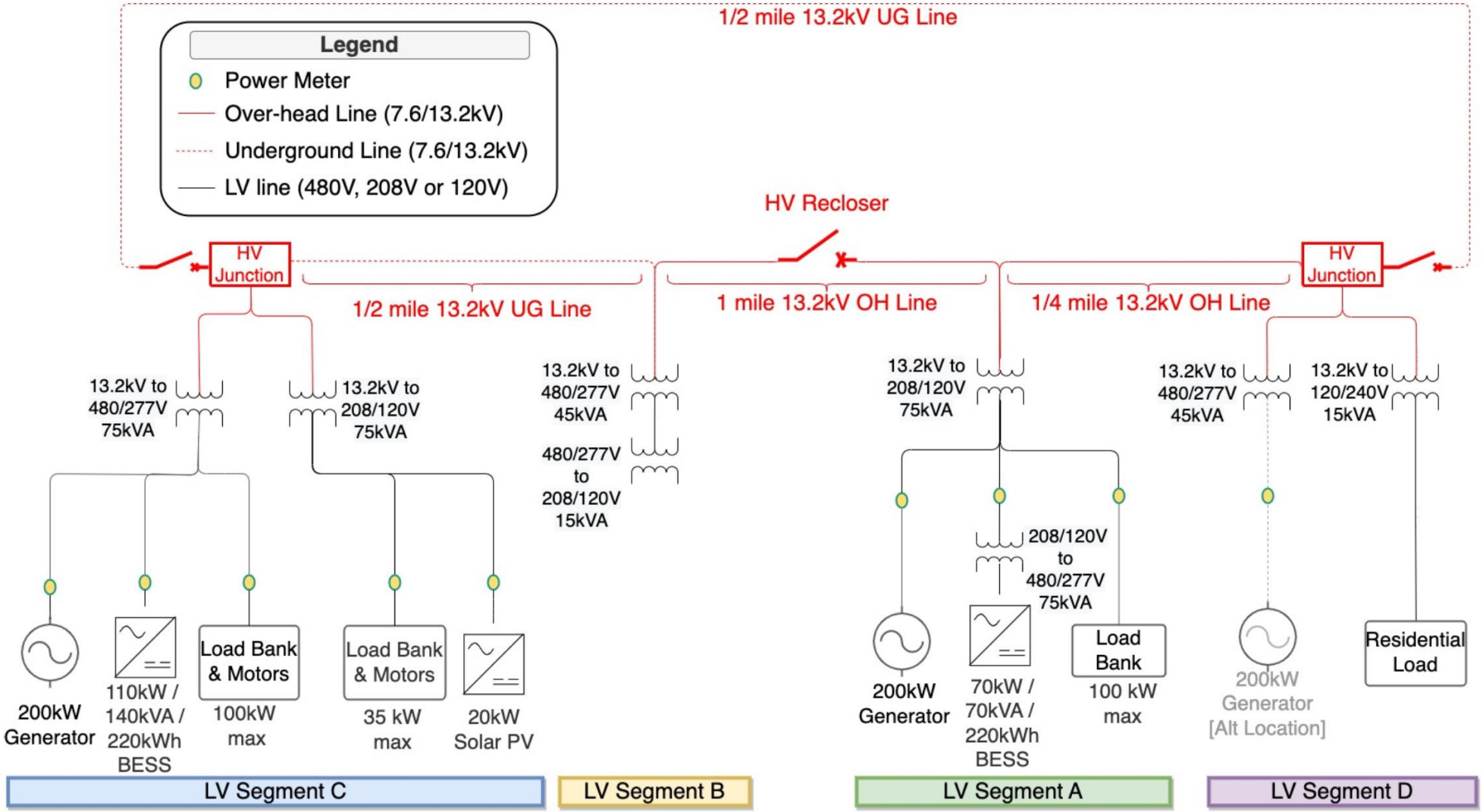
GMLC 2.3.1: Validation, Restoration and Black Start Testing of Sensing, Controls and DER Technologies at Plum Island

- Key objectives
  - ***Improve grid reliability and security*** by developing and demonstrating (through field-testing) novel methods of ***power system recovery*** (black start) using ***battery energy storage and solar PV systems***.
  - Develop recovery methods that are resilient to an ongoing cyber attack
  - Develop new sensing and measurement tools that can assist in the recovery process
  - Develop and test new model calibration methods utilizing high resolution sensor data

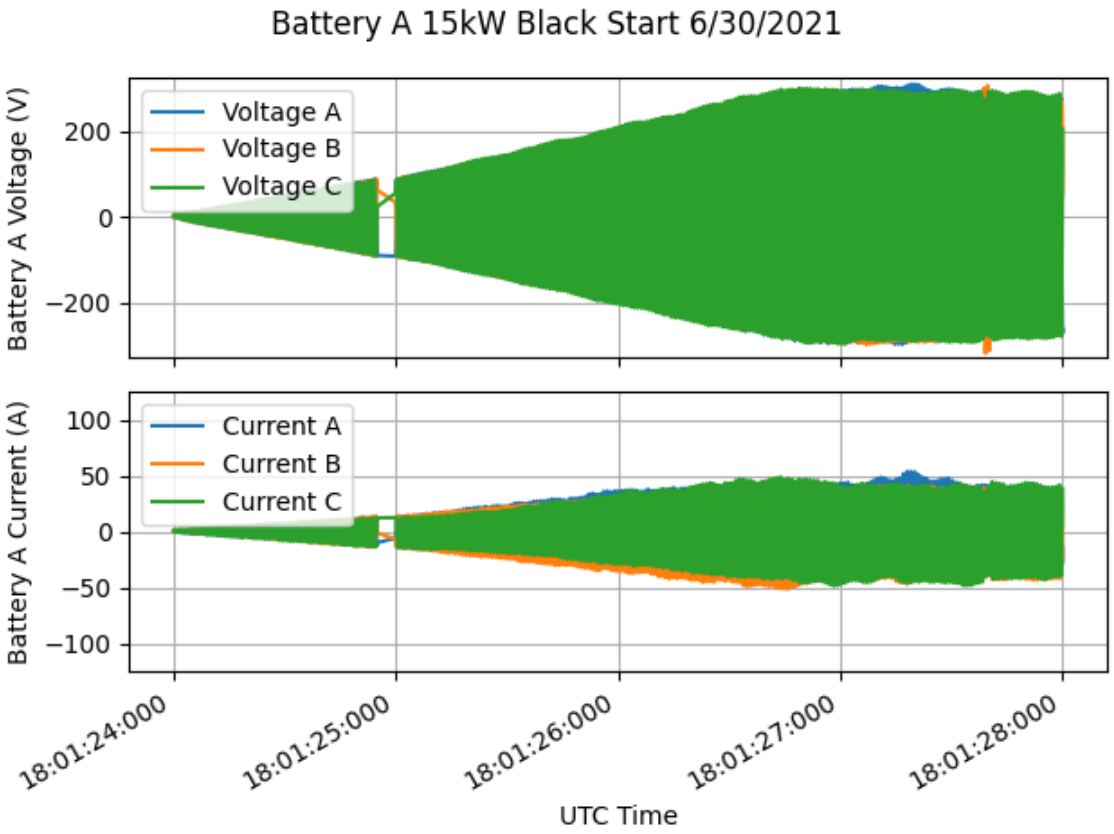
Introduction: Testing Site and Next Steps

- Plum Island Microgrid Test Bed
  - GMLC project added renewables, storage and sensors to the existing Plum Island experimental microgrid, originally constructed to support the DARPA RADICS program
    - For more info on DARPA RADICS exercises: https://www.wired.com/story/black-start-power-grid-darpa-plum-island/
  - Equipment added included: Two 100kVA grid-forming batteries, 20kW solar PV, power meters with PMU and oscillography capture functionality, data logging and visualization system

Plum Island Microgrid



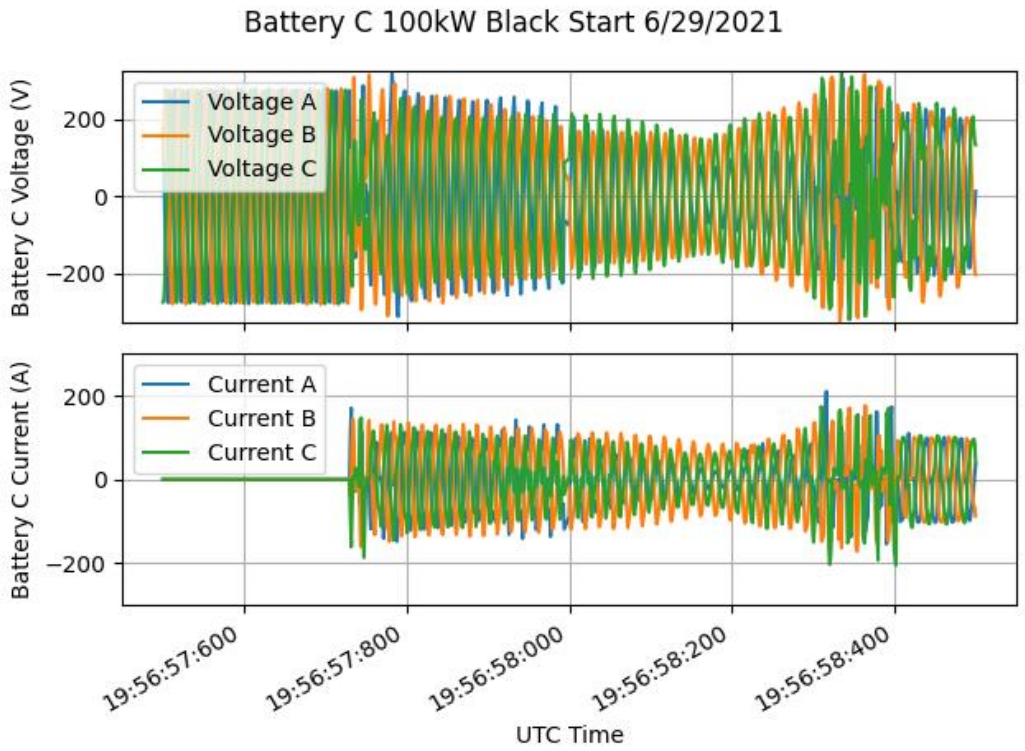
Battery Black Start Overview

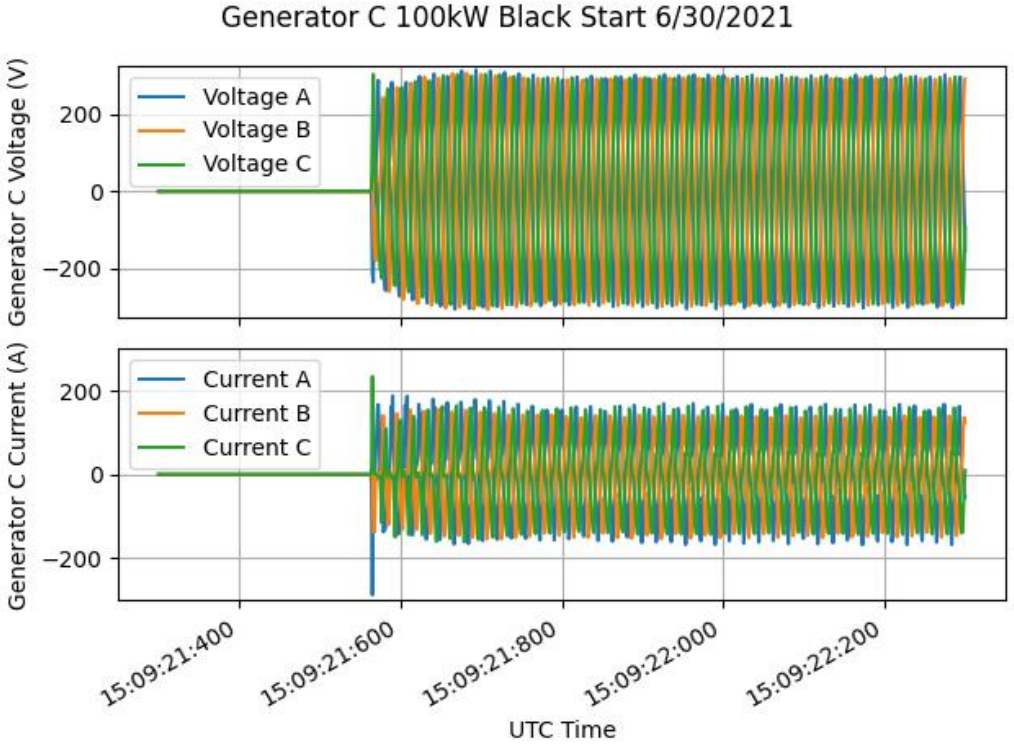


- Battery A successfully black starts 15kW of load
- Black starting into resistive load leads to **half** the peak current in **three-quarters** the time
- Batteries able to support load steps after black start up to total load equal to rated power of battery
- Magnitude of ***load step*** that batteries can support in grid-forming is greater than magnitude of ***load*** that they can black start into

Inverter-based resource (battery) successfully black started Plum Island microgrid.

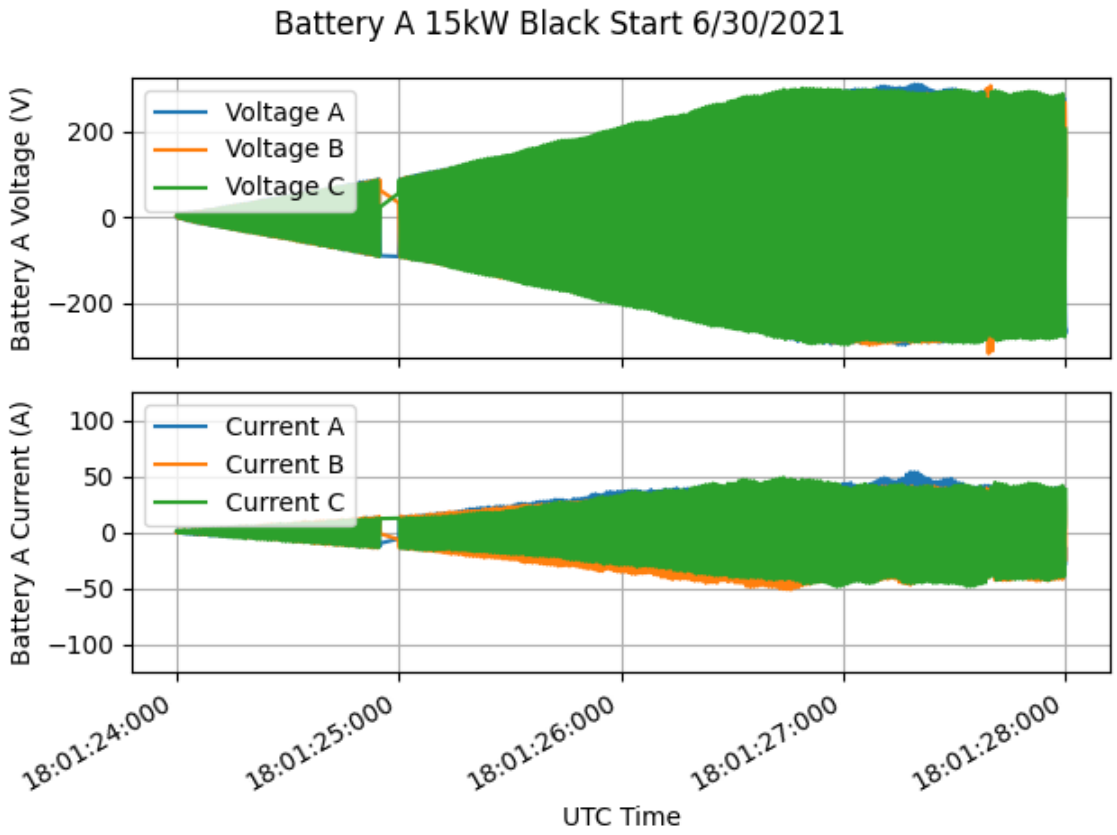
Black Start: Battery/Diesel Comparison

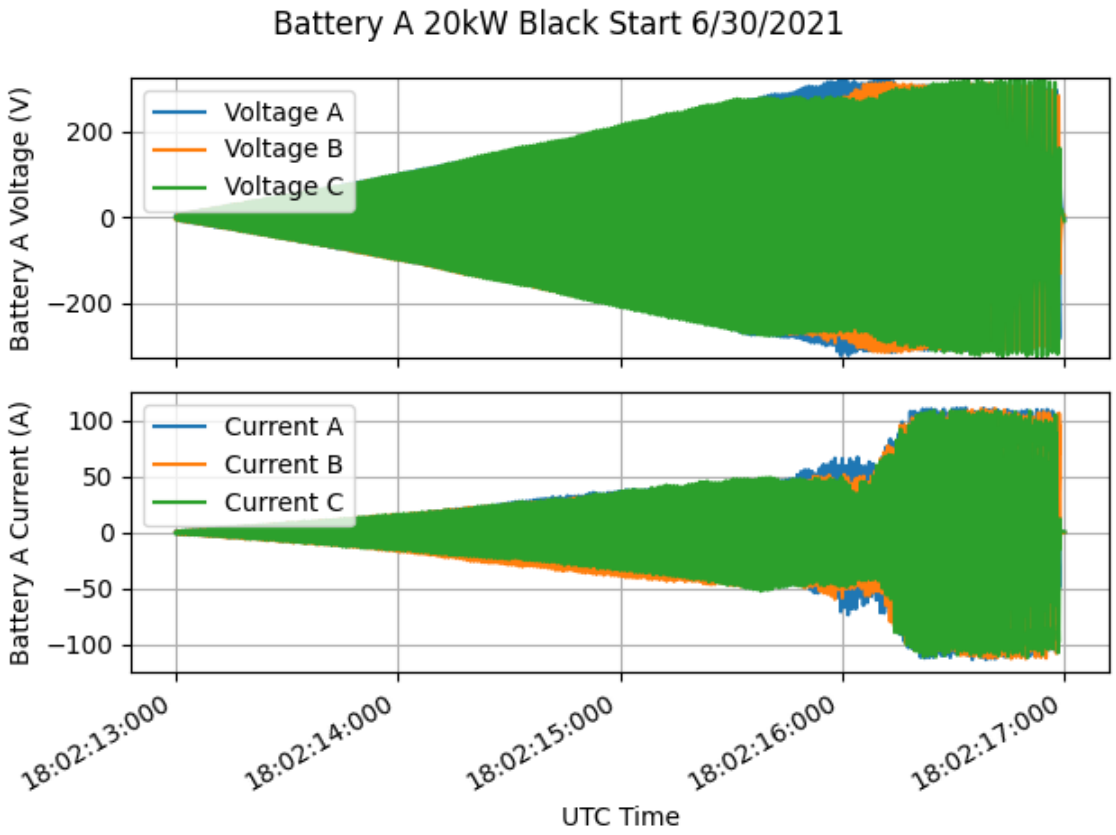




- Battery C Black Start Attempt 100kW (Hard Switch)
  - Failure (>200A Peak)
  - Successful with less load,
- Generator C Black Start Attempt 100kW
  - Success (>200A Peak)

Battery Black Start Capabilities – Success and Failure

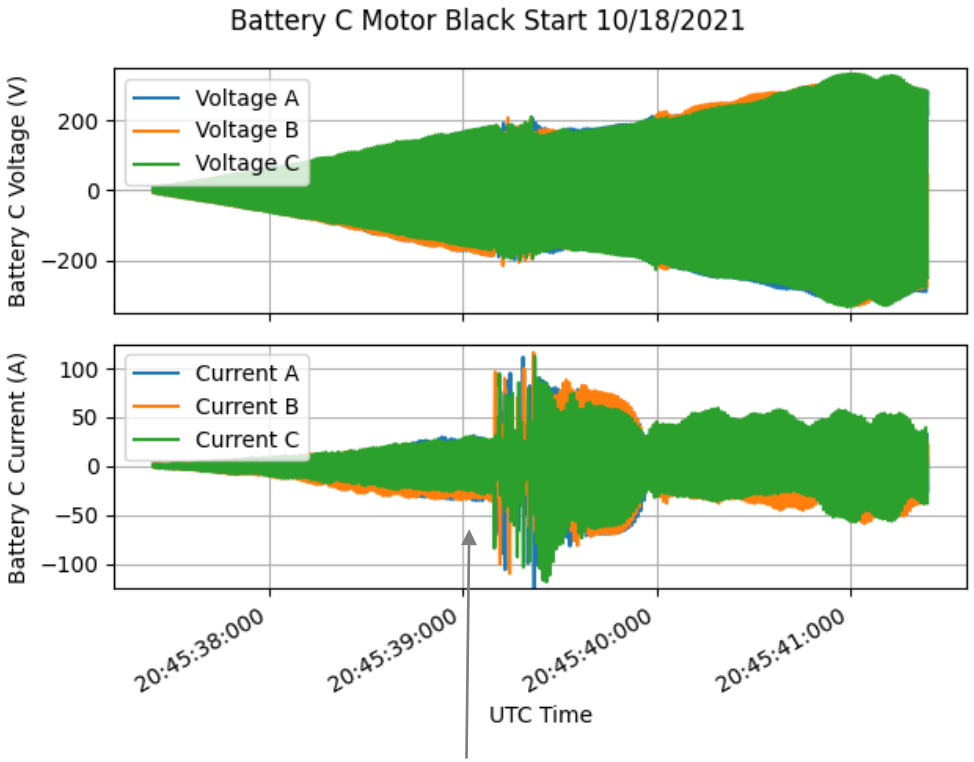




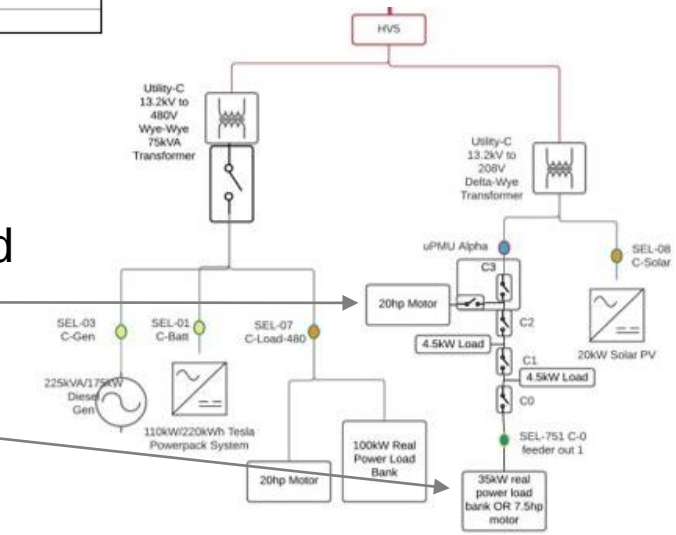
- Battery A successfully black starts 15kW of load
- Battery A attempts and fails to black start 20kW of load

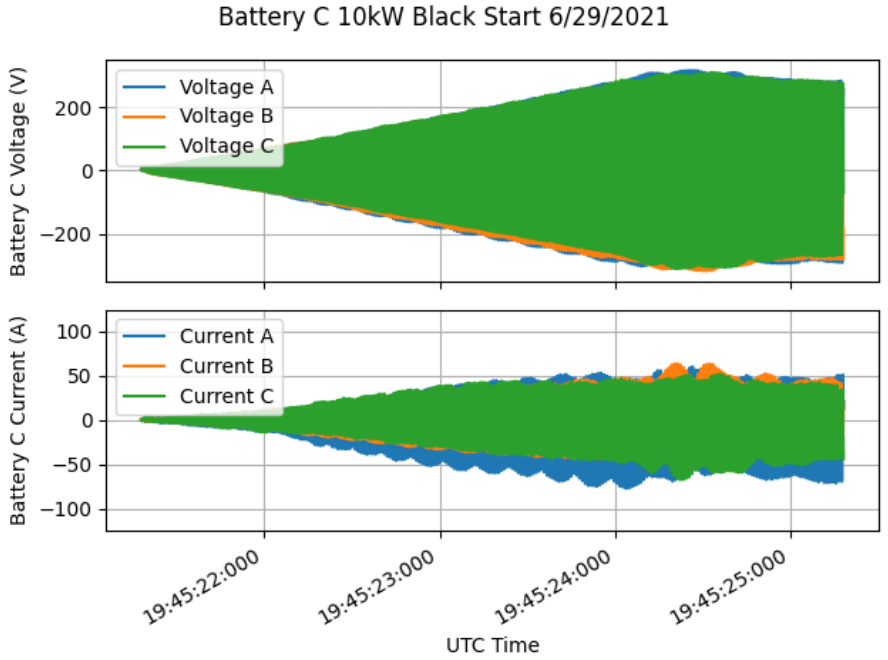
Battery 'soft-start' slow ramp of voltage to limit in-rush current.

Black Start: Load Type Comparison



- 20hp @ 480V joins when ~65% ramped
- 20hp @ 208V stays closed
- C-0 trips open



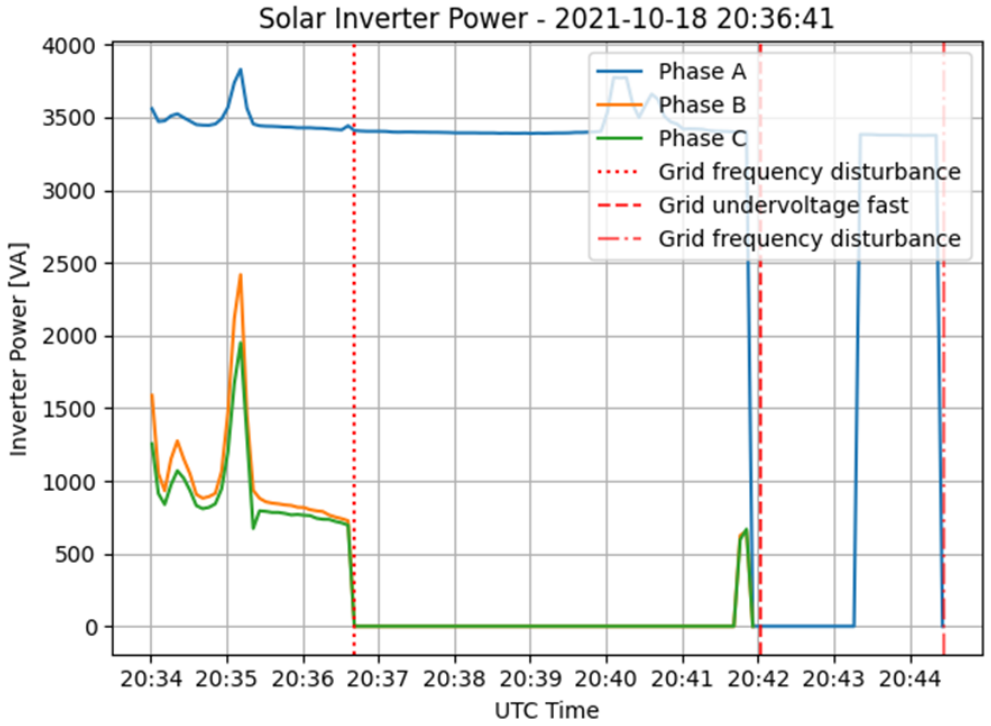


- Black starting into resistive load leads to **half** the peak current in **three-quarters** the time

Solar Inverter Performance

- Key Results
  - Solar PV inverters in grid-following could run in parallel with batteries in grid-forming stably
  - Solar PV inverter grid code configuration determined the severity of grid disturbance that they could continue operating through
    - Inverter A, with wider grid trip thresholds, rides through motor start transients while inverters B and C trip on grid frequency disturbance.
    - All three inverters trip on undervoltage

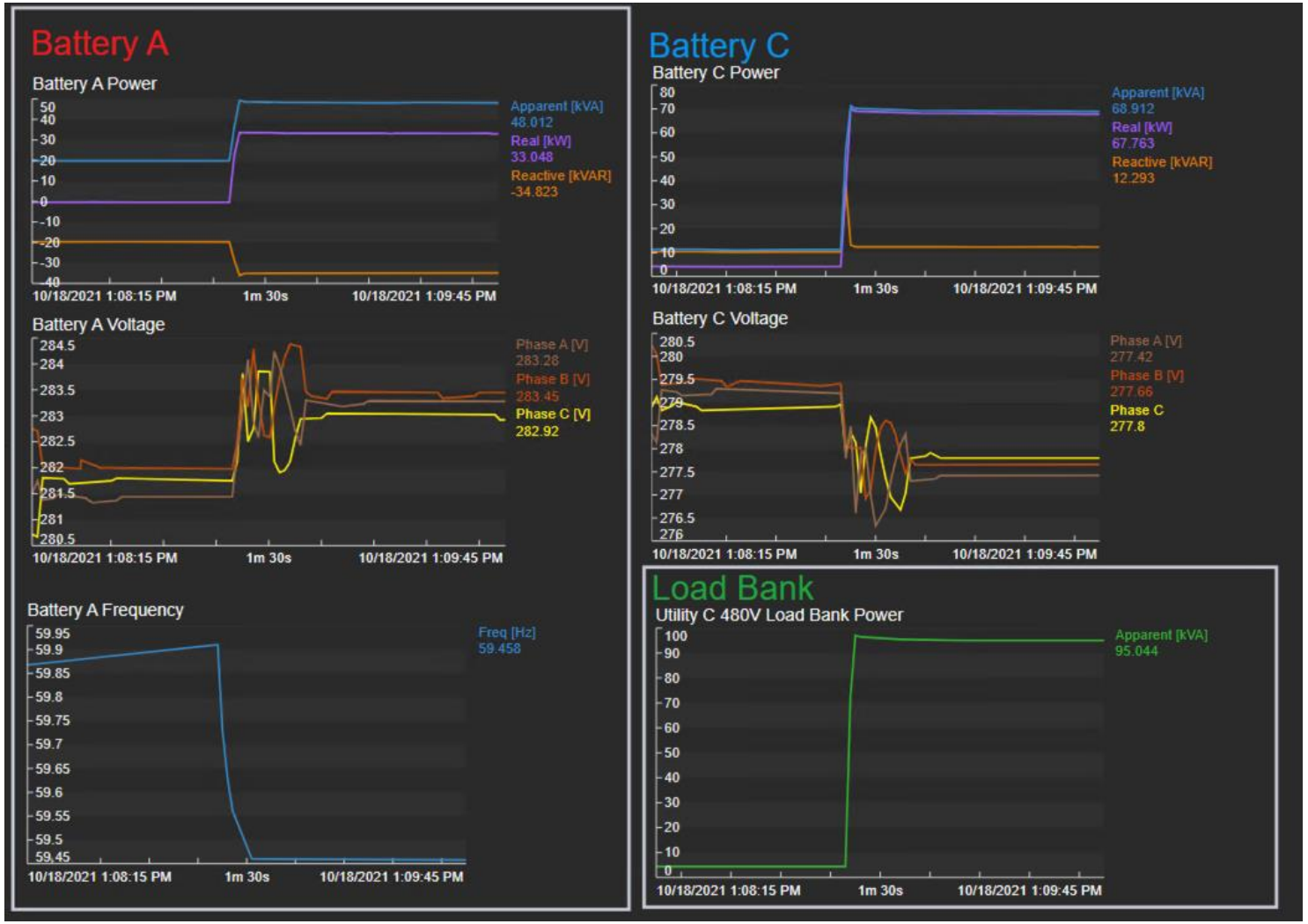
Solar Inverter Grid Code Settings Comparison



Inverter A, with wider grid trip thresholds, rides through motor start transients while inverters B and C trip on grid frequency disturbance (at 20:36:40).
All three inverters trip on undervoltage (when microgrid source is turned off) at 20:42.

Black Start: Load Steps

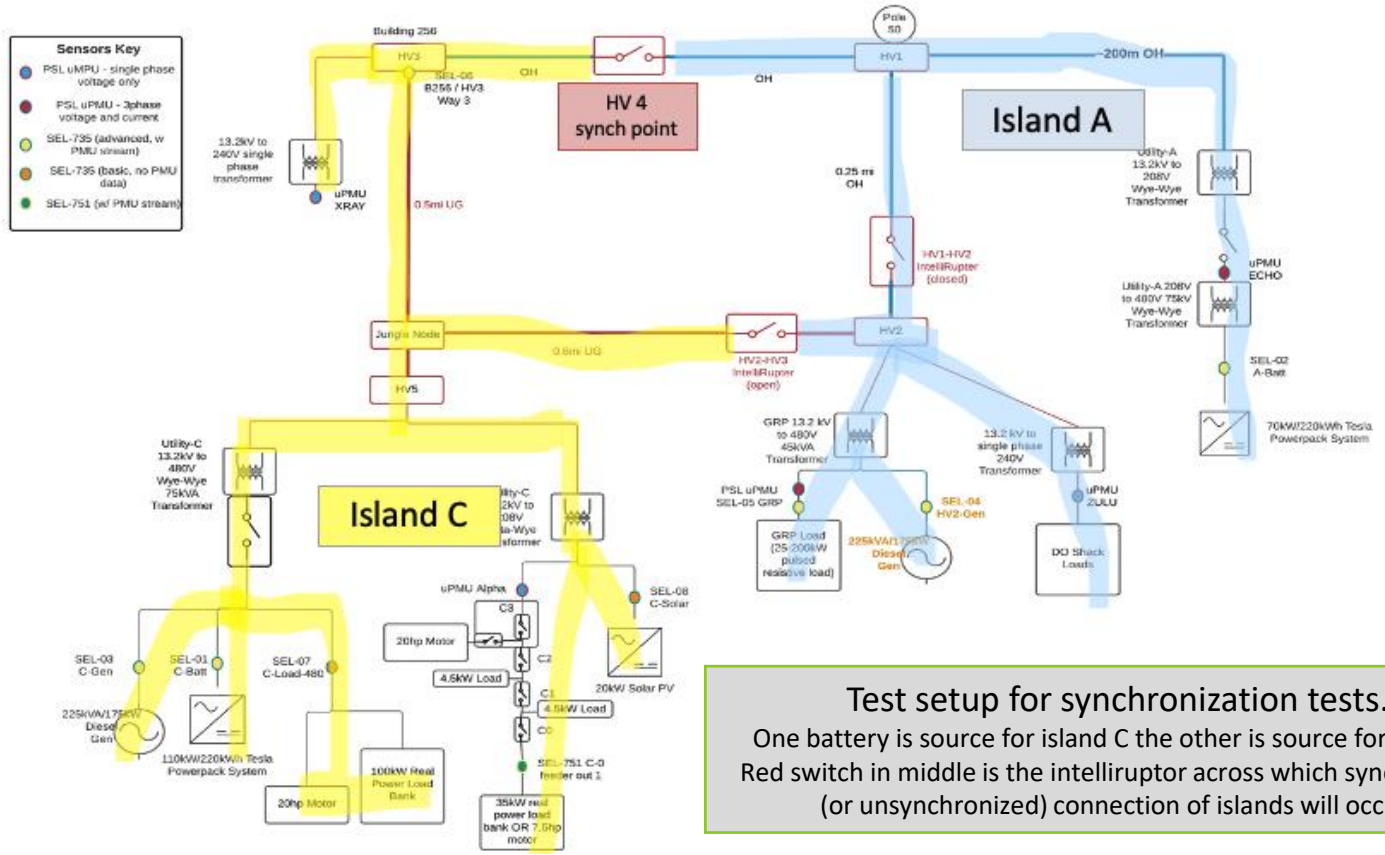
- Batteries able to support load steps after black start up to total load equal to rated power of battery
- Magnitude of ***load step*** that batteries can support in grid-forming is greater than magnitude of ***load*** that they can black start into
- Example on right shows 100kW load step with the two batteries in parallel (both in grid-forming), similar size load step can also be stably supported by a single battery.



Modbus data 1.5min zoom

Grid-Forming Battery Synchronization Across Intelliruptor

- Tested synchronization of isolated microgrids with inverter-based generators as sources across an intelliruptor
- Key Results:
  - Synchronization achievable with frequency modification method
  - Both batteries ride through the transient event of the intelliruptor closing (if synchronized) and share power evenly once connected
  - No loss of load during a forced (and unsynchronized) intelliruptor close event (one battery rides through, the other battery self-protects and trips)



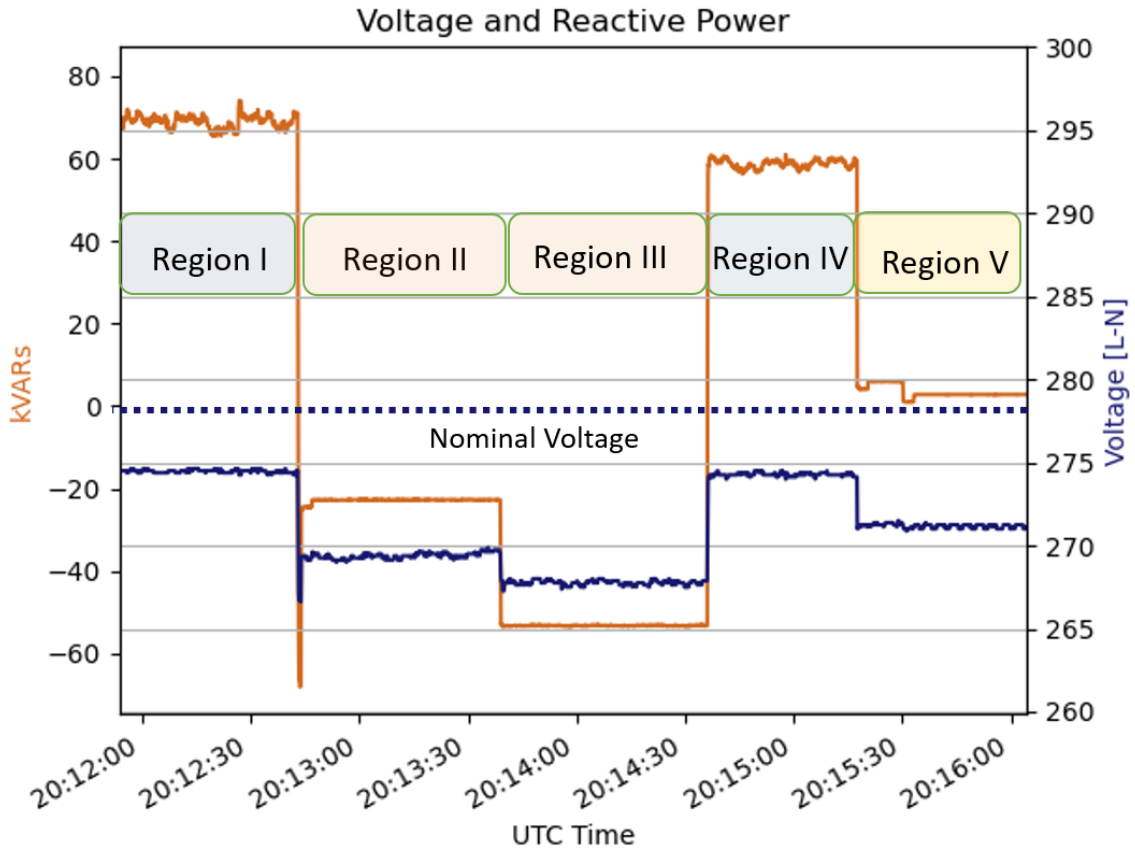
Test setup for synchronization tests.
One battery is source for island C the other is source for island A. Red switch in middle is the intelliruptor across which synchronized (or unsynchronized) connection of islands will occur.

Inverter-based islands can be smoothly combined together or re-integrated with the bulk system without device tripping or loss of load.

Cyber – API Manipulation

- API Manipulation assumes adversary has full network access and credentials, and operates BESS with malicious intent

Command	Outcome
Volt-Var setpoint manipulation	Inverted Volt-Var curves were allowed, and could be used to have adverse effects on local voltage
Manipulation of direct power setpoints	Direct power setpoints (and similar settings) could be modified to change the battery output adversarially.
Manipulation of power modes (including off)	Changing the battery mode could have adverse impacts, particularly by changing islanding modes or engaging total shutdown.
Simultaneous commands	Code was written to execute commands simultaneously on both batteries, doubling the impact of any adversarial commands.



Malicious Volt-VAR setpoints cause the voltage to dip even lower when the baseline is already below nominal voltage

Cyber – Manual Fuzzing

Action	Successful execution?
Mixed protocols	Yes
No token	Partial
Incorrect token	No
No certificate	Partial
Incorrect certificate	Partial
Invalid parameter names	No
Invalid parameter values	No
Control parameters outside documented limits	Partial

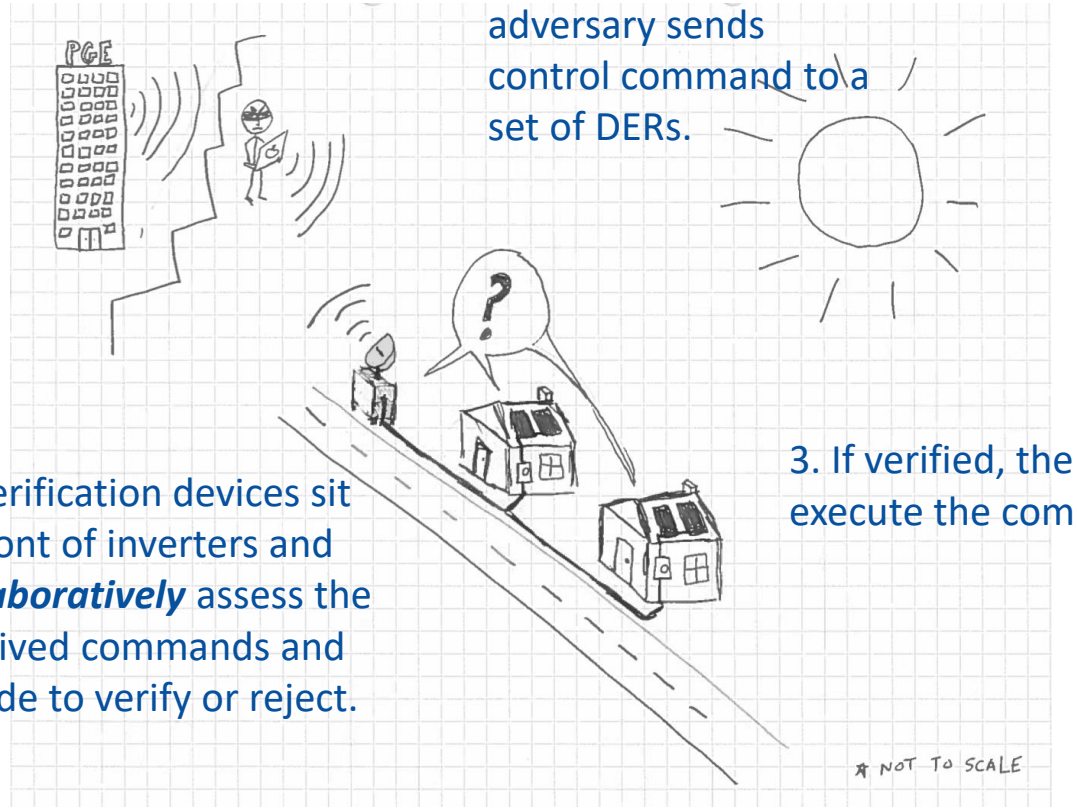
- Modus is always enabled, so protections can always be circumvented
- Authentication still allows some unexpected behaviors that could lead to broken confidentiality
- API parameters must be matched
- Most documented limits were enforced, some were not, which could potentially cause unexpected behaviors

Cyber – Network and Interface Monitoring

Scanned network interface to search for other potential interfaces

- Scanned 65535 ports
- 7 ports were open
  - HTTP and HTTPS
  - SSH
  - Modbus
  - Vendor-provided interface
  - Alternate web interface
  - Unknown service
- SSH was open, but required a key, not just a password
- Discovered additional UIs beyond those we were aware of
- Unknown service – no information available about this open port
  - Certificates were not valid

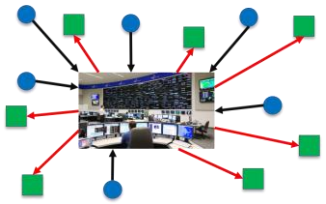
Collaborative Autonomy: Robust DERMS Control Verification



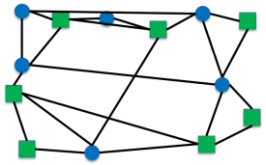
1. An operator or adversary sends control command to a set of DERs.

2. Verification devices sit in front of inverters and ***collaboratively*** assess the received commands and decide to verify or reject.

3. If verified, the DERs execute the command.

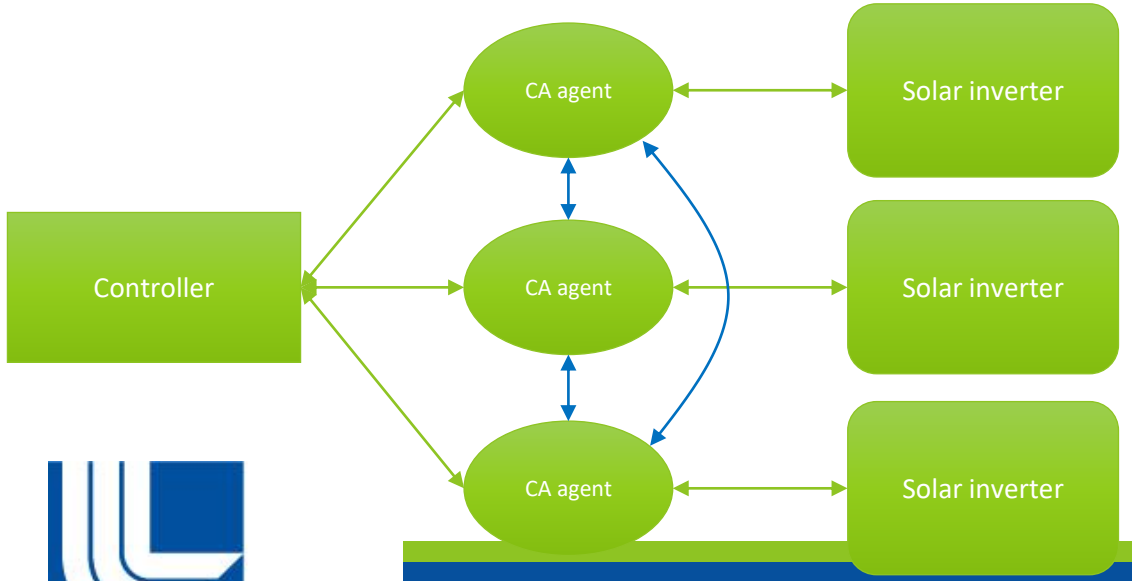


Traditional central approach



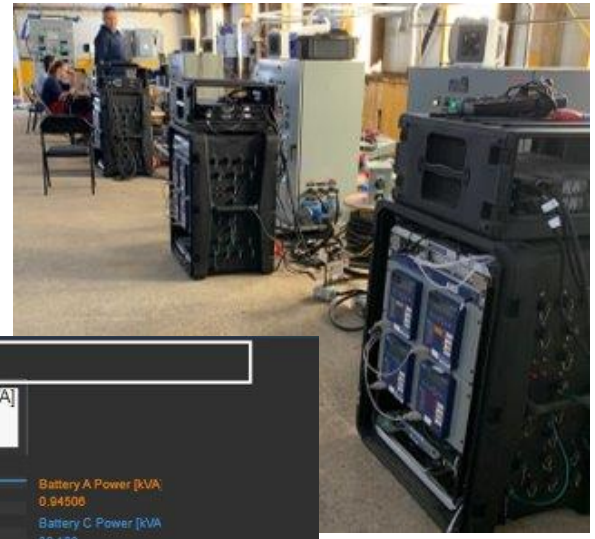
Novel collaborative approach

- With deep solar penetration, spurious commands can cause system instability.
- Collaborative autonomy can detect improper commands, protecting system efficiency and stability.



Novel Decentralized Black Start Control Demonstration

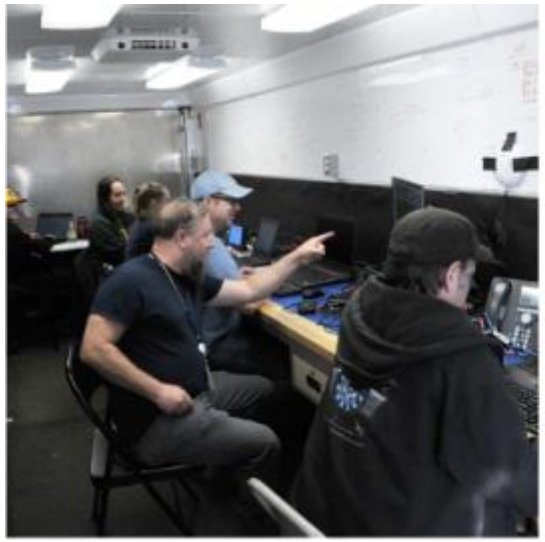
- Six distributed agents successfully worked together to black start the system:
  - Agent logic running on 6 separate Raspberry Pis
  - Hardware setup included 2 sources (grid-forming batteries) and 4 controllable switches (SEL 751 relays) each with load behind them

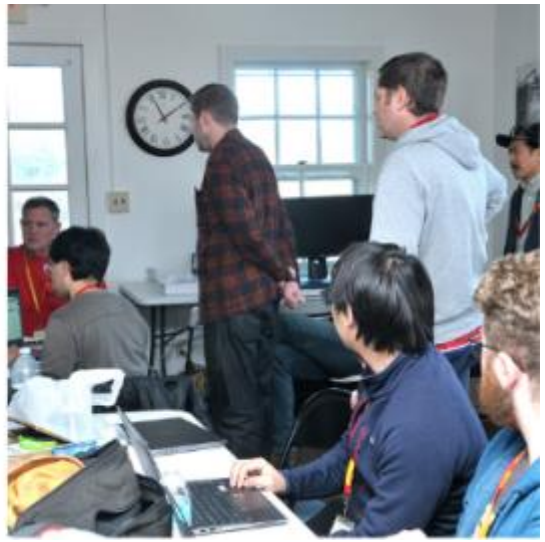


- Black start from C (Priority 1)
  - Switch in load in according to priority
- System showed resilience to two interferences:
  - Manually opening a switch, algorithm identified incorrect switch position and re-closed it
  - Oversized load, initial black start attempt failed but algorithm retried and succeeded on second attempt

Putting Research into Practice: Liberty Eclipse

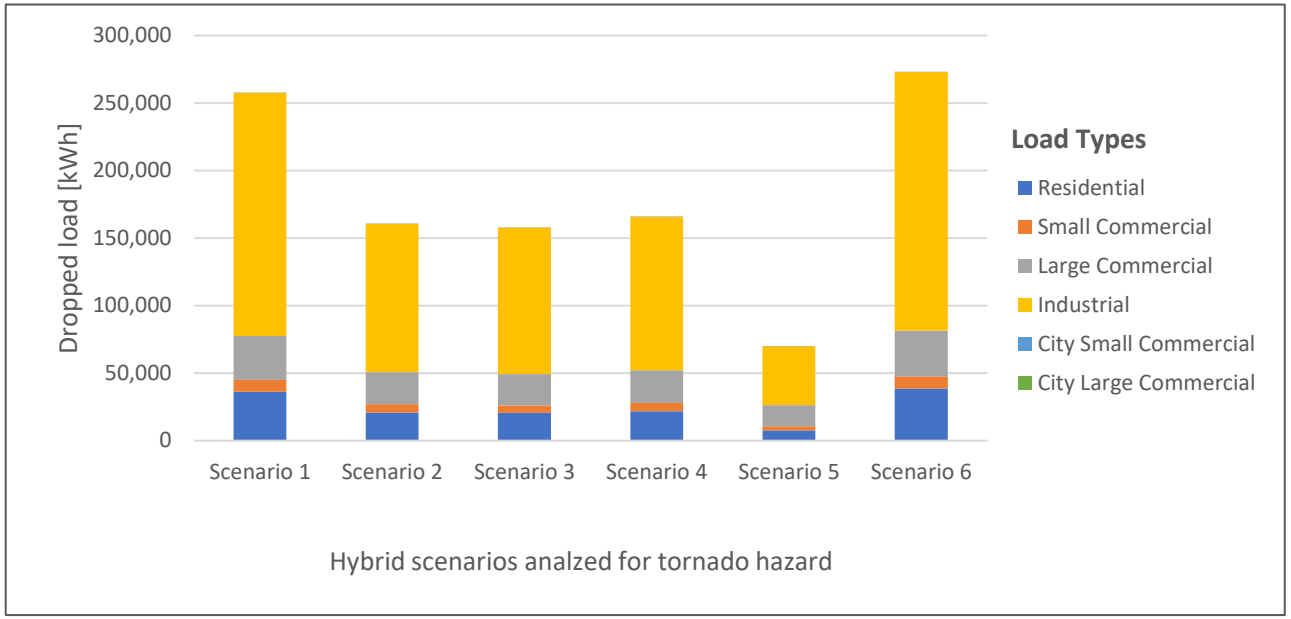
- Full-scale exercise in cybersecurity preparedness
- Allows utilities to practice incident response
- Collaboration between security operations center (SOC) and Operations teams





Putting Research into Practice: Technical Assistance for Communities

- Distributed wind integration projects (MIRACL and On Site Wind for Rural Load Centers) that analyze resilience benefits of distributed generation
- Quantifiable resilience metrics
- Technical Assistance provided to address coop needs and support funding applications



Total load loss in for various hybrid power plant scenarios for the resilience analysis of the tornado scenario hazard.
Scenario 1: Base Case, 1.8 MW wind.
Scenario 2: 5 MW wind, 5 MW solar, 5 MWh battery, resilient dispatch.
Scenario 3: 5 MW wind, 5 MW solar, 10 MWh battery, resilient dispatch.
Scenario 4: 5 MW wind, 5 MW solar, 5 MWh battery, max dispatch.
Scenario 5: 25 MW wind, 25 MW solar 25 MWh battery, max dispatch.
Scenario 6: No renewables.

Working with labs

- FOA – Funding Opportunity Announcements
  - Industry or academia can lead (labs can sometimes lead)
- Lab Calls
  - Labs lead, industry and academic partners
- SPP – Strategic Partnership Projects
  - Leverage lab personnel and facilities (non-govt. funding)
- Internships - https://inl.gov/internships/
- Graduate Fellowships - https://inl.gov/inl-initiatives/education/graduate-fellowship-program/
- DOE Programs - https://inl.gov/content/uploads/2023/02/NUP-DOEInternship.pdf
  - Science Undergraduate Laboratory Internships (SULI) - https://science.osti.gov/wdts/suli
  - NNSA Minority Serving Institution Partnership Program (MSIPP) https://www.energy.gov/nnsa/nnsa-minority-serving-institution-partnership-program-msipp
  - EERE Postdoctoral Research Program
  - Omni Technology Alliance Internship Program (cybersecurity and IT)

More on INL's Research

- GMLC Blackstart Project: https://www.powermag.com/how-the-doe-plans-to-modernize-the-grid-in-the-near-term/
  - https://ieeexplore.ieee.org/document/10252637/
- Liberty Eclipse: https://www.energy.gov/ceser/liberty-eclipse
- On Site Wind & MIRACL: https://resilience.inl.gov/miracl/
  - Resilience Framework: https://resilience.inl.gov/wp-content/uploads/2021/07/21-50152_RF_EEDS_R4.pdf
- Cyber-Informed Engineering: https://inl.gov/cie/
  - National Cyber-Informed Engineering Strategy: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf
  - CIE Implementation Guide: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

News Articles

- https://www.klfy.com/local/st-martin-parish/lafayette-man-charged-with-shooting-transformer-at-st-martinville-substation/
- https://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears
- https://www.nytimes.com/2023/10/17/climate/electric-grids-climate-iea.html
- https://apnews.com/article/renewable-energy-climate-change-electrical-grids-82d1fedd21e58d36e27c6c2396498c0c
- https://apnews.com/article/texas-power-grid-heat-emergency-alert-de76bc9fe6fd16e97ab6fc8d0c165065
- https://www.reuters.com/business/energy/us-energy-regulator-recommends-revising-reliability-standards-extreme-weather-2023-09-21/
- https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/
- https://therecord.media/cosmicenergy-malware-russia-critical-infrastructure-power-grid

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.