Setting the Stage:

U.S. Bulk Grid & Assets Vulnerable to Physical and Cyber Threats

Sarah H. Davis, P.E.
Transmission Manager

IEEE Tech Talk – Protecting the National Grid

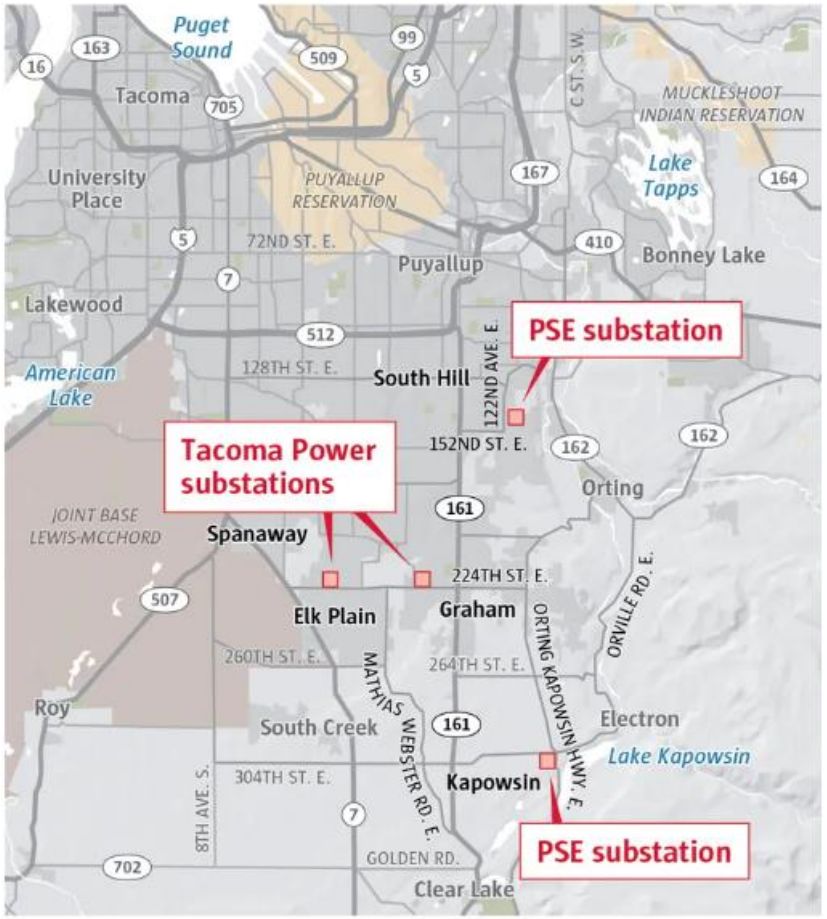
APEX CLEAN ENERGY

March 1st, 2023

Human-related grid disturbances on the rise…

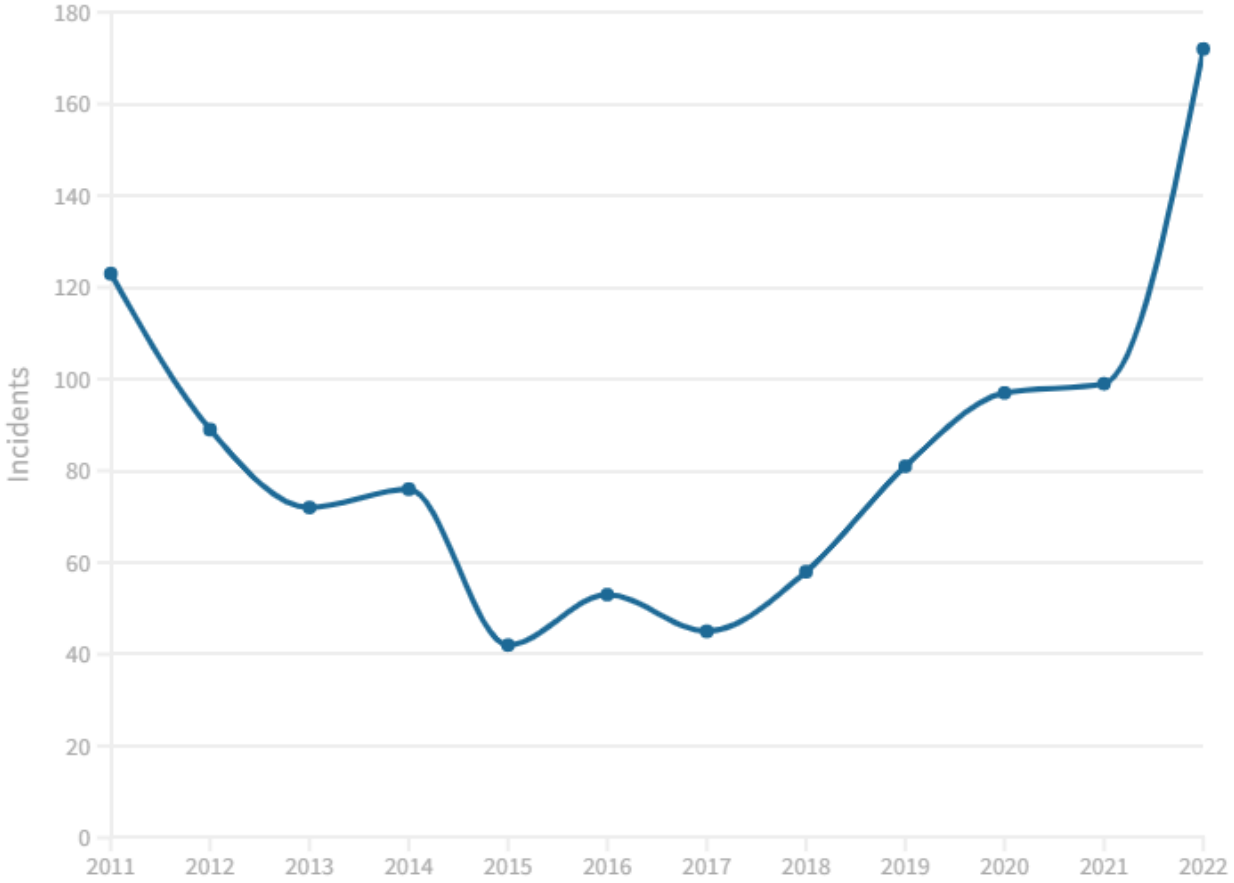
Pierce County Christmas Day substation attacks

The first of four attacks was estimated to have happened in the early morning and the last in the evening on Christmas Day.



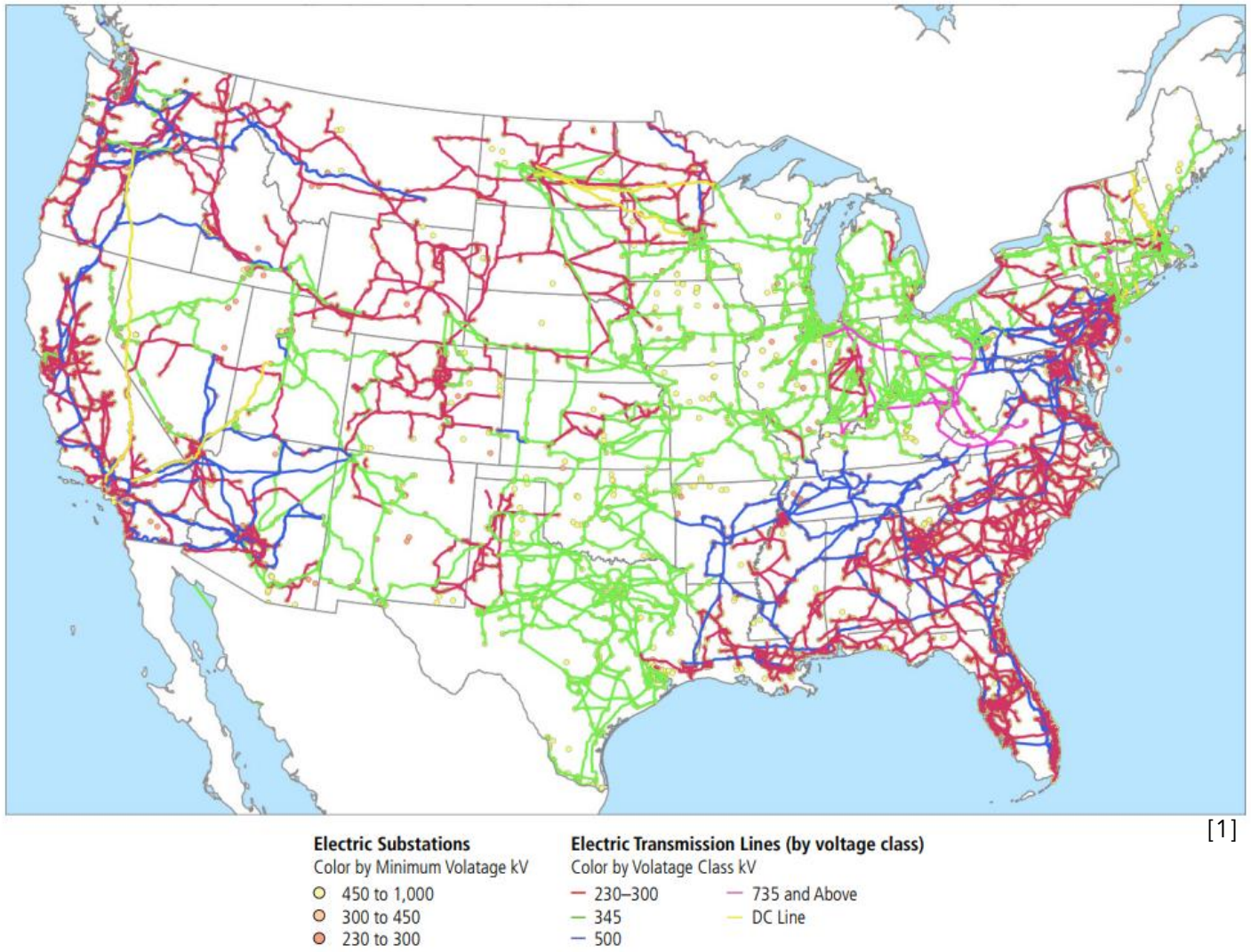
Source: Pierce County Sheriff's Department FIONA MARTIN / THE SEATTLE TIMES

Human-related disturbances and unusual incidents at U.S. electrical facilities



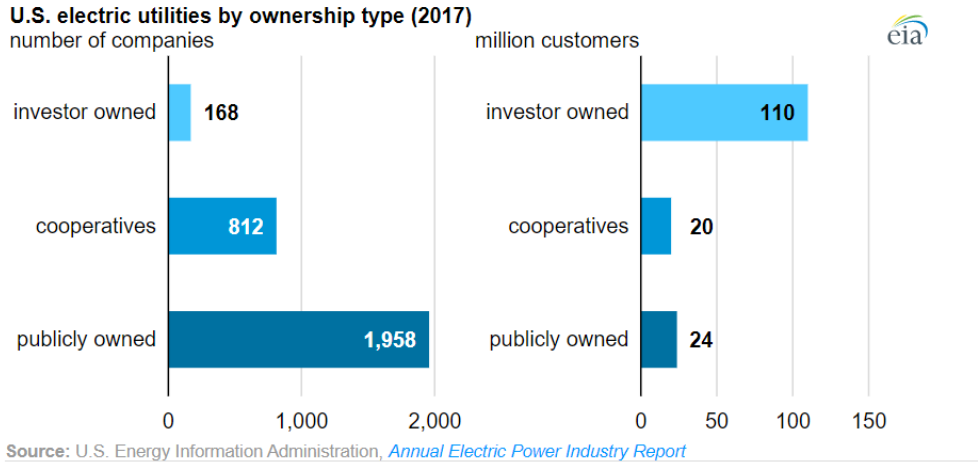
Source: Department of Energy • USA TODAY analysis of reports utilities submit to the Department of Energy

The World's Largest Machine: US Power Grid



[1]

Investor-owned utilities served 72% of U.S. electricity customers in 2017



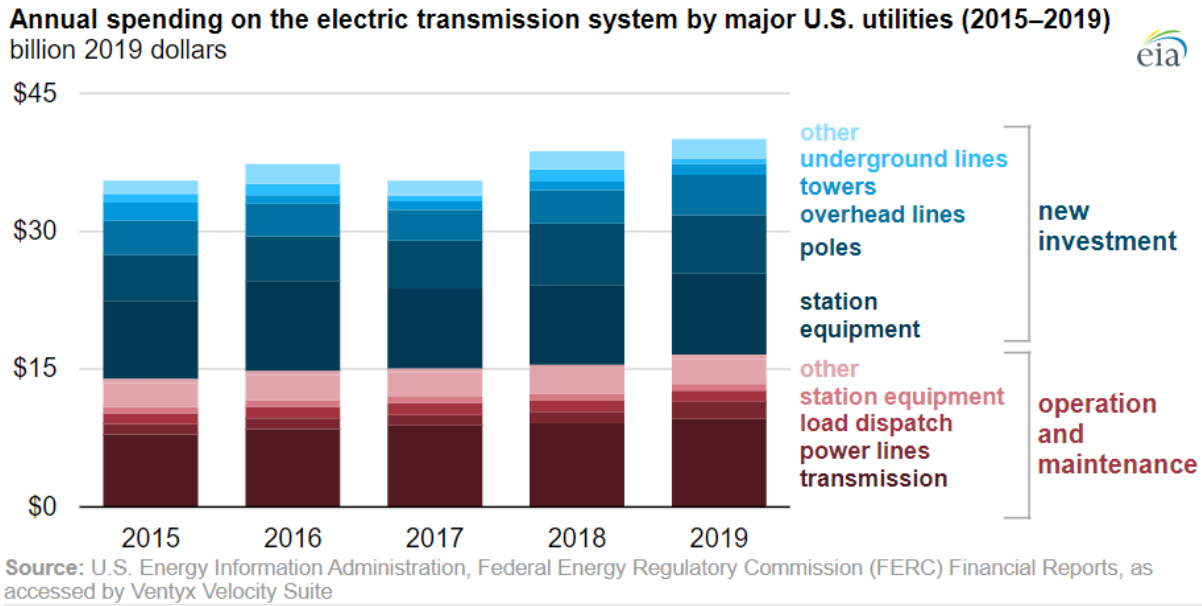
[2]

- **700,000 circuit miles of power lines**
  - 240,000 operating >= 230kV
- **55,000 substations**
  - 21,500 operating >= 100kV
- **12,000 utility-scale power plants**
- **3,000 utilities**

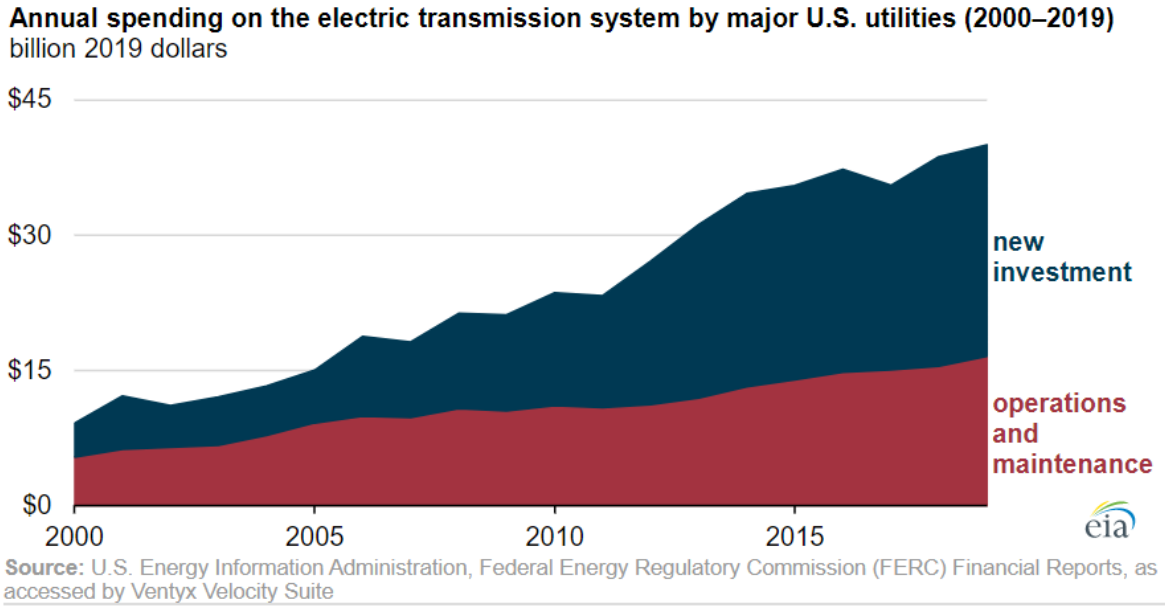
[1][2]

[1] https://www.energy.gov/sites/prod/files/2017/02/f34/Appendix--Electricity%20System%20Overview.pdf
[2] https://www.eia.gov/

Aging Infrastructure



[3]



[3]

- 70% of power transformers are 25+ years old
- 60% of circuit breakers are 30+ years old
- 70% of transmission lines are 25+ years old

[4]

[3] https://www.eia.gov/
[4] https://www.energy.gov/sites/prod/files/2015/09/f26/QTR2015-3F-Transmission-and-Distribution_1.pdf

Critical Nature of Substations

[5]

- Critical to reliably and safely deliver energy
- Expensive power electronics
- Protective devices (breakers, relays, etc.)
- Communications equipment
- Backup battery power
- Higher voltage → more critical
- Requires physical & cyber security

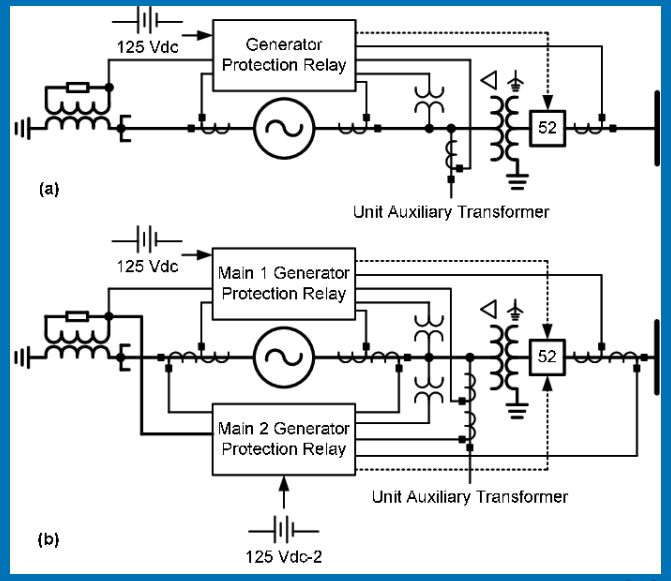
Note: Many substations are OLD. Significant amounts of electromechanical devices still on grid. Gradually replaced by smarter devices that are more vulnerable to threats.

[5] David Neale [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons

Designing the Bulk Grid with Redundancy, Reliability, Resiliency

Redundancy

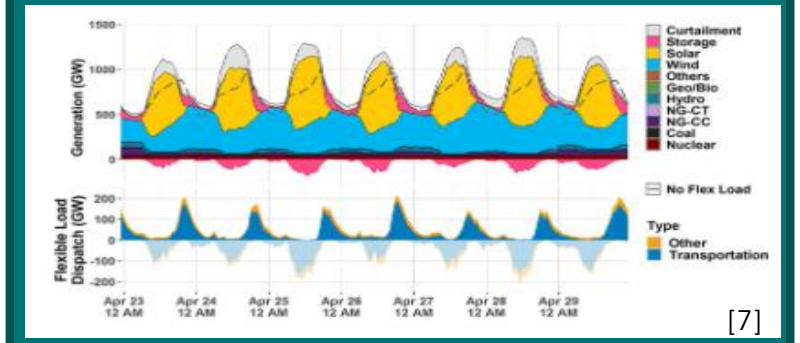
- Duplication of system components



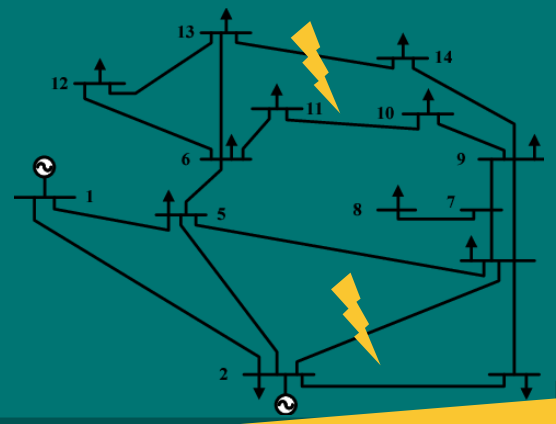
[6]

Reliability

- Designing to ensure energy delivery under worst case planned-for conditions



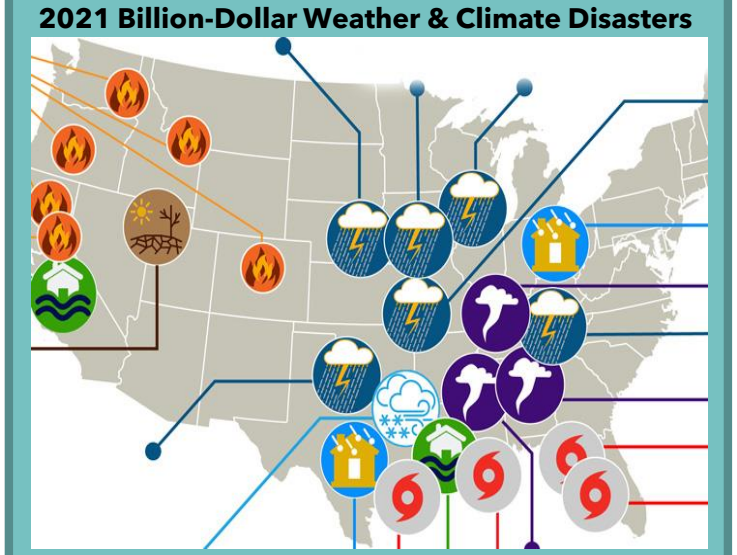
[7]



[8]

Resiliency

- Ability to bounce back quickly after an extreme event



[9]

Design aspects of Redundancy, Reliability, and Resiliency are all lines of defense against physical & cyber attacks. **But they can also be targeted.**

[6] Sandoval, Ramon et al. "Using Fault Tree Analysis to Evaluate Protection Scheme Redundancy." (2015).
[7] https://www.nrel.gov/analysis/electrification-futures.html
[8] IEEE 14 bus system
[9] https://www.noaa.gov/, 2021 Billion-Dollar Weather and Climate Disasters

NERC* Standards: Cyber & Physical Security

Critical Infrastructure Protection (CIP)

Family	Standard Version	Title	Effective Date of Standard
CIP	CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	12/27/2016
CIP	CIP-003-8	Cyber Security — Security Management Controls	4/1/2020
CIP	CIP-004-6	Cyber Security — Personnel & Training	7/1/2016
CIP	CIP-005-7	Cyber Security — Electronic Security Perimeter(s)	10/1/2022
CIP	CIP-006-6	Cyber Security — Physical Security of BES Cyber Systems	7/1/2016
CIP	CIP-007-6	Cyber Security — System Security Management	7/1/2016
CIP	CIP-008-6	Cyber Security — Incident Reporting and Response Planning	1/1/2021
CIP	CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	7/1/2016
CIP	CIP-010-4	Cyber Security — Configuration Change Management and Vulnerability Assessments	10/1/2022
CIP	CIP-011-2	Cyber Security — Information Protection	7/1/2016
CIP	CIP-012-1	Cyber Security – Communications between Control Centers	7/1/2022
CIP	CIP-013-2	Cyber Security – Supply Chain Risk Management	10/1/2022
CIP	CIP-014-3	Physical Security	6/16/2022

[10]

* North American Electric Reliability Corporation (NERC)

[10] https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

Critical Energy Infrastructure Information (CEII)

FERC's* Definition:

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:

1) Relates details about the production, generation, transmission, or distribution of energy
2) Could be useful to a person planning an attack on critical infrastructure
3) Is except from mandatory disclosure under the Freedom of Information Act
4) Gives strategic information beyond the location of the critical infrastructure

Critical Energy Electric Infrastructure (CEII) is a system or asset of the bulk-power system (physical or virtual), the incapacity or distribution of which would negatively affect:

- National Security
- Economic Security
- Public Health or Safety

[11]

Examples:

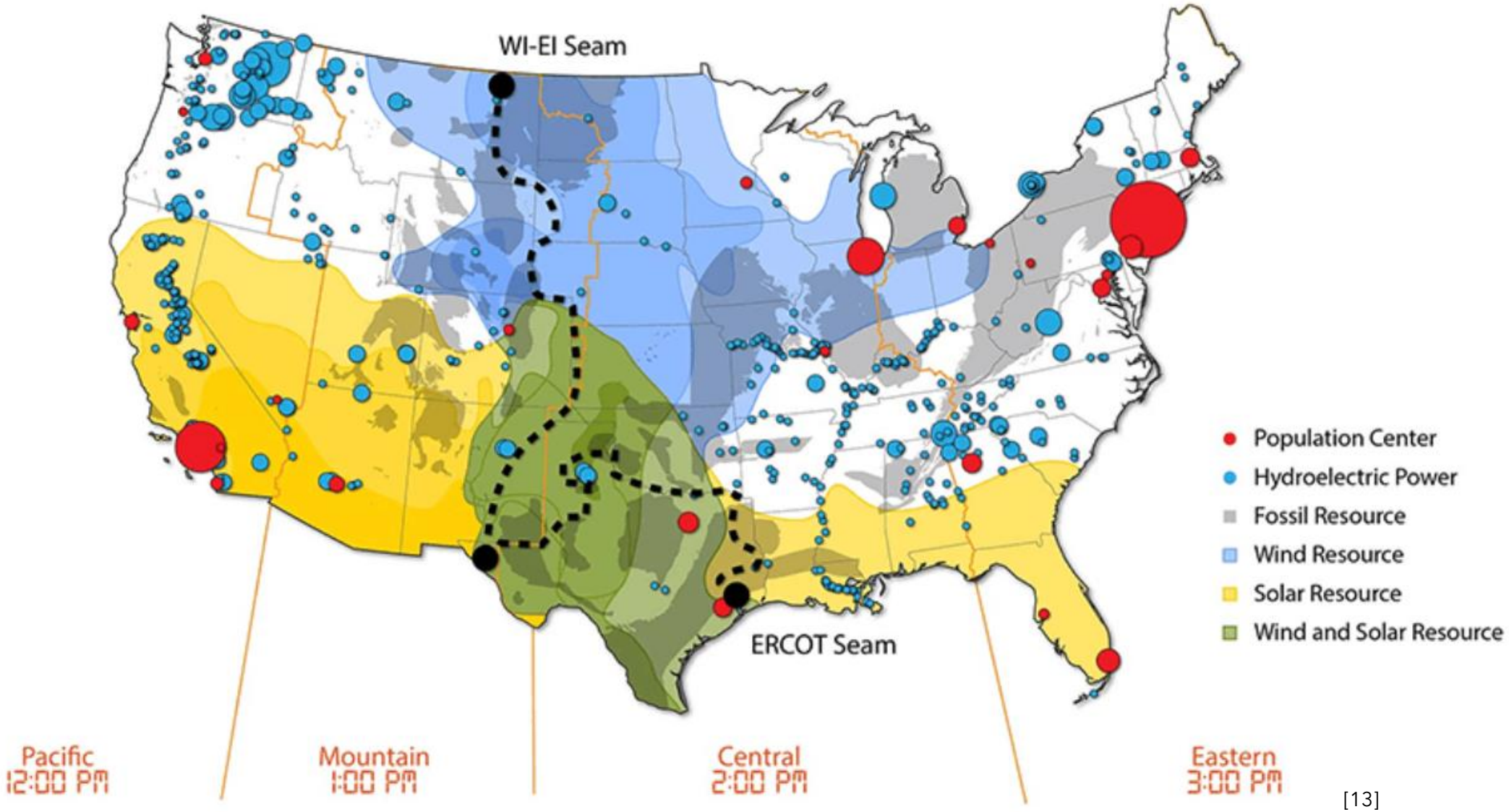
- Drawings and specifications
- Technical reports
- System Models
- Protection Scheme Definitions
- Emergency Action Plans
- Etc.

[12]

* Federal Energy Regulatory Commission (FERC)

[11] https://www.ferc.gov/ceii
[12] https://www.powerworld.com/products/simulator/overview

Resource Mix is Changing: Today vs. Future's Critical Assets



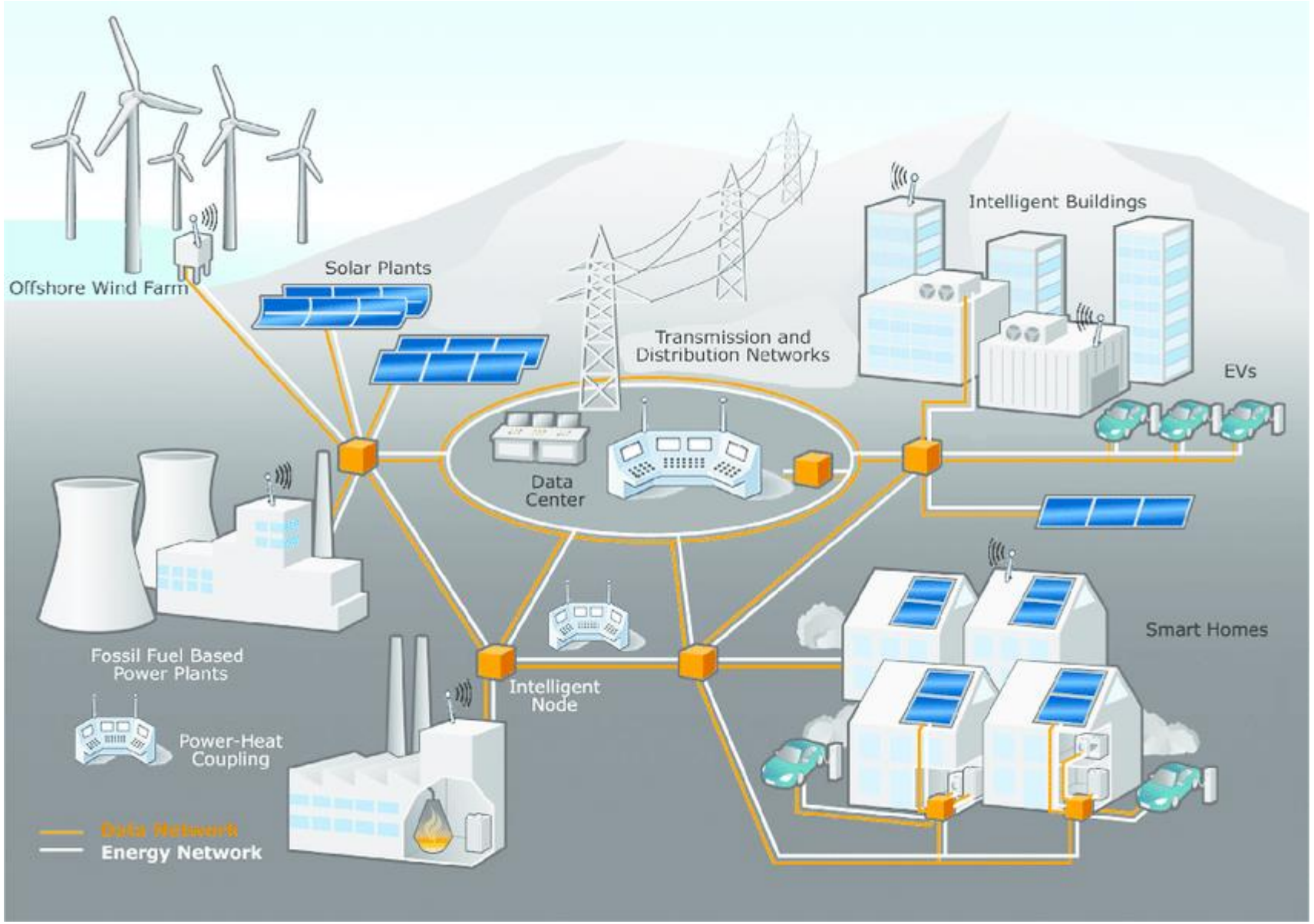
[13]

[13] https://www.nrel.gov/analysis/seams.html

Expanding Communication Networks

New Tech w/ Comm Dependency:

- Expanding markets
- Gen & Load Forecasting
- Large Energy Storage
- DER
- Demand response
- Distributed automation
- Microgrids
- Smart EV charging
- Virtual power plants/V2G
- Transactive Energy
- Etc.



[14]

[14] Kabalci, Yasin. (2016). A survey on smart metering and smart grid communication. Renewable and Sustainable Energy Reviews. 57. 302-318. 10.1016/j.rser.2015.12.114.

Conclusions

- The U.S. power grid is the worlds largest machine with a massive number of infrastructure spread throughout the country
- Owned and maintained by many different transmission and distribution providers
- Electricity infrastructure is aging and wasn't originally designed with cybersecurity in-mind
- Roll out and dependency of new technologies could put our grid at higher physical & cyber security risk

Thank you!

Contact info:

sarah.davis@apexcleanenergy.com

APEX CLEAN ENERGY