Artificial Intelligence: Risks and Potential

From the perspective of SERC and the Bulk Power System

September 2024

Maggie Peacock
Manager, Analytics and Data Management

Agenda

- SERC Overview
- What I mean when I say AI
- AI Potential
- AI Failures (not every problem is a nail)
- Trends in Global AI Public Policy and Regulations
- Discussion of AI Risks
- Risk Mitigation
- Use Case Discussion

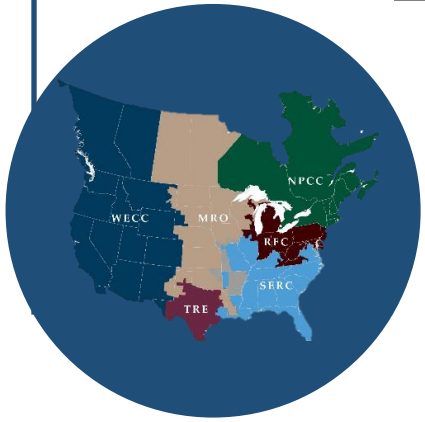
Electric Reliability Organization Enterprise

Standard Development	Assessments	Studies	Whitepapers
Over 90 Reliability Standards	Long Term and Seasonal	Risk Reliability Studies, Transfer Capability	Technical Whitepapers and Reports

Audits	Enforcement	Outreach	Regional Studies
In the field and on-site compliance verification	Mandatory Mitigation; monetary and non-monetary sanctions for non-compliance	Webinars, Workshops, Newsletters	Sub-regional assessments and studies

NERC

NERC as the ERO operates under specific authorities established in the 2005 Federal Power Act. NERC has oversight of the six regions and is evaluating reliability risk on an inter-national scale.



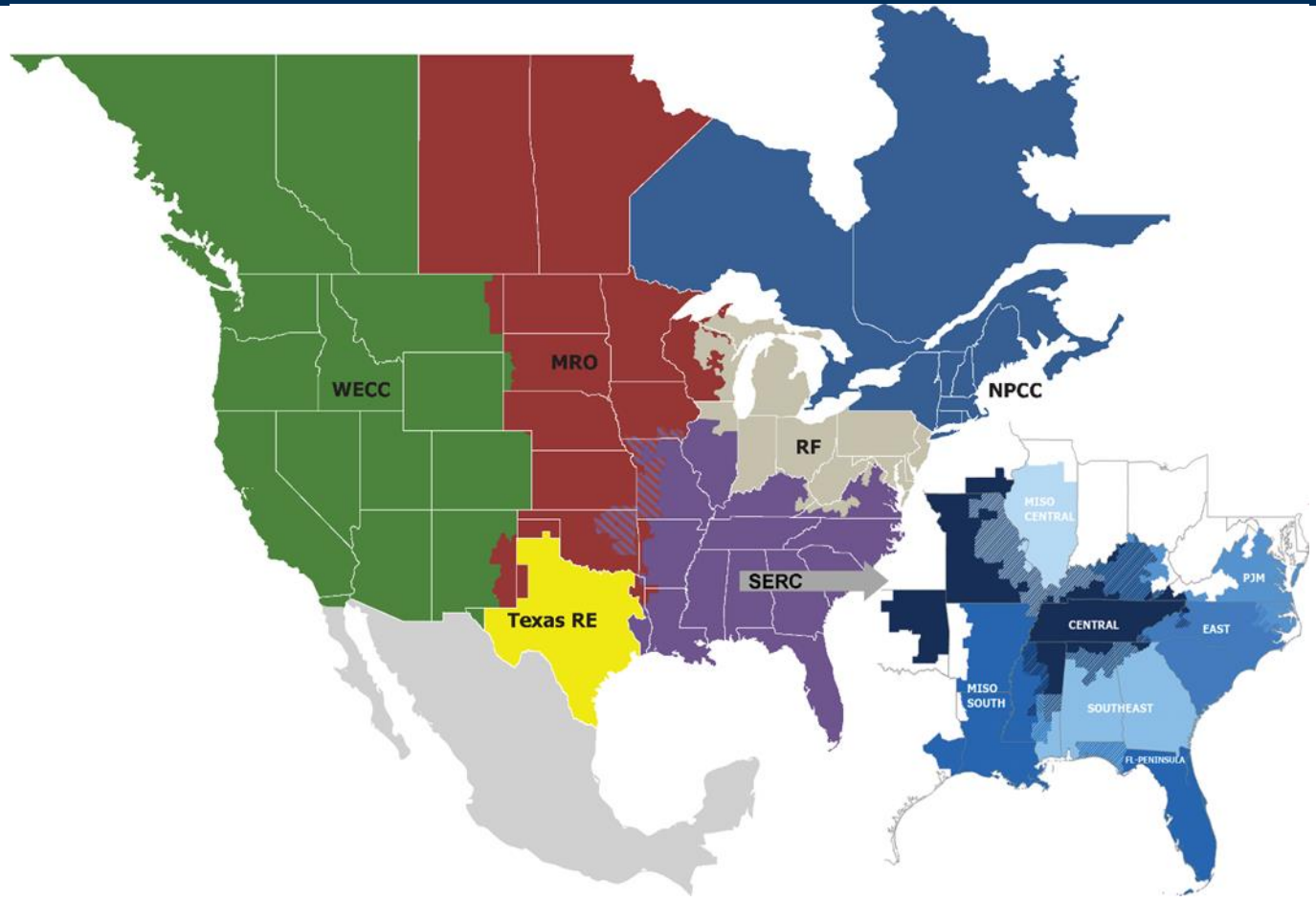
Regions

The regions have the authority to audit and enforce the NERC Reliability and Security Standards with their Entities. The regions also provide studies, assessments and evaluate Reliability Risk specific to their region as well as providing outreach and training.

SERC

SERC Overview

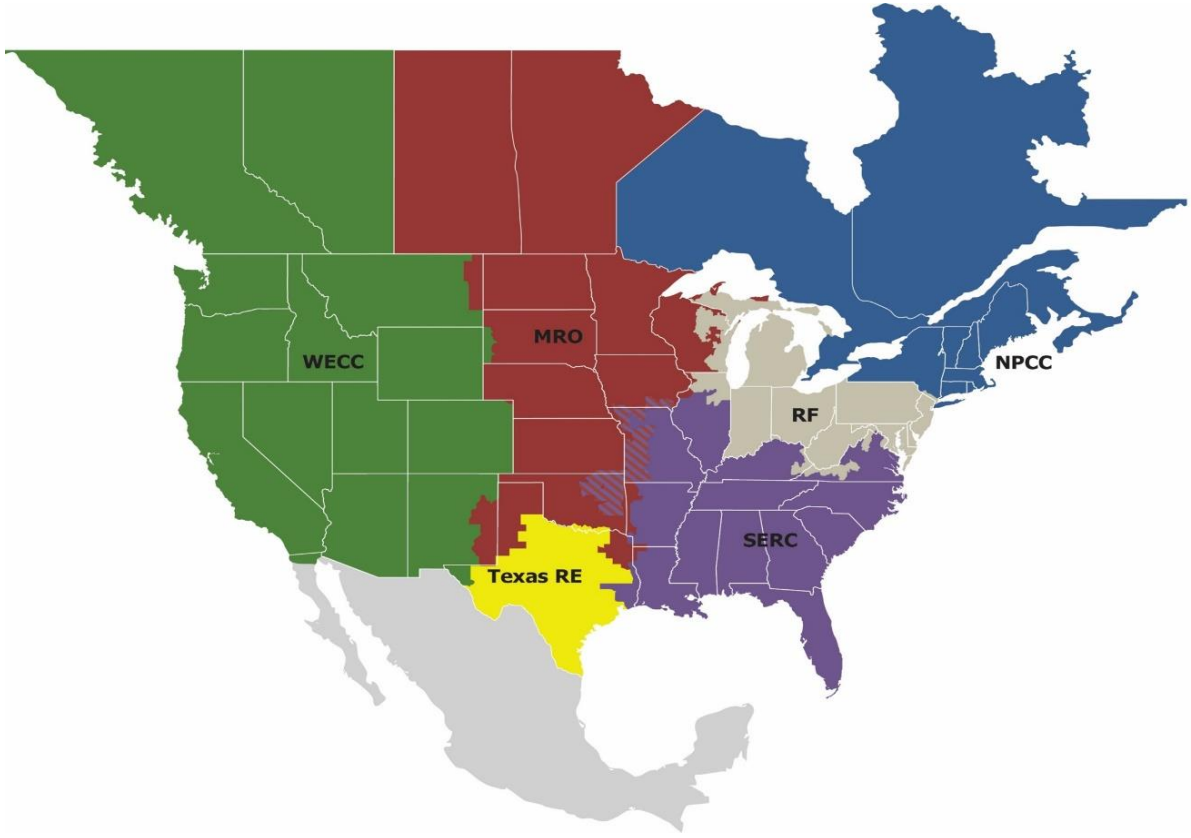
SERC's Mission is to assure effective and efficient reduction of risks to the reliability and security of the bulk power system.



16 states	97M people	300+ Registered Entities	310 GW generation	122k miles of transmission	261 GW load

The Electric Reliability Organization Enterprise

- We are regulators of the electric industry
- We do not own or operate grid assets or energy markets
- Our mission is solely reliability and security of the bulk electric system
- We are an objective and independent resource



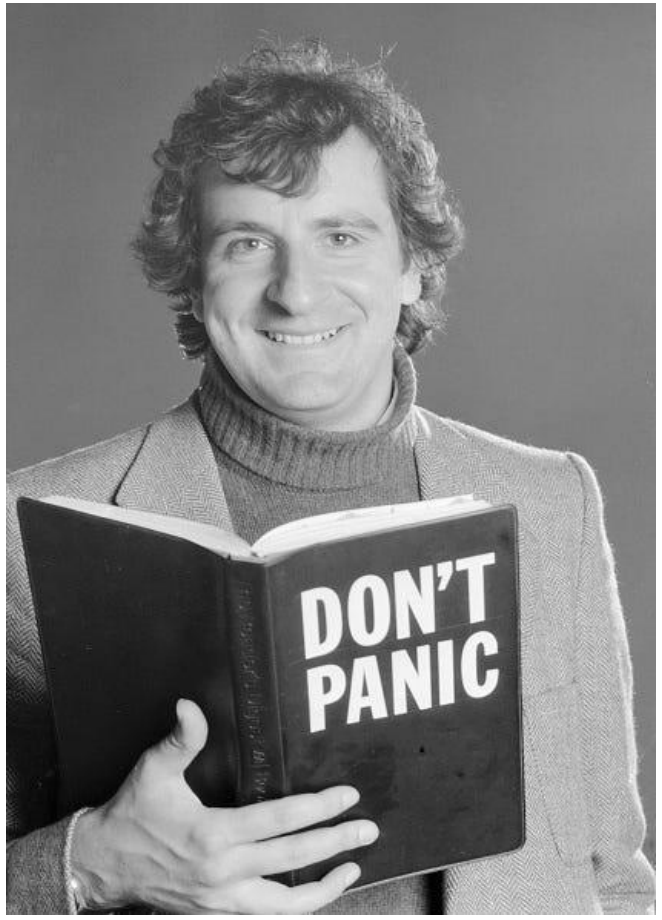
Artificial Intelligence

Rules to describe our relationship with technology:

1) Everything that's already in the world when you're born is just normal,
2) Anything that gets invented between then and before you turn thirty is incredibly exciting and creative and with any luck you can make a career out of it.
3) Anything that gets invented after you're thirty is against the natural order of things and the beginning of the end of civilisation as we know it…

<u>until it's been around for about ten years when it gradually turns out to be alright really.</u>

- Douglas Adams, August 1999



Artificial Intelligence

"…machine-based recommendations or system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."

-National Artificial Intelligence Act of 2020

In other words, technology that simulates human intelligence.

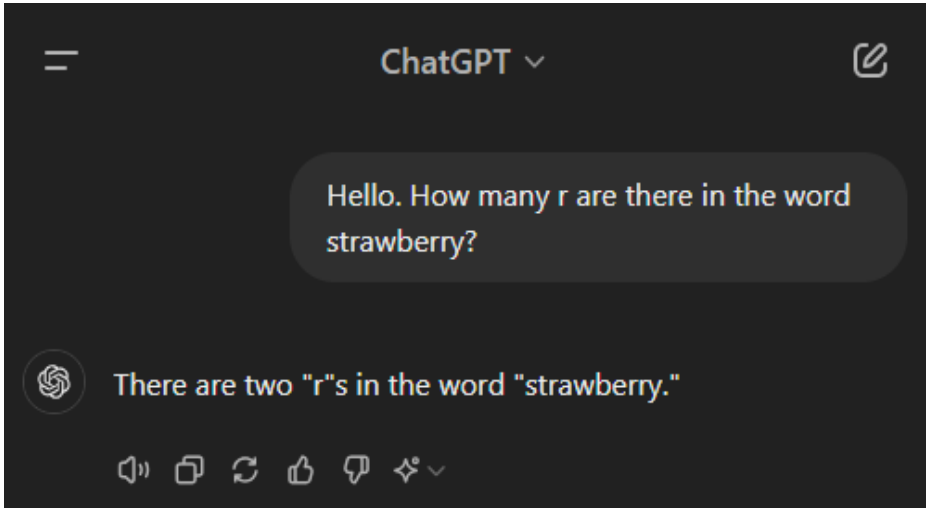
Artificial Intelligence

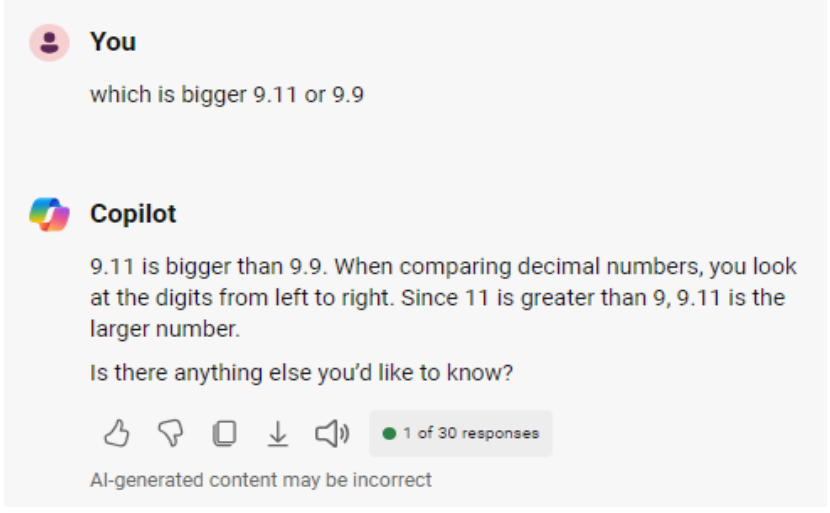
AI is not

- Human Intelligence
- Infallible
- Operate in a vacuum or isolation
- Replacement for Human Creativity
- Bias-free
- Free from ethical concerns
- Immune to technical limitations

Not every problem is a nail

AI: the right tool for the job?





Top Trends in Global AI Public Policy and Regulations

Trustworthy and Responsible AI

- Human-centricity and diversity
- Responsible innovation
- Governance and accountability
- Transparency and explainability
- Contestability and redress
- Safety and security
- Robustness and resilience
- 21st century intellectual property rights
- Effective and efficient regulatory process

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47843

April 3, 2024

Laurie Harris
Analyst in Science and Technology Policy

Chris Jaikaran
Specialist in Cybersecurity Policy

Highlights of the 2023 Executive Order on Artificial Intelligence for Congress

On October 30, 2023, the Biden Administration released Executive Order (E.O.) 14110 on *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. It establishes a government-wide effort to guide responsible artificial intelligence (AI) development and deployment through federal agency leadership, regulation of industry, and engagement with international partners.

The E.O. directs over 50 federal entities to engage in more than 100 specific actions to implement the guidance set forth across eight overarching policy areas.

- *Safety and security*. The E.O. promotes the development and implementation of repeatable processes and mechanisms to understand and mitigate risks related to AI adoption, including with respect to biosecurity, cybersecurity, national security, and critical infrastructure.
- *Innovation and competition*. The E.O. compels actions to attract AI talent to the United States, understand novel intellectual property (IP) questions, protect inventors and creators, and promote AI innovation, including at startups and small businesses.
- *Worker support*. The E.O. states that AI adoption may be disruptive to
- *Consideration of AI bias and civil rights*. The E.O. states that AI mode
- *Consumer protection*. The E.O. instructs agencies to enforce existing,
- *Privacy*. The E.O. calls for the evaluation and mitigation of privacy ris
- *Federal use of AI*. The E.O. requires the Office of Management and Bu
- *International leadership*. The E.O. declares that the United States shou

Congressional Research Service

BRIEFING
EU Legislation in Progress

European Parliament

Artificial intelligence act

OVERVIEW

European Union lawmakers signed the artificial intelligence (AI) act in June 2024. The AI act, the first binding worldwide horizontal regulation on AI, sets a common framework for the use and supply of AI systems in the EU.

The new act offers a classification for AI systems with different requirements and obligations tailored to a 'risk-based approach'. Some AI systems presenting 'unacceptable' risks are prohibited. A wide range of 'high-risk' AI systems that can have a detrimental impact on people's health, safety or on their fundamental rights are authorised, but subject to a set of requirements and obligations to gain access to the EU market. AI systems posing limited risks because of their lack of transparency will be subject to information and transparency requirements, while AI systems presenting only minimal risk for people will not be subject to further obligations.

The regulation also lays down specific rules for general purpose AI (GPAI) models and lays down more stringent requirements for GPAI models with 'high-impact capabilities' that could pose a systemic risk and have a significant impact on the internal market.

The AI Act was published in the EU's Official Journal on 12 July 2024. It entered into force in August 2024.

Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts		
Committees responsible:	Internal Market and Consumer Protection (IMCO) and Civil Liberties, Justice and Home Affairs (LIBE) (jointly under Rule 58)	COM(2021)206 21.4.2021 2021/0106(COD)
Rapporteurs:	Brando Benifei (S&D, Italy) and Dragoș Tudorache (Renew, Romania)	
Shadow rapporteurs:	Deirdre Clune, Axel Voss (EPP); Petar Vitanov (S&D); Svenja Hahn, (Renew); Sergey Lagodinsky, Kim Van Sparrentak (Greens/EFA); Rob Rooken, Kosma Złotowski (ECR); Jean-Lin Lacapelle, Jaak Madison (ID); Cornelia Ernst, Kateřina Konecna (The Left)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Procedure completed.	Regulation (EU) 2024/1689 OJ L, 2024/1689, 12.7.2024	

EPRS | European Parliamentary Research Service

Author: Tambiama Madiega
Members' Research Service
PE 698.792 – September 2024

EN

Source: Gartner Research 2023 Data and Analytics Summit *Navigating the New AI and GenAI Global Regulatory Dynamics* & https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf & https://crsreports.congress.gov/product/pdf/R/R47843

Risk Categories Highlighted by CESER & LLNL

Unintentional Failure Modes of AI

AI created for beneficial purposes, but which is unintentionally misused or has unintentional failures, leading to negative outcomes. This risk category encompasses challenges with bias, extrapolation, misalignment, and the energy use of AI.

Adversarial Attacks Against AI

AI systems are susceptible to a variety of novel vulnerabilities, in addition to traditional cybersecurity vulnerabilities. Common types of attacks include poisoning, evasion, and data extraction.

Hostile Applications of AI

AI can be created and used by adversaries to plan or execute cyber or physical attacks on energy infrastructure. The use of AI by threat actors has lowered the difficulty of attacks, enabling less-sophisticated adversaries to carry them out.

Compromise of the AI Software Supply Chain

As AI is software, it is subject to the same cybersecurity risks of other software. An adversary may exploit AI software not only to attack the AI system, but also as an intrusion vector to a victim's broader energy infrastructure systems.

Embargoed
2024 SERC Regional Risk Report

Supply Chain Constraints: Increased attack surface due to multiple entities securing the bulk power system's infrastructure.

Extreme Weather Impacts: Extreme weather in the SERC region can damage infrastructure and disrupt fuel supply.

Resource Uncertainty: Accelerating changes in generating resources and fuel complicate planning and operations.

Shortage of Required Skillsets: This risk arises from a critical shortage of skilled staff in electrical operations, planning, and cybersecurity.

Exploitation of Vulnerabilities: Advanced tools and processes exploit bulk power system vulnerabilities, including ransomware.

06 **Rapid Nontraditional Load Growth:** Rapid load growth from new data centers and AI, is challenging the planning and operation of the BES.

07 **Lack of Fuel Diversity and Availability:** Transition to natural gas and variable generation challenges energy adequacy.

08 **Legacy Architecture Compatibility:** Aging infrastructure struggles with compatibility and support from vendors.

09 **Extreme Physical Events: Sabotage & Attacks:** Deliberate disruptions to Bulk Electric System facilities and equipment.

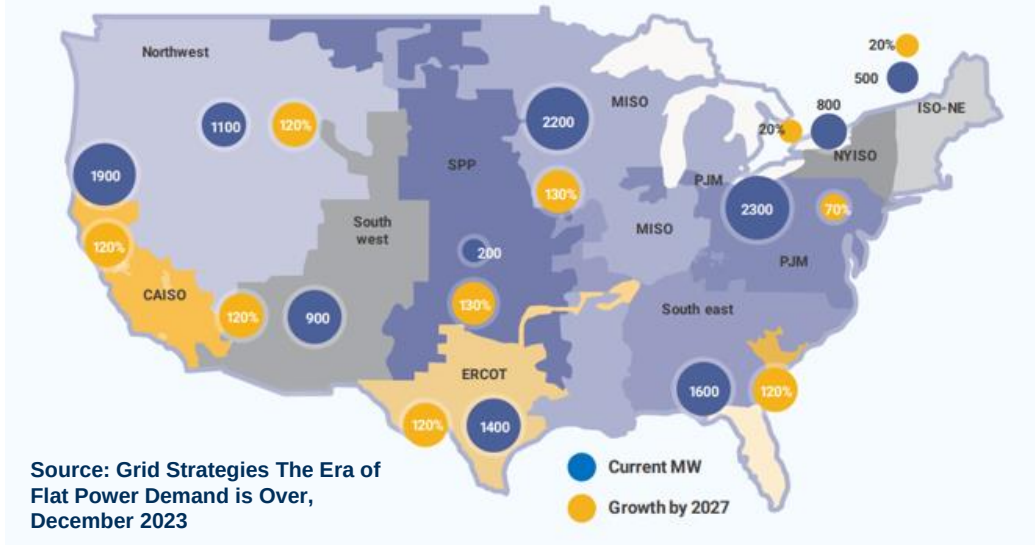
10 **Integrating Variable Energy Resources:** Renewable energy integration requires backup planning due to weather dependence.

Embargoed
2024 SERC Regional Risk Report

Upcoming 2024 Regional Risk Report

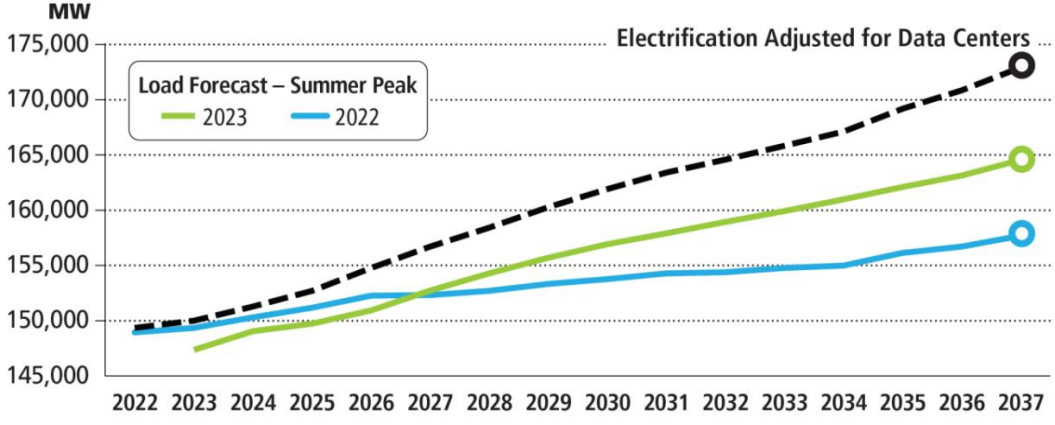
- SERC identifies Rapid Nontraditional Load Growth as a top regional risk - *"Rapid load growth from new data centers and AI is challenging the planning and operation of the Bulk Power System"*
- SERC has also identified Lack of GenAI Governance as an emerging risk

Data Center Growth by 2027 ©2022 BCG Analysis



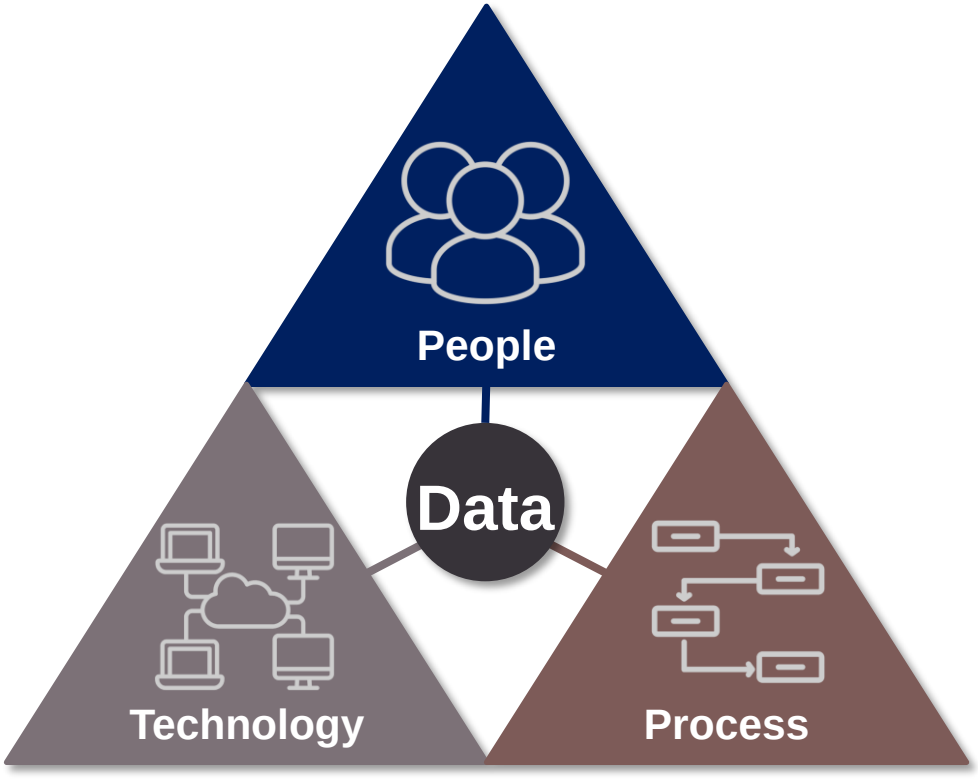
Source: Grid Strategies The Era of Flat Power Demand is Over, December 2023

PJM: Impacts of Electrification and Data Center Load on Forecasts



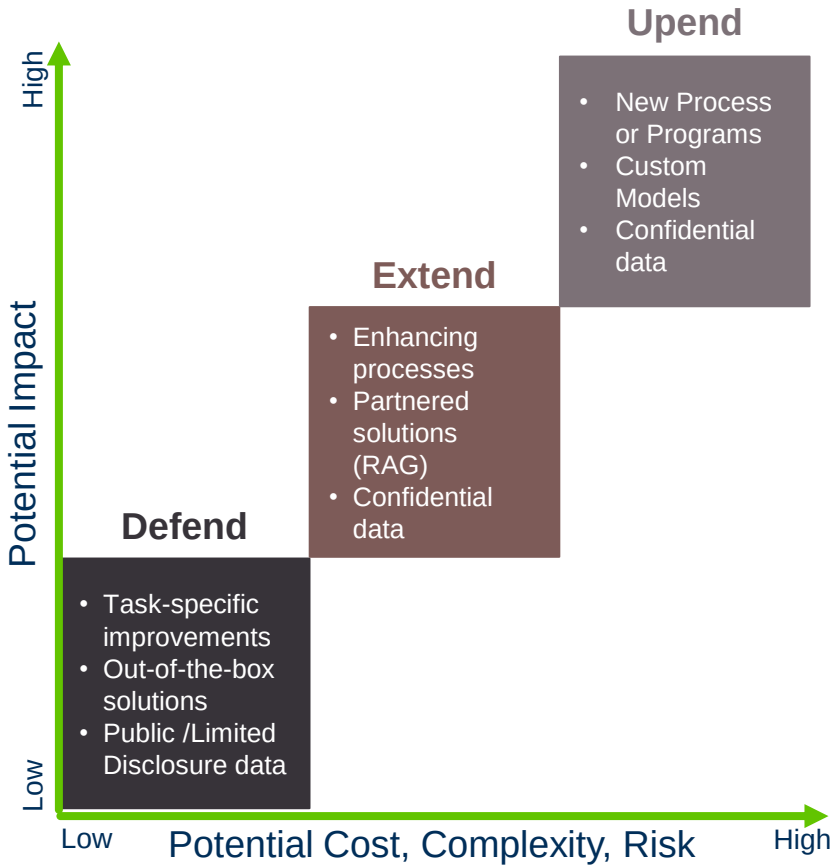
Source: Energy Transition in PJM Resource Retirements, Replacements & Risks

Mitigations



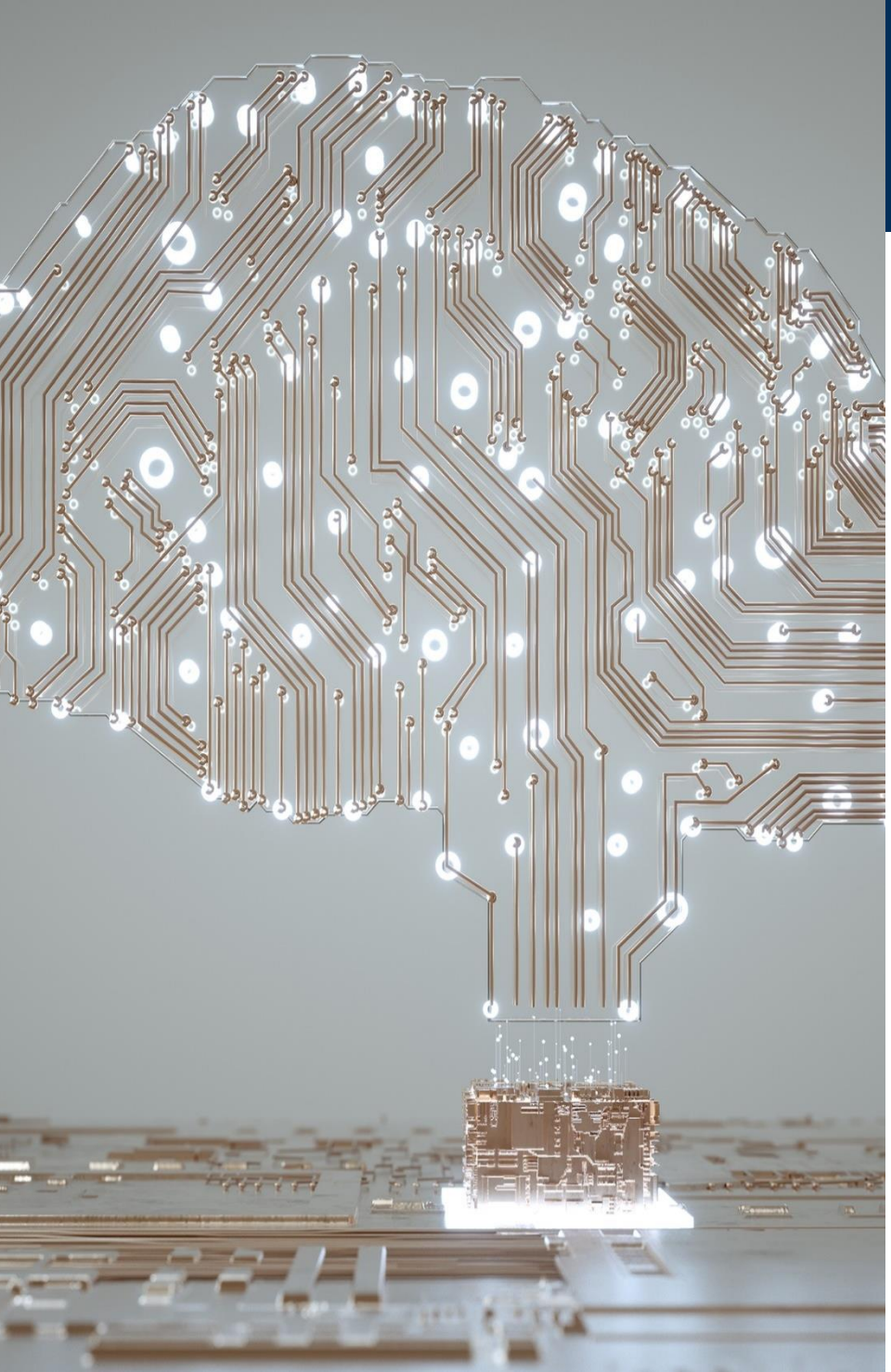
- AI Governance
  - AI Strategy
  - Policy
  - Risk Framework
  - Education & Training
- Data Management
  - Data Classification
  - Data Quality
- IT & Security
  - Security Controls
  - AI ready Infrastructure

Opportunities



Next Steps

- Use Case Development
- Partnerships
- Proof of Concepts
- Scalability



Upcoming Events & Contact Information

- regulatoryaffairs@serc1.org
- mpeacock@serc1.org
- mlitz@serc1.org

- www.serc1.org/outreach

References

- National Artificial Intelligence Initiative Act of 2020, H.R. 6216 116th Congress, March 2020
  - *Source: https://www.congress.gov/bill/116th-congress/house-bill/6216*
- Machine learning (ML) is one among many other branches of AI.
  - *Source: https://aws.amazon.com/compare/the-difference-between-artificial-intelligence-and-machine-learning/*
- Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure, U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response, April 2024.
  - *Source: https://www.energy.gov/sites/default/files/2024-04/DOE CESER_EO14110-AI Report Summary_4-26-24.pdf*
- Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST, January 2023
  - *Source: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf*
- Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST, April 2024
  - *Source: https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf*
- *Grid Strategies The Era of Flat Power Demand is Over, December 2023*
  - *Source: https://gridstrategiesllc.com/wp-content/uploads/2023/12/National-Load-Growth-Report-2023.pdf*
- *Energy Transition in PJM Resource Retirements, Replacements & Risks, February 2023*
  - *Source: https://www.pjm.com/-/media/library/reports-notices/special-reports/2023/energy-transition-in-pjm-resource-retirements-replacements-and-risks.ashx*

SERC Reliability Corporation (SERC) is one of six regional entities that, in conjunction with the North American Electric Reliability Corporation (NERC), collectively form the Electric Reliability Organization (ERO) Enterprise. Our primary responsibility is to preserve and enhance the reliability, resilience, and security of the bulk power system.

Mission:

To ensure effective and efficient reduction of risks to the reliability and security of the bulk power system

Under the authority of the Federal Energy Regulatory Commission (FERC), NERC, SERC, and the other regional entities develop and enforce Reliability Standards, conduct annual assessments of seasonal and long-term reliability, monitor the bulk power system through system awareness, and educate stakeholders about risks to the system.

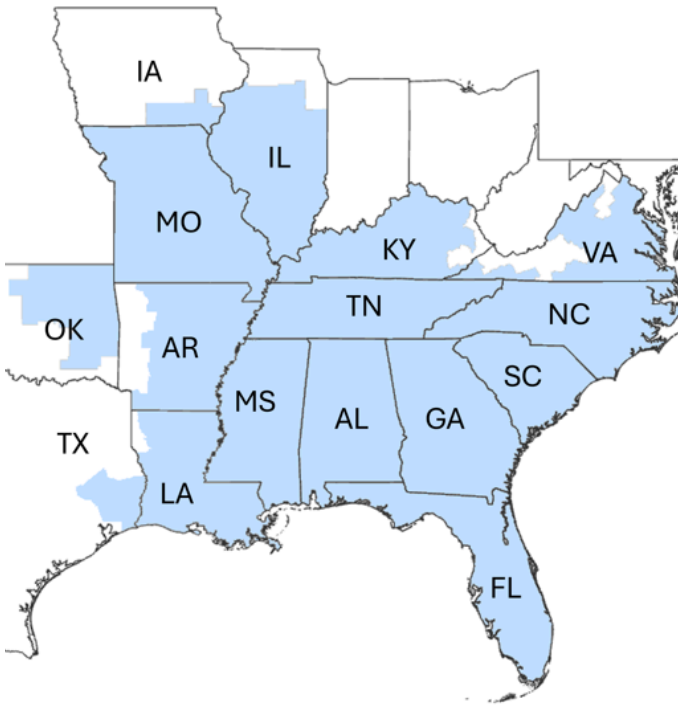
SERC at a Glance

300+ Registered Entities

97 million estimated population

118k miles of bulk electric system transmission lines

261 GW forecasted load in 2024

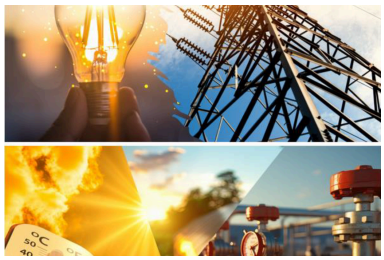


Resource for States

- Trusted and credible independent expert
- Grid reliability-focused education
- Available to discuss reliability and security issues important to you

Contact Us

www.serc1.org
regulatoryaffairs@serc1.org
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273



What Does SERC Do?

Reliability Assessment & Performance Analysis

- Deliver and empower industry professionals with essential skills and knowledge critical to safeguarding the electric grid via our enterprise-level learning management system (LMS), **SERC University, newsletters**, **webinars,** and through various **workshops** and **training** throughout the year.

Topic Matter(s):

-Physical and Cybersecurity
-CIP and O&P Standards
-Supply Chain Resources
-Insider Threats
-Inverter-Based Resources (IBRs)
- Assessment/Analysis/Report brief

Outreach & Training

- Provide Bulk Power System (BPS) analysis, data gathering, and investigation of events to identify BPS reliability risks in the SERC footprint.

Content:

- Regional Winter/Summer Reliability Assessment(s).
- Annual Long Term Reliability Assessment Report.
- Probabilistic Assessment for Resource Adequacy Report.
- Situation Analysis
- Events Analysis
- Reliability Risk and Operational Assessments.
- Reliability assessment and performance analysis.

Audit

- In the field and on-site compliance verification.

Compliance & Enforcement

- Monitoring compliance with and enforcing mandatory Reliability Standards (both North American wide and regional), certification of registered entities, and registration of owners, operators and users of the Bulk Power System (BPS).
- Mandatory Mitigation; monetary and non-monetary sanctions for non-compliance.

regulatoryaffairs@serc1.org

www.serc1.org

3701 Arco Corporate Dr, Office 300,
Charlotte, NC 28273 United States