Accessing Careers in Energy Summit

CASE COMPETITION INFO
READ FIRST & RESOURCES

Gridlock: Securing the Future of Load-Driven Energy Risk

Case Competition Title: Gridlock: Securing the Future of Load-Driven Energy Risk

Background:
Over the past decade, the electric power grid has evolved rapidly in response to decarbonization, digitization, and decentralization. Today, that evolution is accelerating due to the rise of large, dynamic, and often unpredictable loads. Examples include:
- Data centers, including those supporting AI model training
- Crypto mining operations
- Large-scale electric vehicle (EV) charging depots
- Direct-to-grid industrial electrification (e.g., green hydrogen)

These new high-demand loads are being integrated into regional grids faster than some infrastructure and cybersecurity strategies can adapt. These types of large electrical loads can be defined as a significant amount of power consumption when these systems are connected or used. The types of which are explained above. While these loads provide economic and technological benefits, they also introduce new vulnerabilities to the physical and cyber aspects of the grid.

Case Challenge:
Your team has been hired by an electric utility company that operates in a North American ISO/RTO market (A market where these local utilities buy energy wattages and sells to a consumer from an entity that controls the transmission of electrical energy). The utility is observing a rapid influx of requests to connect large, non-traditional loads to the grid. They are particularly concerned about how these loads could be:
1. Weaponized through cyber means (e.g., malware in control systems or automated demand manipulation)
2. Used as a vector for attacks (e.g., malicious actors targeting insecure APIs of load aggregators)
3. Disruptive to grid stability if cyber-physical risks are not mitigated

Prompt:
Develop a strategic analysis and response plan for the utility that addresses the following:

Part 1: Risk Assessment*:*
- Identify at least three categories of large loads that pose emerging threats to grid operations due to cybersecurity vulnerabilities.
- Explain how each could introduce new attack surfaces/vectors or systemic risks (e.g., through IoT, SCADA, DERMS platforms).
- Map how these risks align to the NIST Cybersecurity Framework and/or the NERC CIP standards.

Part 2: Cybersecurity Focus:
- Propose cybersecurity controls or detection mechanisms for utilities to deploy when onboarding large new

loads.
- Recommend methods for monitoring and responding to anomalous behavior, such as unexpected ramp-up/down cycles or unauthorized configuration changes.
- Address how the utility might collaborate with third-party operators (e.g., data centers or EV fleet owners) to enforce a baseline cybersecurity posture.

Part 3: Business and Regulatory Considerations:
- Outline how your cybersecurity strategy balances grid reliability, customer onboarding timelines, and regulatory expectations (e.g., FERC, DOE, state PUCs).
- Include recommendations for policies or interconnection agreements that ensure cybersecurity due diligence before permitting large load integration.

Deliverables:
1. Executive Briefing Slide Deck (15 slides max)
   - Summarize key findings, recommendations, and risk mitigations.

2. Technical Memo (5–7 pages)
   - Provide a detailed breakdown of identified risks, proposed cybersecurity architecture, and implementation roadmap.

3. Bonus (Optional): Simulated Risk Scenario Response
   - Outline how your proposed plan would address a specific attack (e.g., a coordinated demand spike initiated via compromised EV chargers).

Judging Criteria:
- Technical Depth (30%) – Clear understanding of grid operations, cyber threats, and defensive strategies.
- Practicality and Innovation (20%) – Feasibility of your recommendations and originality in solving complex problems and demonstrates understanding of relevant policies and compliance obligations.
- Communication and Presentation (20%) – Clear, concise, and compelling storytelling for both technical and executive audiences.
- Quality of Q&A (20%) – Clear, confident, and relevant responses to anticipated questions and demonstrates that preparedness.
- Overall Performance (10%) – How confident, composed, and effective communication are within the team. How team members engage together. The effectiveness of engagement towards the audience. The team can convey all pertinent information in a comprehensive manner.

Resources Provided to Participants:

- *Case study materials on major blackouts and cyber events (e.g., Ukraine 2015, Colonial Pipeline/Dragos).*

  https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

  https://www.dropbox.com/scl/fi/7quwk2eqwbllg044zv24y/Dragos_WP_TSA_SecurityDirective_2021-02C_Final.pdf?rlkey=ups6d5qkd9fi0sa027s6t97lw&st=o3fpa4hv&dl=0

- *Sample utility interconnection request forms for large loads.*

  https://www.dropbox.com/scl/fi/brtw6acgniqp28xxyroag/nc-interconnect-request-over-20kw.pdf?rlkey=nbzo0h7akys2a6c9e3kjav4im&st=v131ls9g&dl=0

- *NIST CSF v2.0 and NERC CIP v6 overview documents.*

https://www.dropbox.com/scl/fi/amp17zhtedq4wtyrw4vum/NIST.CSWP.29.pdf?rlkey=7cx0jtk6wioj6uq2dz7i90ciz&st=kl23kgz9&dl=0

- *NERC Critical Infrastructure Protection (CIP) standards*
  https://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx
- *News articles and technical whitepapers on data centers and EV fleet impacts on grid reliability.*

  https://www.ethree.com/what-is-the-deal-with-new-large-loads/

  https://www.esig.energy/engaging-with-large-loads/

  https://rmi.org/ev-loads-are-coming-heres-how-theyll-affect-the-grid/

Target Audience:
- Undergraduate and graduate students in cybersecurity, electrical engineering, energy policy, or business.