INL/CON-24-78128-Revision-0



# Cybersecurity Considerations for Emerging Energy Technologies

May 2024

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/CON-24-78128-Revision-0

# Cybersecurity Considerations for Emerging Energy Technologies

**Megan Jordan Culler**

**May 2024**

**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**

May 15, 2024

**Megan Culler**
Infrastructure Security

# Cybersecurity Considerations for Emerging Energy Technologies

## SEIA's Security and Reliability Forum

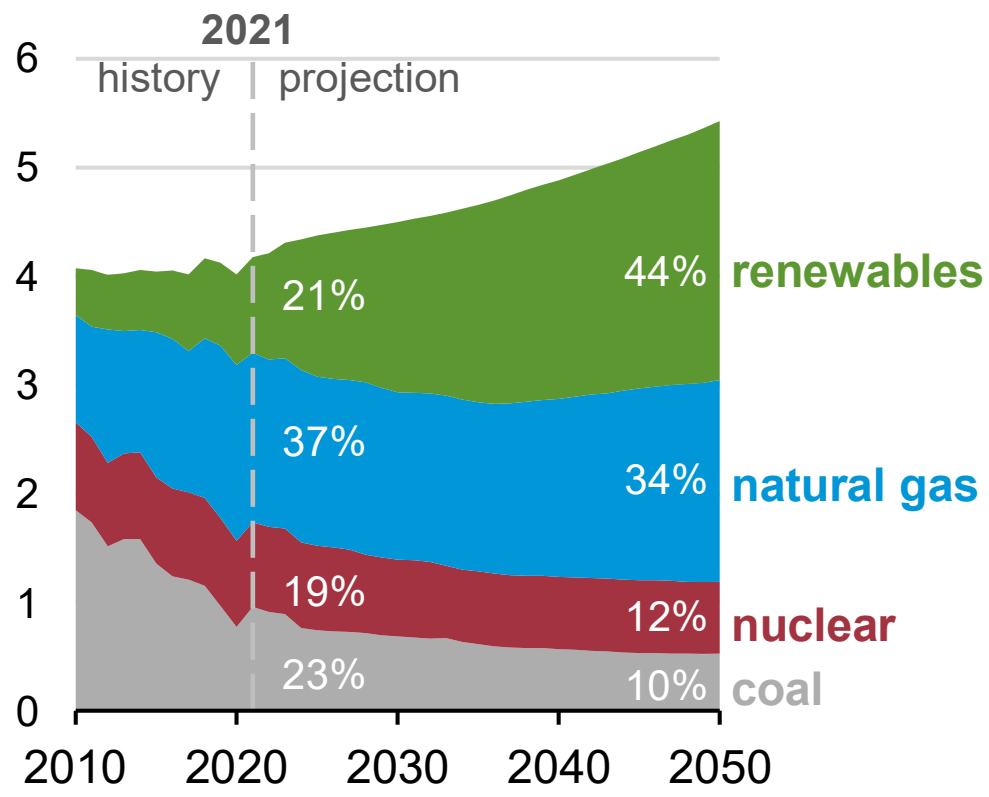
Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

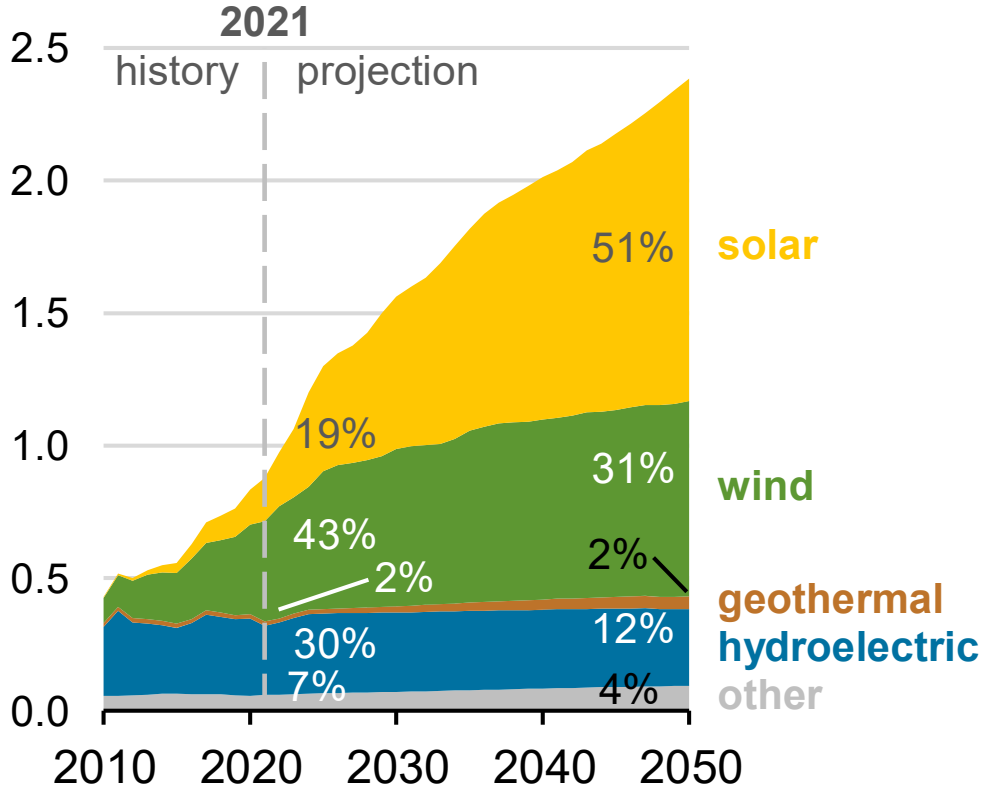
INL/CON-24-78128

# 2020 to 2050 Capacity and Energy Production in the U.S.

**U.S. electricity generation**
**AEO2022 Reference case**
trillion kilowatthours

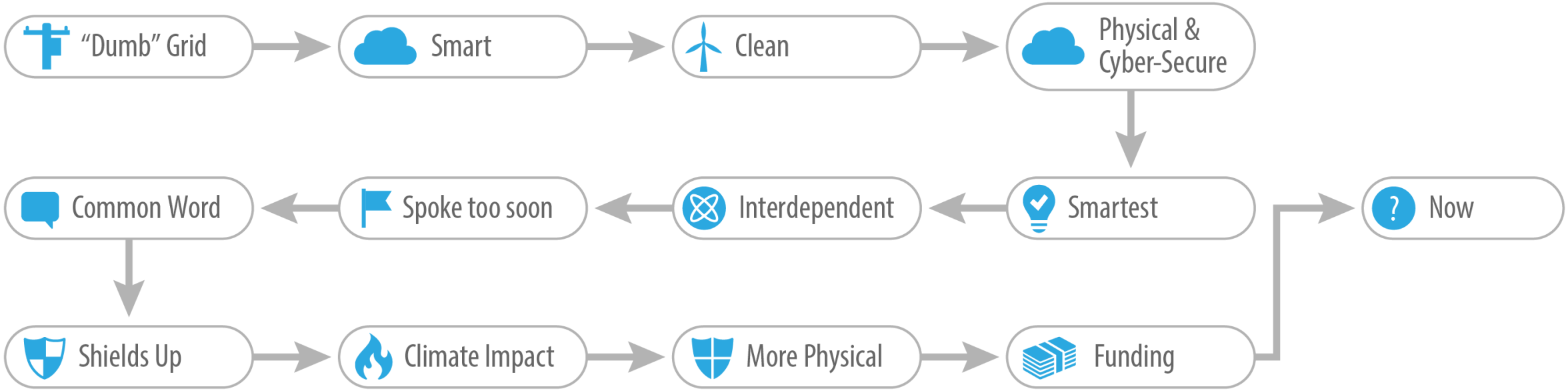



**U.S. renewable electricity generation**
**including end use**
trillion kilowatthours




https://www.eia.gov/todayinenergy/detail.php?id=51698

# Energy Delivery Digital Transformation:
*Where are we Going?*



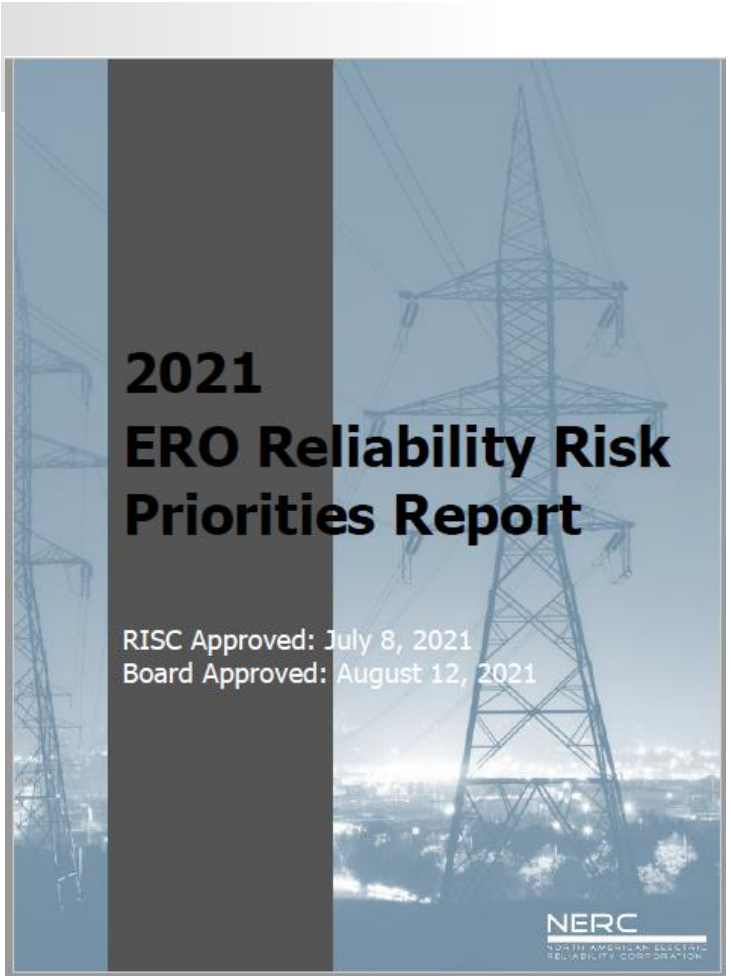
# Future of IBR

| Changes in IBR | | 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

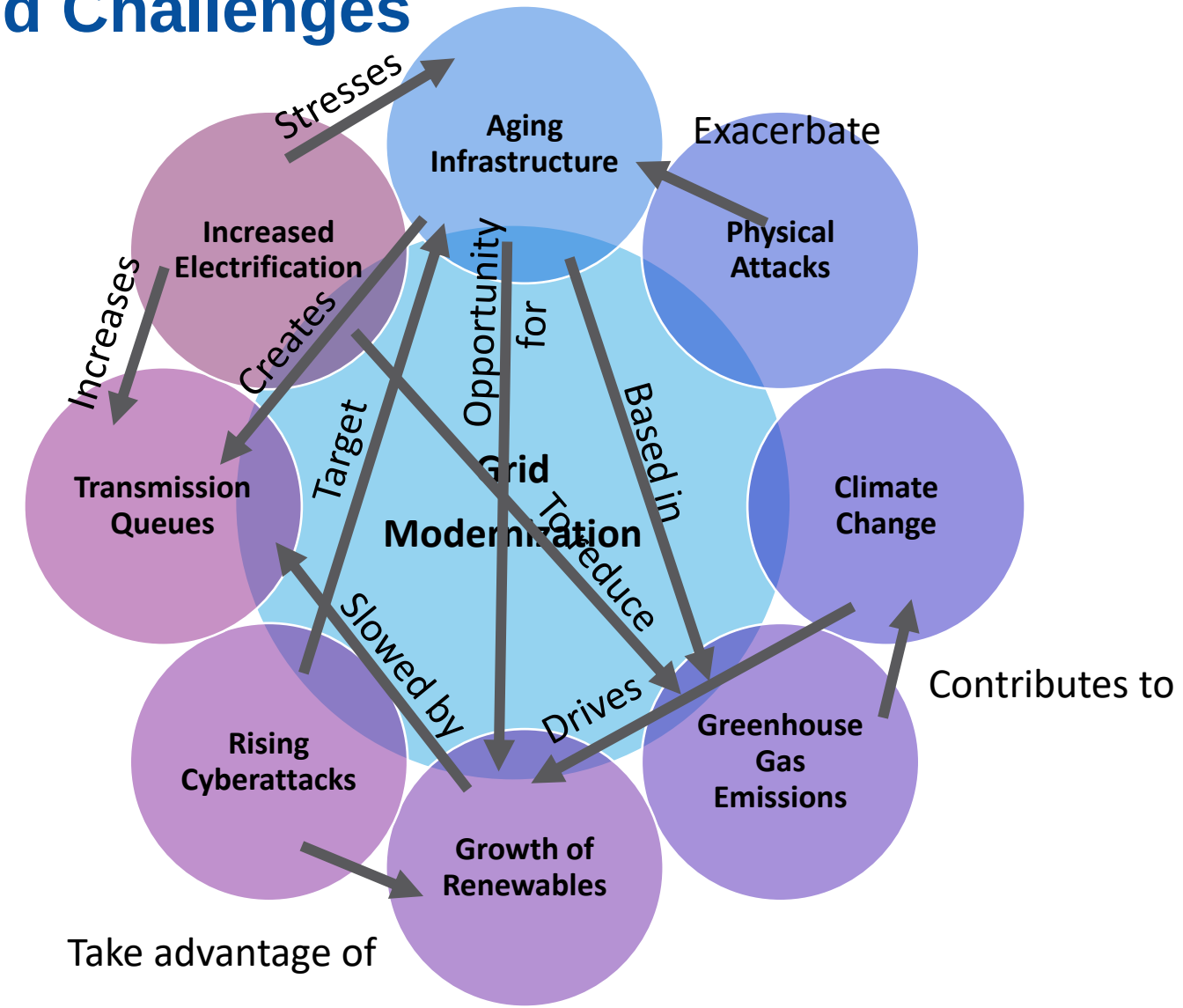
## Changing Resource Mix and Cybersecurity are the highest Ranked Risks

*NERC Reliability - Risk*

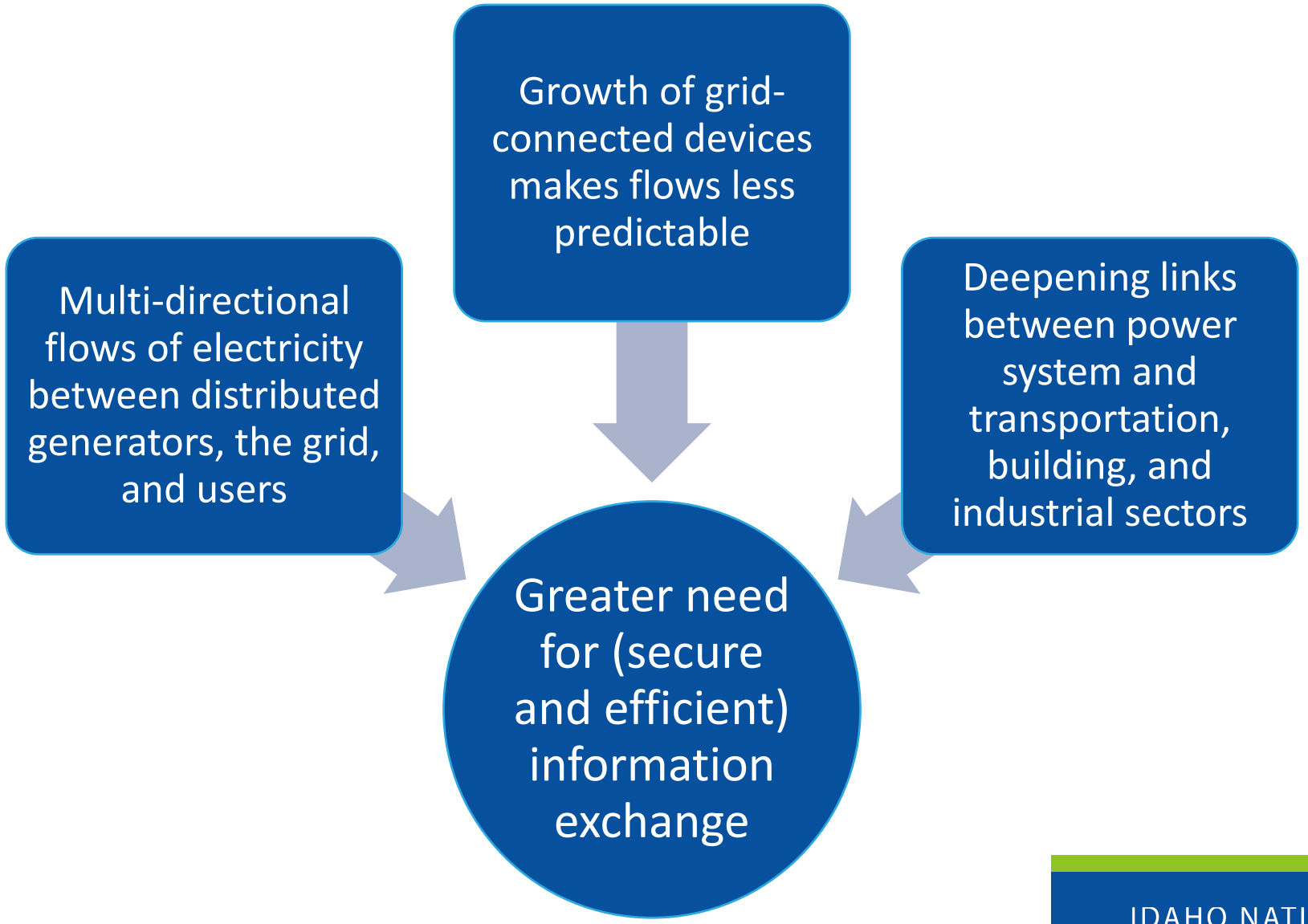




# Interconnected Challenges

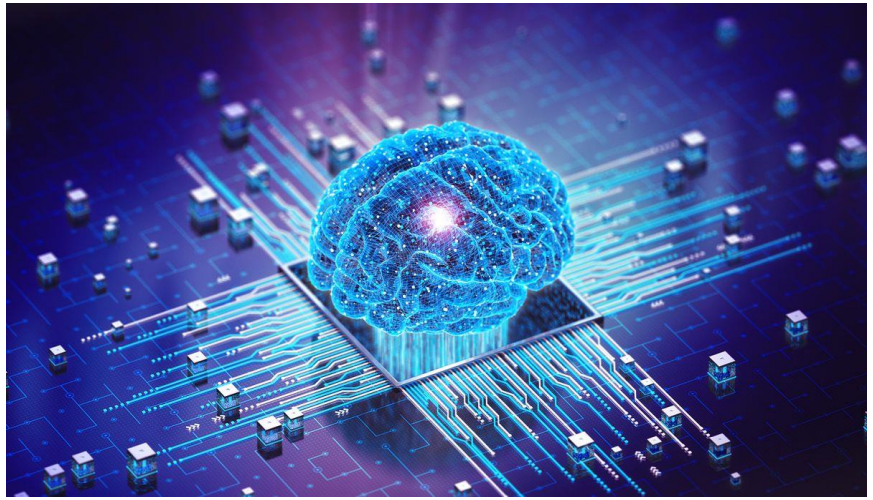


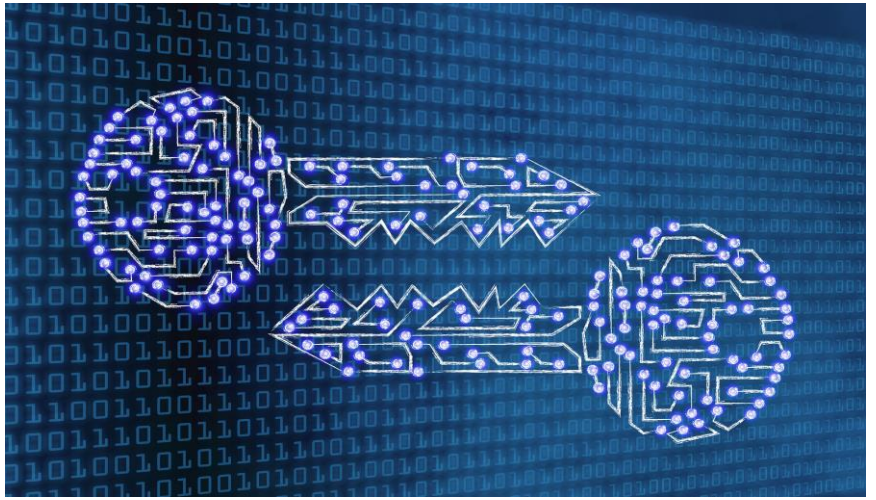
# Drivers of Technology Changes



# Emerging Technologies for the Energy Landscape

Artificial Intelligence





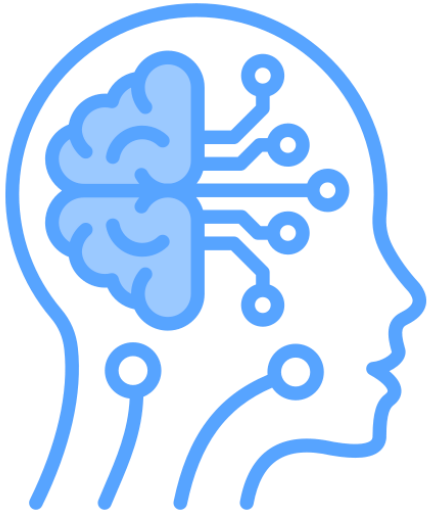
Post-Quantum Cryptography

Zero-Trust Architectures


Cloud Computing

# Artificial Intelligence

Artificial Intelligence



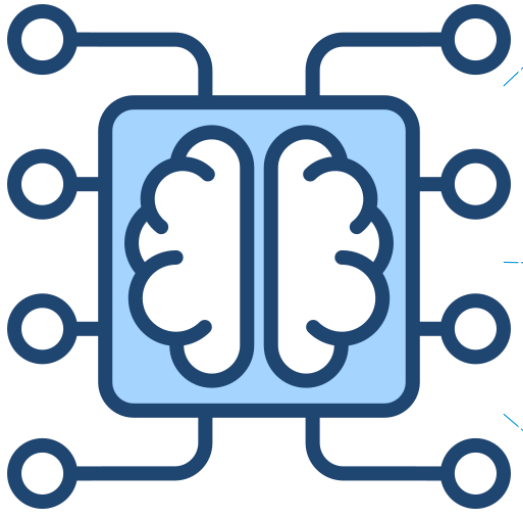
What is it

Applications

Cyber Considerations

# Artificial Intelligence

~~Artificial Intelligence~~
Machine Learning



**What is it**

- ML is a subset of AI
- ML extracts knowledge from data and learns autonomously
- AI mimics human decision making
- All rely on large datasets

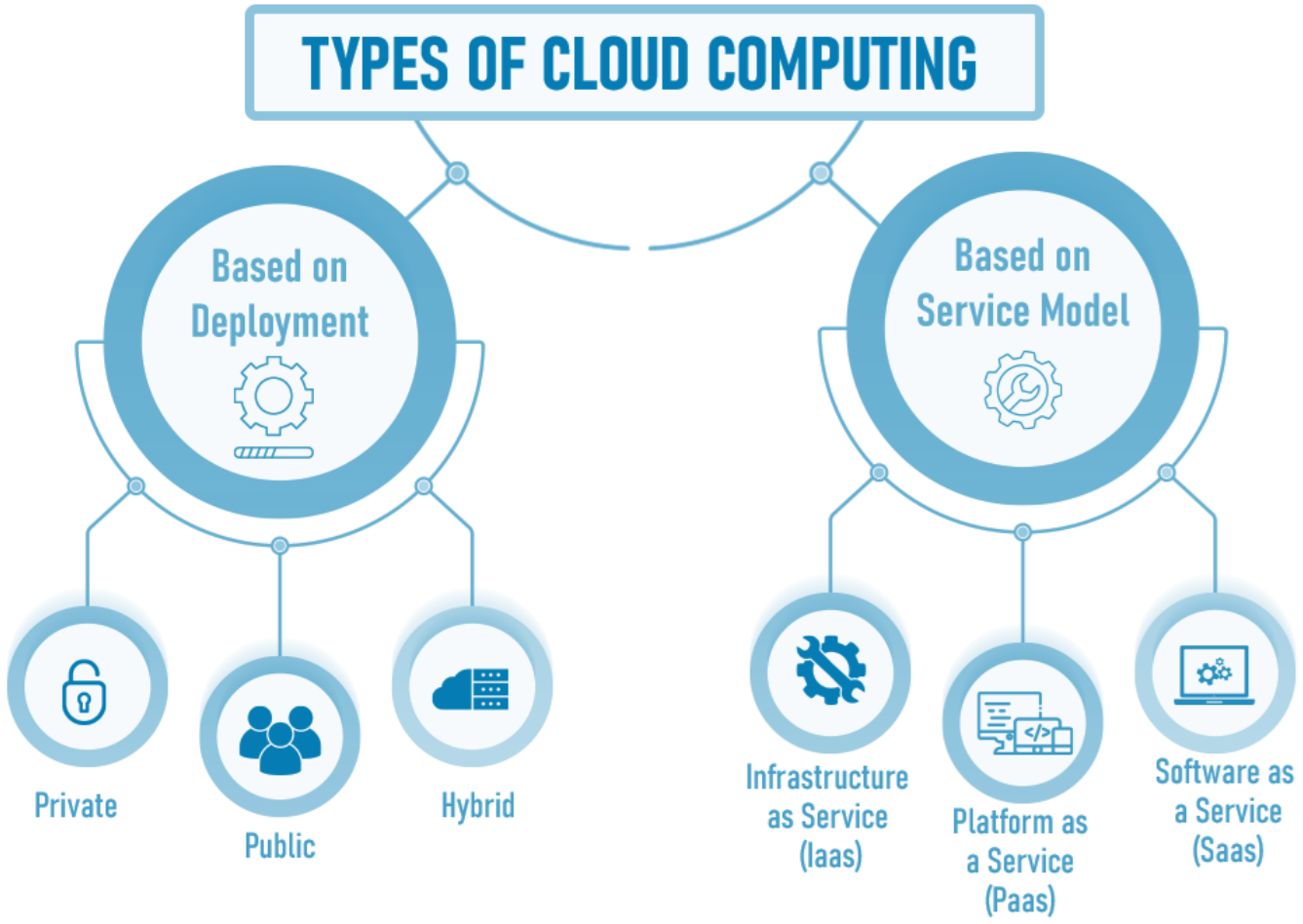
**Applications**

- Improve predictions of supply and demand
- Predictive maintenance
- Facilitate demand response
- Manage and control grids

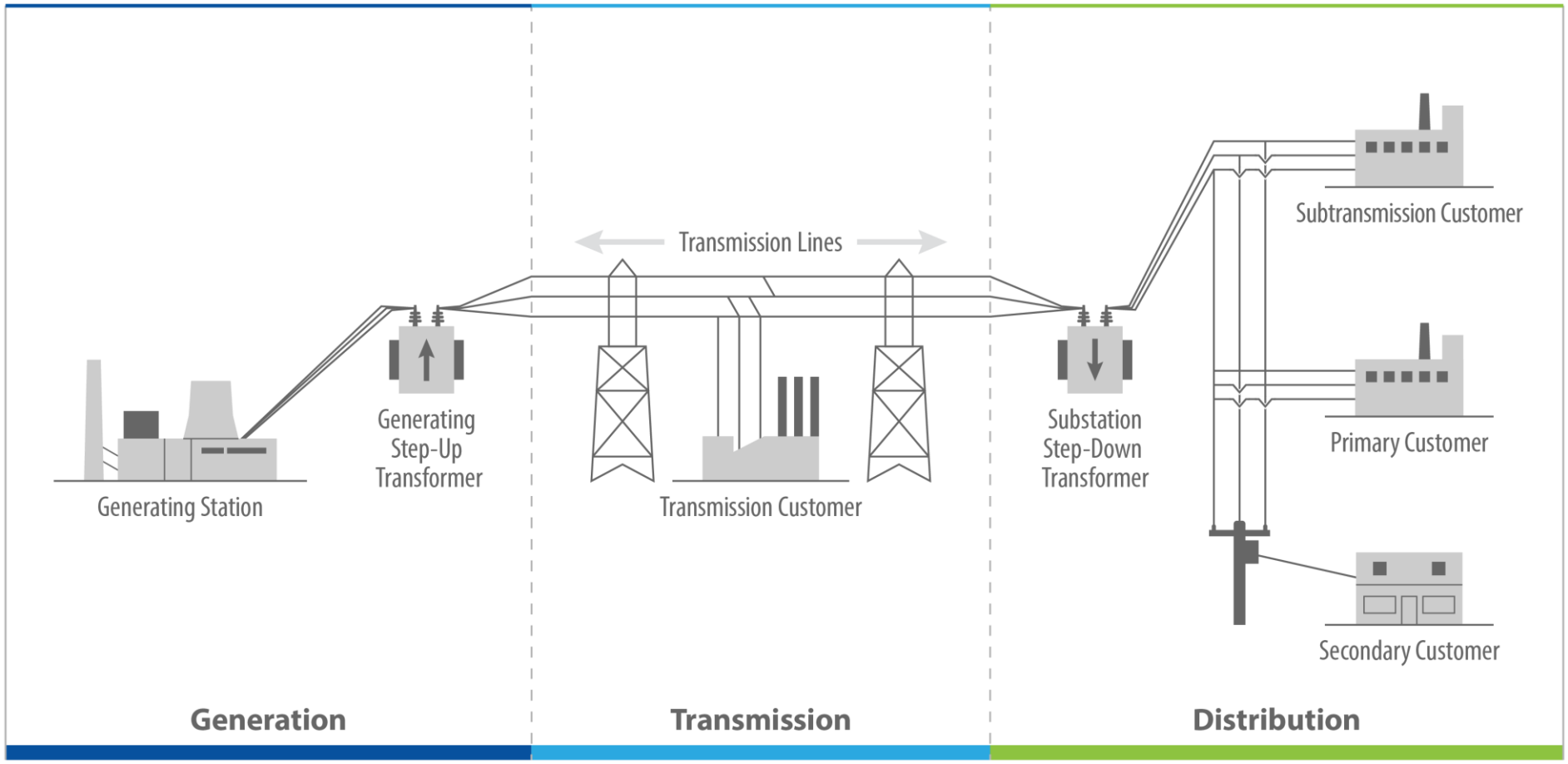
**Cyber Considerations**

- Data security
- Influence of biases or errors
- Miscorrelations due to insufficient training, data, or coding mistake
- Adversarial ML

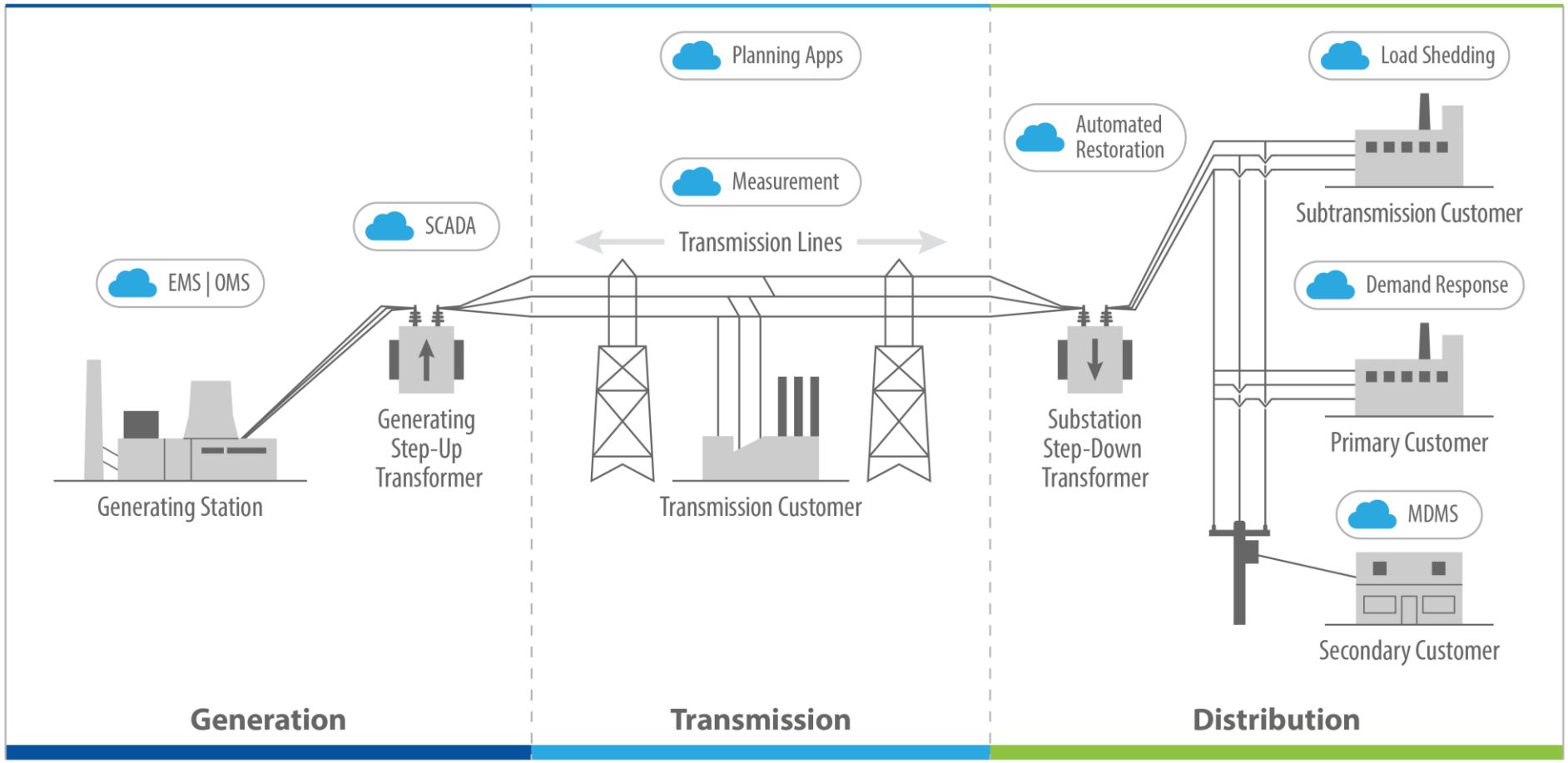
# Cloud Computing



# Cloud is Everywhere



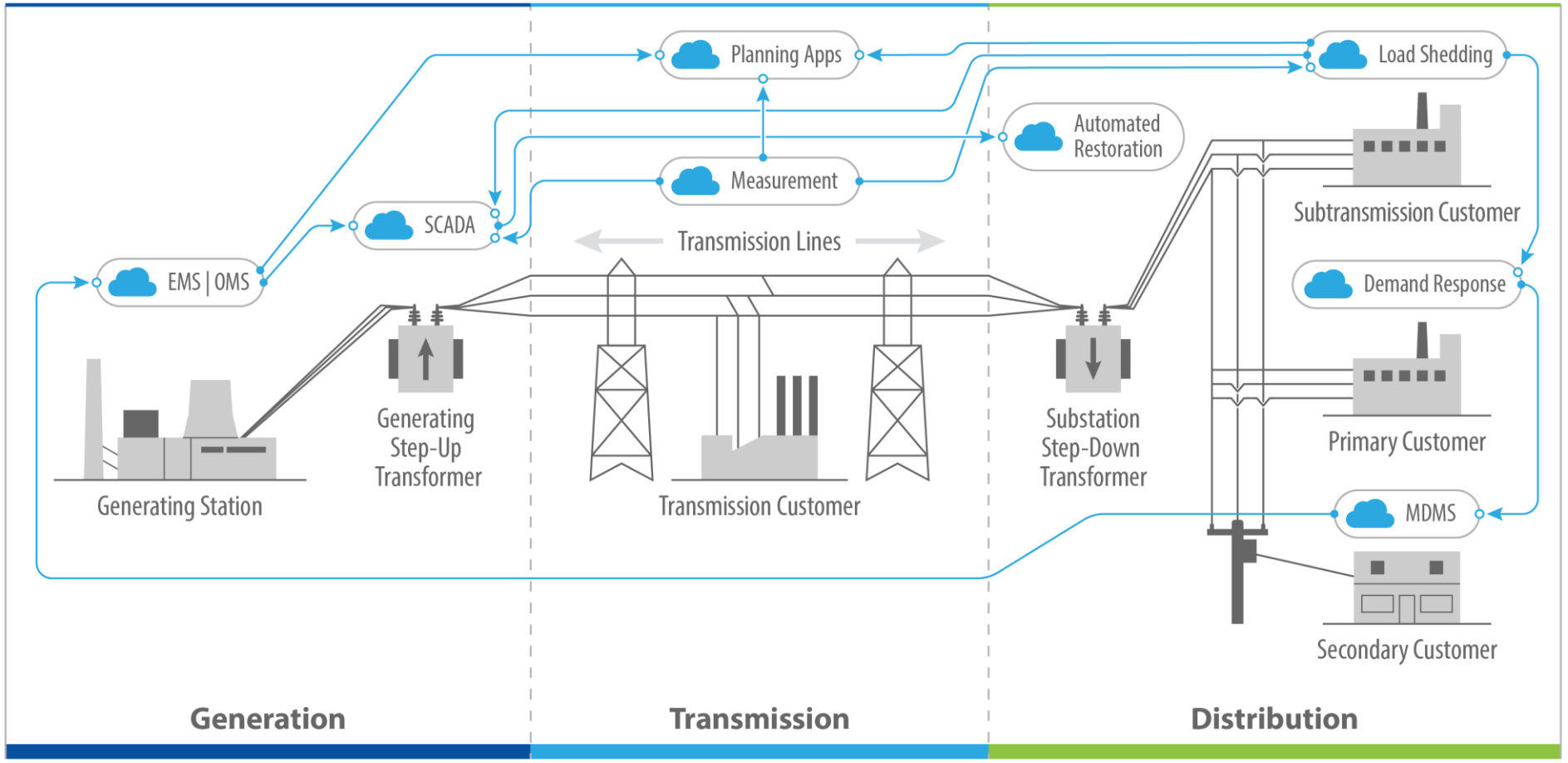
# Cloud is Everywhere




## Applications

- Analyze sensors that collect vast amounts of data
- Digital twins
- Supply chain management
- Access to third-party services

# Interconnected Interdependent Cloud is Everywhere




## Cybersecurity Considerations

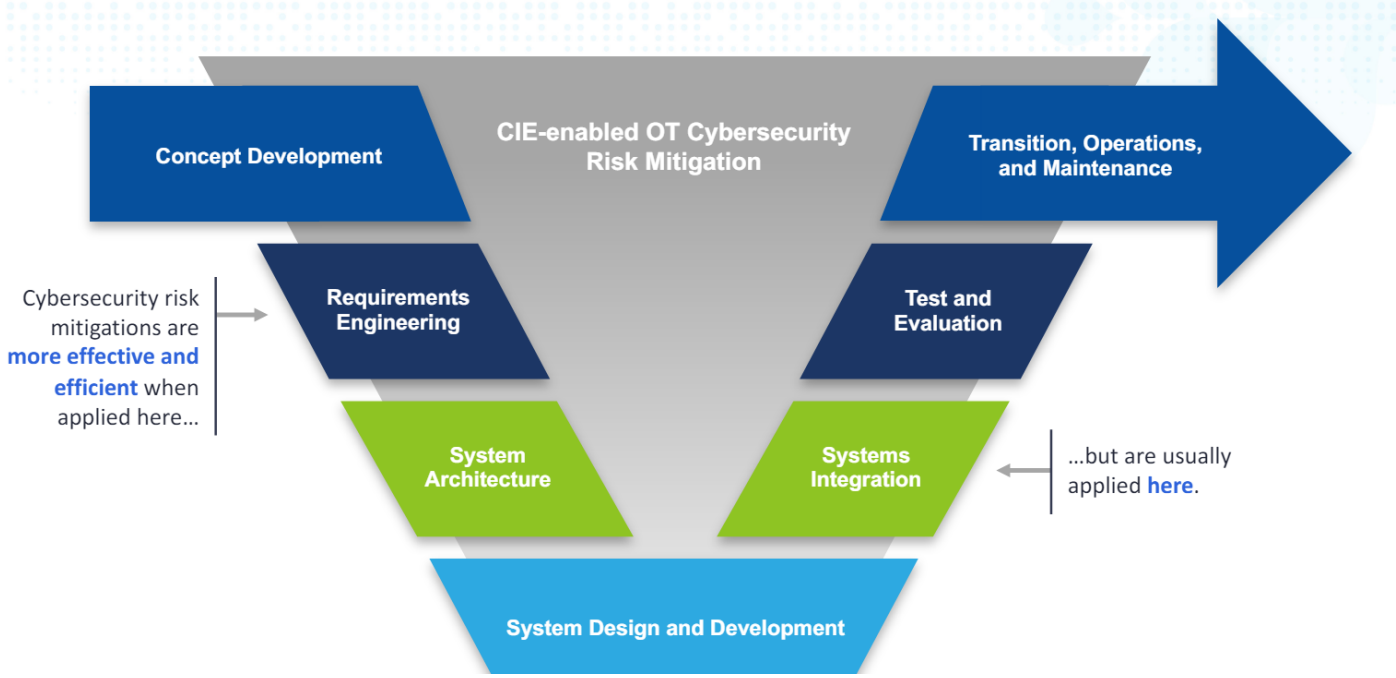
- Where is your data and who has access to it?
- What critical functions are in the cloud?
- Potential consequences if the system fails
- Cloud computing supply chain

# INL's Solution: Cirrus

- A **consequence-driven decision support framework** for entities to assess their grid modernization deployment strategy in the cloud
- Test against use cases and partner users **enabling adequate assessment** of deployment plans.

# INL's Solution Pt. 2: Cyber-Informed Engineering

- Uses design **decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- Offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.



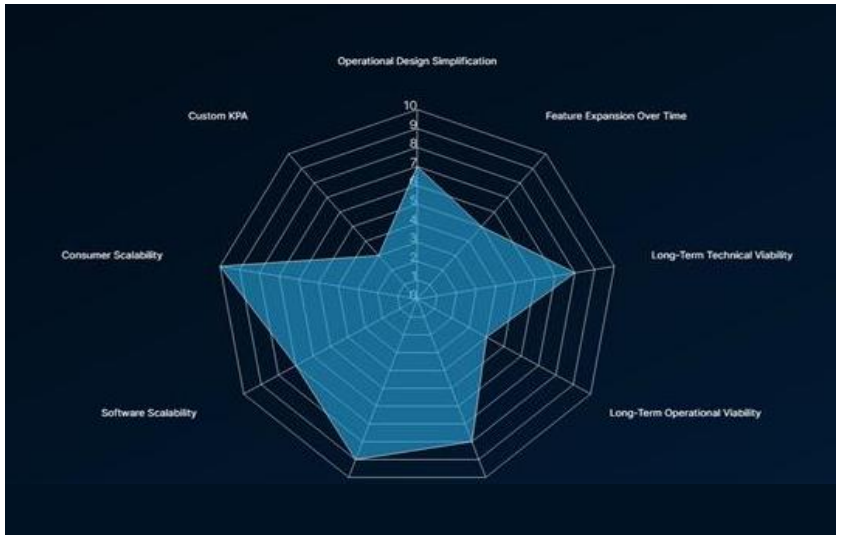

- Focuses on **engineers and technicians**, and provides a framework for cybersecurity education, awareness, and accountability.
- Aims to engender a **culture of security** aligned with the existing industry safety culture.

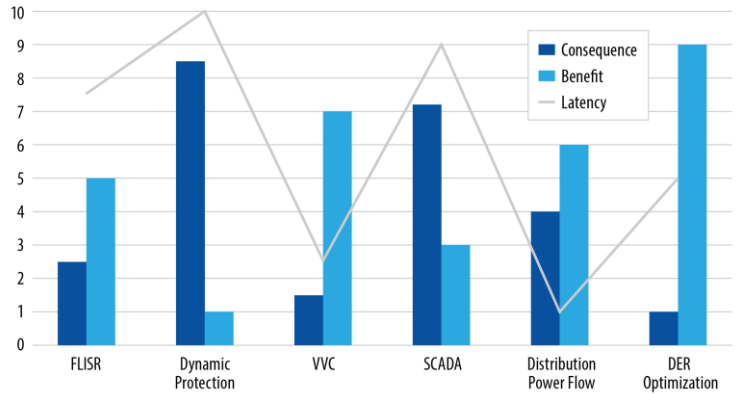
# **Output:** *So You Did the Framework, What Do You Get at the End?*

**Cloud Solution Utilities: your use case**

- **Infrastructure Evaluation:** audit existing systems for seamless cloud integration
- **Benefits:** (e.g., efficiency, scalability)
- **Risk Areas and Consequences:** (e.g., cyber threats, data breaches)
- **RFP Guideline**

- **Key Guidelines for Cloud Integration:** (e.g., infrastructure evaluation, regulatory compliance, workforce capability, etc.)
- **Cost-benefit Analysis:** analyze costs for justifying cloud migration investment
- **Workforce Capability:** equip your workforce for a smooth cloud transition
- **Path Forward:** strategize your path with informed decision-making



# Cloud Application: Present and Future

**Today:**

- Consider **interdependent consequences and benefits** of a cloud deployment for electric grid controls and applications
- Develop understanding of framing cloud applications.

**Tomorrow:**

- **Apply lessons** learned and driven cyber-informed frameworks.

**Future:**

- **Evaluate trends** in cloud deployment in infrastructure.

Learn more or get involved: emma.stewart@inl.gov.

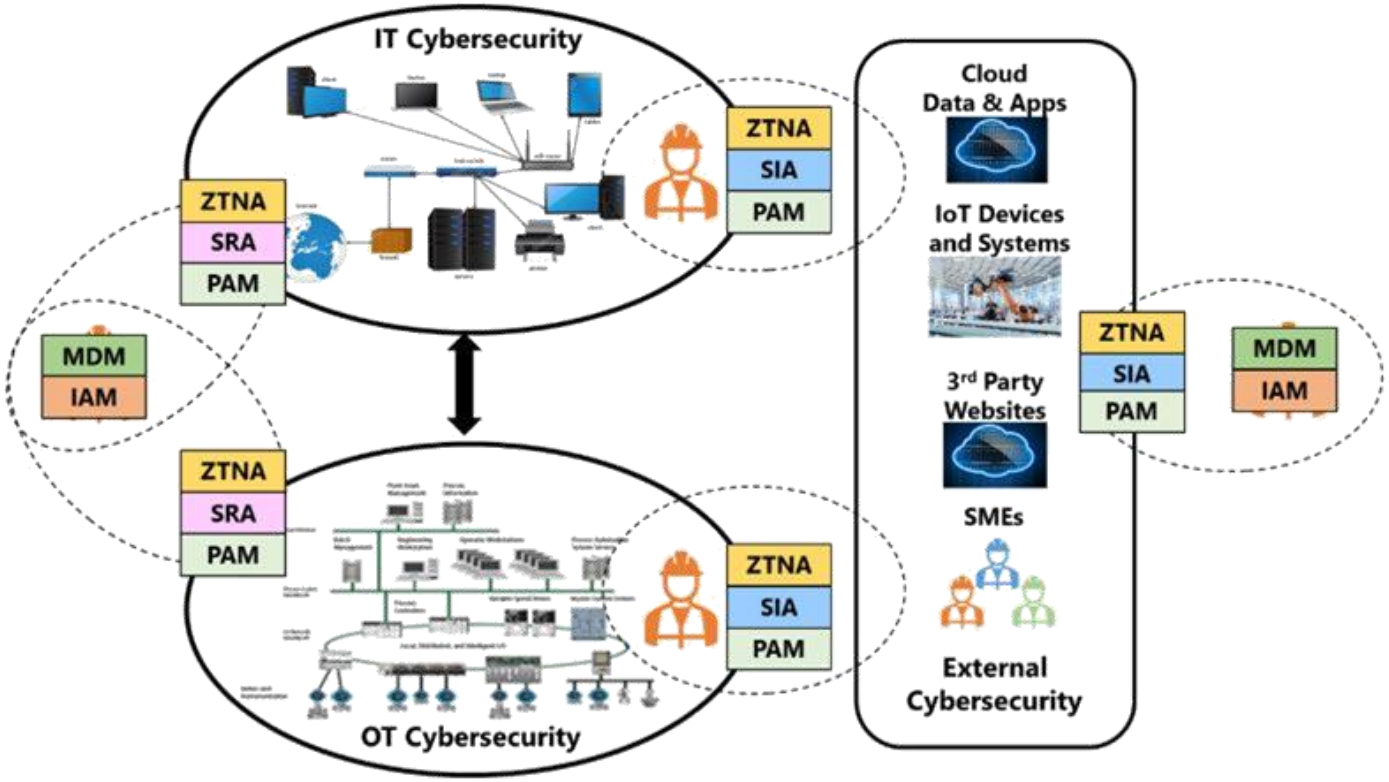
# Zero-Trust Architectures

***Trust but verify***

- **Why**
  - OT networks are an attractive target
  - 3rd party access increasingly common
  - Shared accounts among users make monitoring difficult
  - VPNs and other network architecture components have known vulnerabilities
- **What**
  - Move from static, network-based perimeters to focus on assets, users, and resources
  - Authentication and authorization (both subject and device) performed for each new session

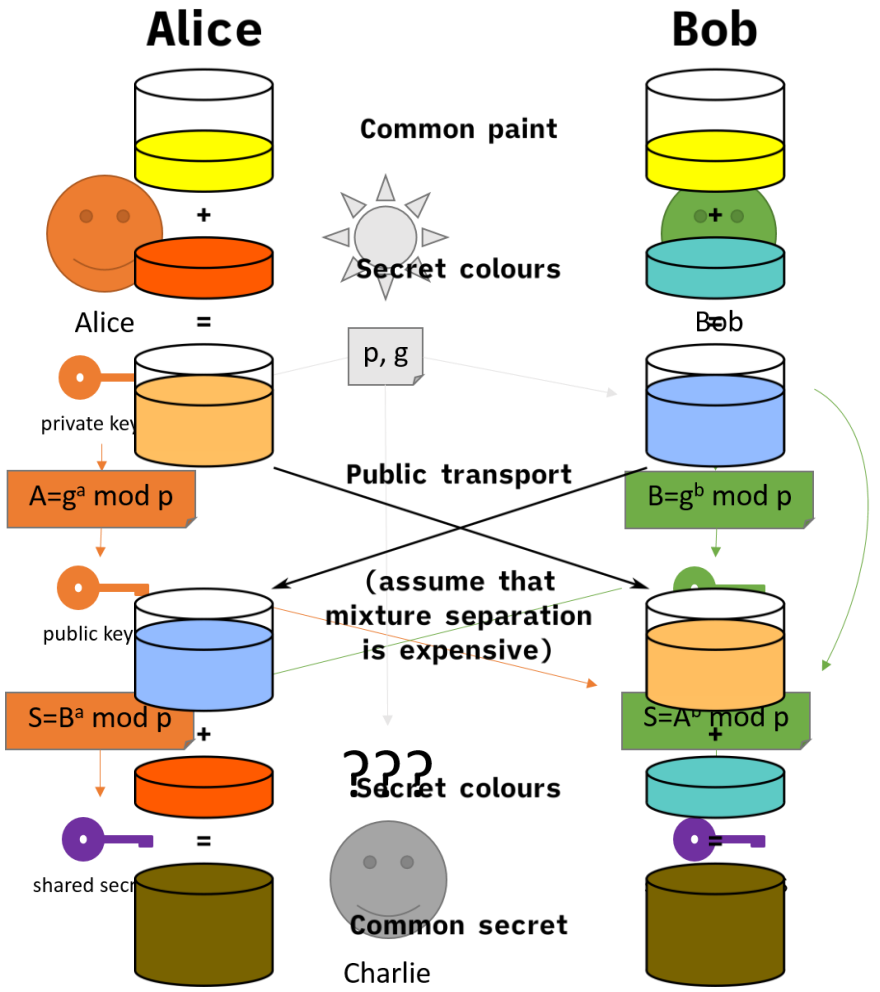
# Zero-Trust Architectures

- **Applications**
  - BYOD policies for grid-edge devices
  - Third-party vendor access
  - Generic and shared user accounts
- **Challenges**
  - Can be difficult to get full visibility in OT networks
  - Many OT assets have longer lifetimes than IT assets
  - Security must not impede critical functionality
  - Wholesale changes unlikely to work within organizational cultures



# Post Quantum Cryptography

- **Why?**
  - Existing algorithms are not unbreakable, they just take a long time to brute force
  - Quantum computing can break traditional encryption much faster
- **Applications**
  - Small, lab scale quantum computers have been built
  - NIST announced first four quantum-resistant algorithms in 2022
  - Three algorithms expected to be ready for use in 2024
- **Risks**
  - Early stages of research




**Public key exchange**
**Diffie-Hellman algorithm**

# References


Machine learning and AI

- https://www.iea.org/commentaries/why-ai-and-energy-are-the-new-power-couple
- https://www.latitudemedia.com/news/seven-ways-utilities-are-exploring-ai-for-the-grid
- https://www.energy.gov/articles/doe-announces-new-actions-enhance-americas-global-leadership-artificial-intelligence (multiple reports linked)

Cloud Computing

- https://www.forbes.com/sites/forbestechcouncil/2023/06/26/using-cloud-computing-to-work-toward-a-more-modern-electrical-grid/?sh=19560fe8692f
- https://power.nridigital.com/future_power_technology_apr23/applications-cloud-computing-power-industry



Cirrus Contact:

Emma.Stewart@inl.gov

# References


## Zero Trust Architecture

- https://cyolo.io/blog/how-to-overcome-ot-security-challenges-with-zero-trust-access
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- https://claroty.com/blog/five-important-considerations-to-implementing-zero-trust-in-ot-environments

## Post quantum cryptography

- https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
- https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
- https://www.cisa.gov/quantum
- https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
- **https://doi.org/10.3390/en15030714**
- https://www.mdpi.com/1996-1073/16/5/2240

Contact: Megan Culler
Megan.Culler@inl.gov

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.*