U.S. DEPARTMENT OF
ENERGY

Office of Electricity

North American Energy Resilience Model

July 2019

United States Department of Energy
Washington, DC 20585

EXECUTIVE SUMMARY

The Nation's energy resilience could benefit from national-scale energy planning and real-time situational awareness capabilities based on rigorous and quantitative assessment, prediction, and improvement. An ambitious effort led by the U.S. Department of Energy (DOE) — the North American Energy Resilience Model (NAERM) — will enhance this capability to ensure reliable and resilient[1,2] energy delivery across multiple energy sectors while considering a range of large-scale, emerging threats.[3] DOE will undergo this effort in support of its critical infrastructure protection responsibilities for the energy sector under Presidential Policy Directive-21.

A collaboration between DOE, its National Laboratories, and industry, the NAERM will develop a comprehensive resilience modeling system for the North American energy sector infrastructure, which includes the United States and interconnected portions of Canada and Mexico. The United States is increasingly experiencing threats, natural and man-made. The NAERM will enable prediction of the impact of threats, evaluation and identification of effective mitigation strategies, and support for black start planning,[4] benefiting the United States by enhancing energy and economic security.

The motivation for NAERM is not without precedent. A massive blackout in 1965 prompted proposed legislation calling for creation of a council on power coordination, ultimately leading to the formation of what is now the North American Electric Reliability Corporation (NERC) and an electric industry-standard definition of reliability. Analogously, DOE believes this to be a critical moment to address the resilience of our Nation's energy systems. NAERM is a potential solution, enabling systematic identification of threats to our energy infrastructure, development of hardening options that reduce our exposure to such threats, and situational awareness and sophisticated analytics to minimize the impact of threats as they evolve in real time.

The NAERM will advance existing capabilities to model, simulate, and assess the behavior of electric power systems, as well as associated dependencies on natural gas, and other critical energy infrastructures. Integration of significant expertise at the National Laboratories, plus data integration and collaboration from all stakeholders, will support threat characterization for the energy sector across varying geographic areas and supporting sectors. The NAERM effort will engage with industry experts to get a better understanding of issues and practices on a regional basis in order to ensure that threat and consequence models are realistic and representative of actual system responses.

---

[1] Resilient systems (versus reliable) anticipate, withstand, and recover critical loss-of-supply resulting from low-probability, high-impact threats.

[2] Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience (Feb. 12, 2013).

[3] For example, threats include natural disasters, coordinated cyber-physical attacks, and electromagnetic pulses due to nuclear detonation.

[4] A black start is the process of restoring electric grid to operation without relying on the external electric power transmission network and generators. The electric power used within the plant is provided from the station's own generators.

The NAERM will ultimately provide real-time situational awareness and analysis capabilities for emergency events for optimal operations and recovery, so that the Federal Government can quickly and effectively prepare and respond, for example, providing recommendations in coordination with State and local governments, Federal Emergency Management Agency (FEMA), and the National Guard. While the primary focus is on the energy sector, the NAERM will further assist industry in assessing the resilience implications of energy planning decisions on associated infrastructure. NAERM capabilities will also be leveraged by DOE's National Nuclear Security Administration (NNSA), the Department of Defense (DoD), and the Department of Homeland Security (DHS) in support of their national security missions.

The main phases of the NAERM will address (1) long-term energy planning; and (2) energy planning and operational studies with real-time data streams, national-level situational awareness for both infrastructure and threats, and analytic and decision support capabilities to anticipate threats and mitigate their impacts (Figure 1). Each phase of the NAERM will advance capabilities developed in the previous phase. By the end of the first phase, the NAERM is expected to have the capability of assessing the expected consequences from a range of scenarios. By the end of the second phase, the NAERM will be a situational awareness model capable of analyzing the power system, predicting potential threat consequences, and providing recommended mitigating actions to those consequences that can provide operate-through capabilities for a diverse array of threats. This model will be the foundation for analyzing the power system and its interdependencies with other infrastructures in real-time. The NAERM capability will be a first-of-its-kind globally and improve energy sector resilience for the well-being of our citizens and national security.

Figure 1: Roadmap of NAERM development phases

DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

NORTH AMERICAN ENERGY RESILIENCE MODEL

Table of Contents

Appendices

I. THE SITUATION

Our Nation's prominence is largely enabled by broad access to abundant, reliable, and affordable energy. Our modern electric power system drives our digital economy and elevates our health, safety, and overall standard of living. Without a functioning power grid, nearly every type of critical infrastructure in the U.S.—from banking and water distribution to telecommunications—would grind to a halt. Yet as our Nation's dependence on the power grid grows, so does the breadth and severity of threats against it.

Weather-related and other natural disasters, which are the dominant cause of high-consequence power outages, are projected to continue to increase in intensity and frequency.[5] The natural disasters of the past few years (including Superstorm Sandy, Hurricanes Katrina, Harvey, Maria, Irma, and most recently Michael) offer a sample of the adverse impacts on the well-being of our citizens. Hurricane Maria caused parts of Puerto Rico to be without full power for more than a year. Superstorm Sandy's impact was widely experienced by 24 states, totaling $72 billion USD in damage, and caused widespread outages to critical electrical and water services. Superstorm Sandy also resulted in 159 deaths and the closure of the New York Stock Exchange for two business days.[6] Such large economic impacts pose a significant financial and safety risk to the Nation.

Extreme events initiated by our Nation-state adversaries cause concern across our national security community. A 2018 report by the U.S. Director of National Intelligence (DNI) Dan Coats states that malware and related cyber threats directed at the power grid continue to evolve and grow.[7] In July of last year, DNI Coats noted the growing threat of cyberattacks on US infrastructure, noting: "The warning signs are there. The system is blinking." Nation-state adversaries, with knowledge of our infrastructure and a desire to maximize impacts, stand to exploit any potential vulnerabilities to achieve significantly greater and longer-lasting damage. And in his 2019 report, DNI Coats further articulated the increasing threat vectors directed at our critical energy infrastructure.[8]

While we must address known threats, including extreme weather and cyber, it is equally critical to focus on the next (unknown) "worst-case" threat—anticipating where our adversaries are directing their efforts. The anticipated threat space is evolving rapidly, from natural, economic, and malicious causes. Potential future threat scenarios range from natural or accidental events to coordinated cyber and physical attacks—for example, widespread attacks on control systems or infrastructure, detonation of nuclear weapons at

---

[5] https://www.climate.gov/news-features/blogs/beyond-data/2016-historic-year-billion-dollar-weather-and-climate-disasters-us

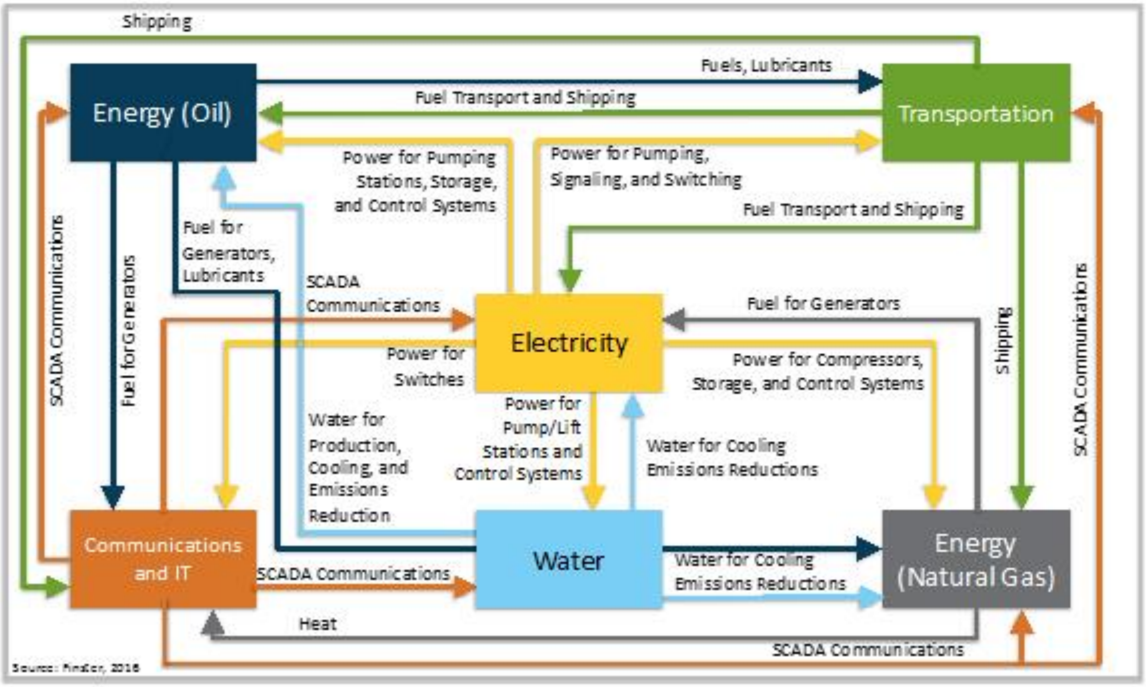
[6] NOAA National Centers for Environmental Information (NCEI) U.S. Billion-Dollar Weather and Climate Disasters (2018). https://www.ncdc.noaa.gov/billions/

[7] Worldwide Threat Assessment of the US Intelligence Community. Daniel R. Coats, Director of National Intelligence. February 13, 2018. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

[8] Worldwide Threat Assessment of the US Intelligence Community. Daniel R. Coats, Director of National Intelligence. January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

high altitude, and effects from directed energy weapons. This diversity of threats further emphasizes the urgency to understand energy infrastructure vulnerabilities and develop mitigation strategies to harden against and operate through such events. It is critical that we incorporate the best available information about how these threats will change over time, predict the likelihood of such events and their associated impacts as the power grid is operated, and recommend mitigation and recovery strategies in real time. The NAERM when fully completed over the next several years will incorporate real-time "next-worse-case" analysis and recommended operational actions.

Traditional solutions to alleviating constraints include expanding, upgrading, or rebuilding the electric infrastructure. While these long-lead-time solutions may be needed in the long term, new and innovative technologies such as dynamic line rating (DLR) may complement NAERM. DLR systems are one of many options for addressing grid constraints and adding system flexibility; other solutions such as power-flow controllers, energy storage, distributed energy resources, and demand response also play key roles in modernizing the grid. An additional benefit of implementing technologies such as DLR is increased situational awareness of the transmission system, the potential for condition-based monitoring of transmission lines, and the mitigation of potential threats.



Source: Finster, 2016

Figure 2: Electric grid dependencies on other infrastructures

The energy subsectors are more tightly coupled than ever, with local impacts cascading into other regions and sectors across the Nation. Furthermore, data streams are disparate and often not analyzed in an integrated framework. As a result, investments and responses from major stakeholders in both private and public sectors are guided by incomplete information. Specifically, we need to ensure reliability and resilience concurrently. Resilience is the ability to prepare for and adapt to changing conditions, and to withstand and recover rapidly from disruptions.[9] Whereas reliability focuses on assuring day-to-day grid operations—such as real-time balancing of load and generation, operating equipment within defined limits, adequate operator training, and tree trimming—in typical conditions, emerging areas of resilience concerns include cybersecurity and changes in the Nation's resource mix.[10]

Notwithstanding an ability to leverage and build upon national laboratory research capabilities developed under DOE programs such as the Grid Modernization Initiative (GMI) and Grid Modernization Laboratory Consortium (GMLC), advanced quantitative tools will help guide our Nation's energy planning for and operations during catastrophic events, particularly those that impact multi-sector infrastructures such as electricity and gas.

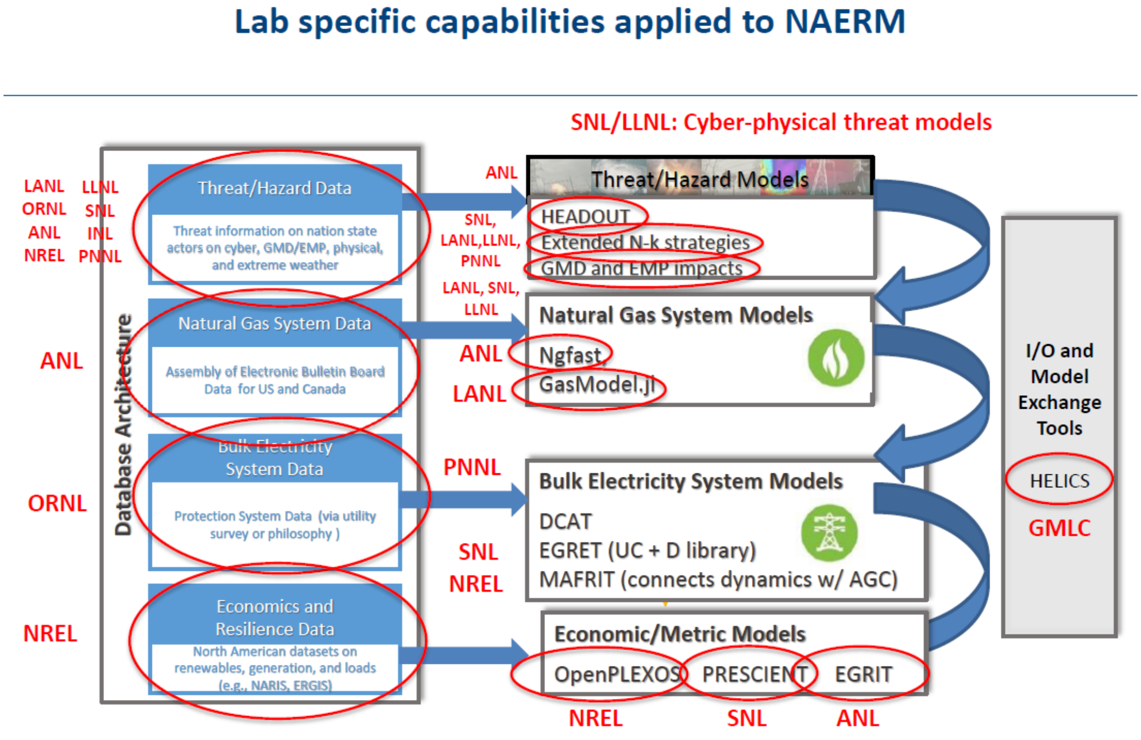


Figure 3: Leveraging and Building Upon National Laboratory Research Investments[11]

---

[9] *Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience* defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats of incidents."

[10] 2016. Federal Energy Regulatory Commission (FERC) Reliability Primer

[11] "LANL" – Los Alamos National Laboratory, "LLNL" – Lawrence Livermore National Laboratory, "ORNL" – Oak Ridge National Laboratory, "SNL" – Sandia National Laboratories, "ANL" – Argonne National Laboratory, "INL" – Idaho National Laboratory, "PNNL" – Pacific Northwest National Laboratory, "NREL" – National Renewable Energy Laboratory

Planning decisions today for the natural gas system consider the reliability implications for gas delivery, but do not always look at the resilience consequences for impacted energy sectors, such as electricity. Resilience for a combined set of critical infrastructures can be improved by looking at the systems and threats holistically, beyond just sector-by-sector assessments. Current investments for resilience are guided in a piece-wise manner and have generally been reactive. Stakeholders look at specific impacts after the fact, studying what went wrong and how to make corrections to avoid the specific event in the future—as opposed to employing state-of-the-art science and engineering modeling approaches to better understand the best strategy for joint-sector hazards ahead of time and in a proactive manner to avoid or limit the impact of the events when they happen. Additionally, cost recovery for resilience or cross-sector investment has not been enabled to realize this future.

Industry capabilities and access to system models, operational data, and domain expertise represent a critical foundation for the NAERM. Coupled models across multiple infrastructure sectors, such as electricity and gas for a single planning area (e.g., in the planning areas of regional transmission organizations PJM Interconnection LLC and ISO New England Inc.) are emerging; however, they are not widely adopted or mature, nor applied or available to the broader community. The success of NAERM is dependent upon the availability and integration of data and models across energy sectors and regions, capturing the inherent dependencies on associated infrastructure that often drive unforeseen consequences.

Improving our Nation's power grid resilience is presently limited by the lack of models and quantitative tools that fully integrate and analyze the interdependencies among energy infrastructure. Investing in the tools, models, and expertise across infrastructure sectors ensures increased preparedness for natural and adversarial events.

II. THE SOLUTION

The NAERM will help us transition from the current reactive state-of-practice to a new energy planning and operations paradigm in which we proactively anticipate damage to energy system equipment, predict associated outages and lack of service, and recommend optimal mitigation strategies. However, predicting the impact of a specific event on energy system operations, restoration, and recovery is vexing due to the scale of the North American energy system—crossing organizational, geographic, and sector boundaries—and the underlying physics of energy transport. Our current ability to analyze extreme events in this context is presently limited due to the lack of (1) unclassified details regarding potential threats, (2) data and predictions on resulting impacts, (3) tools required to model multiple infrastructures, (4) expertise in characterizing and analyzing the relationships between energy and associated infrastructures, and (5) details concerning the coordination and interdependencies of numerous utilities and stakeholders involved in regional and national-scale energy system operations.

The NAERM will provide answers to questions for power grid planning and operations, including the following:

- What is the next best investment that will yield contributions to national security?
- How can we improve electric and gas sector resilience to a wide range of threats?
- What are the impacts and cost-benefit trade-offs of different mitigation plans?
- Can we recommend optimal mitigation strategies to stave off large-scale system damage in real time?

Answers to these questions pose a particular challenge due to the rapidly changing threat space and our ever-evolving energy infrastructure. There is also a critical need to define and analyze resilience for different sectors under disparate threats, such as the ability to carry through normal operations given a relatively low impact event versus enabling critical government and military functions to carry through extreme events. The ability of system-hardening investments to mitigate the impact of extreme events can be limited to direct experience, qualitative investment portfolio comparisons, and analysis of traditional reliability metrics. These approaches can be improved through cross-sector analysis, adoption of standardized resilience metrics, and extended value-of-loss-load metrics, which is varied across end consumers in each of the 16 critical infrastructure sectors.[12] Such advances will provide rigorous and quantitative comparisons of alternative system investment strategies, and coupled resilience-reliability analyses will provide crucial system investment cost justification.

The NAERM is focused on providing advanced analytic tools to address the impacts of both natural (such as hurricanes and flooding) and man-made threats (such as cyber-attacks, combined cyber-physical assaults, and electromagnetic pulses) to our Nation's energy infrastructure. With NAERM, DOE will be able to:

- Integrate, to the extent practicable, Intelligence Community information to enable comprehensive and in-depth understanding of the impact of threats to the Nation's energy supply;
- Assist the U.S. Government and industry in identifying critical energy system vulnerabilities and associated dependencies on other infrastructure;
- Rigorously and quantitatively evaluate technology solutions to improve resilience;
- Utilize artificial intelligence and machine-to-machine capabilities (M2M) to optimize the utilization and security of the energy sector;
- Advise on approaches to mitigate threats, and operate through regional- and national-scale disaster events;
- Increase the likelihood of providing energy services to critical defense facilities during times of crisis;
- Advance the state-of-science of energy system resilience planning and operations; and,
- Utilize situational awareness capability throughout the entire energy infrastructure enabling response to extreme events.

---

[12] The 16 Critical Infrastructure Sectors as defined by DHS: https://www.dhs.gov/cisa/critical-infrastructure-sectors

NAERM will provide engineering-centric guidance essential for evaluating tradeoffs with other energy infrastructure attributes, such as cost and resilience. NAERM will advise on the tradeoffs of different recovery strategies with a unique and differentiating continental and cross-sector focus. NAERM will enable new market approaches for resilience investments that are not being valued today. Additionally, NAERM will provide validation of power-system models and analytical tools in support of secure and effective market operations.

Ultimately, NAERM will enable DOE's provision of situational assessment advice to industry and government to ameliorate the risk of and consequence associated with large-scale service disruptions across infrastructure sectors—and geographic and organizational boundaries—and the lengthy restoration and recovery operations following an extreme event. The NAERM will advance the state-of-science in planning and operations of energy supply in extreme events and provide rigorous resilience and associated economics metrics for these sectors.

III. NAERM STRATEGY

NAERM system development will be organized in two phases. Each phase represents substantial improvements in modeling capability, frequency of model updates, and number of infrastructures supported. Given the complexity of the system's development, risks in acquiring data, and current lack of technology to model multiple infrastructure simultaneously, development will be conducted using agile methods to produce system product implementations. The timelines for each of these phases will be defined via additional planning and technical progress. Note that overlap of work across phases is expected.

The description of the phases follows:

- Phase 1—Long-term Energy Planning with Offline Data: Establish baseline off-line planning capability for bulk electric and gas transmission systems. Includes procuring and adapting DOE, vendor, and open source modeling software packages. Incorporates DOE tools to couple energy infrastructure models. Develop initial integrated analysis environment. Secure agreements to obtain up-to-date detailed planning model databases for interconnects and selected stakeholders (e.g., NERC and independent system operators (ISOs)). Start development of economics and metrics required for cost-benefits analyses. Analyze requirements and start development of energy sector operational communications models. Develop methods to characterize threats for input into NAERM system.

- Phase 2— Situational Awareness and Operational Energy Planning with Streaming Data: Enhance energy planning modeling to enable vulnerability analysis with real-time data feeds. Develop complex multi-infrastructure contingency analysis providing day-ahead snapshots of the National resilience posture. Expand partnerships for sharing data with utilities and ISOs regarding external out-of-band sources (e.g., Phasor Measurement Units located at critical facilities). Harden and integrate research innovations in advanced analytics to rapidly identify system vulnerabilities and enhance decision support for system analysis.

The NAERM is envisioned as a public-private partnership with multiple stakeholders. NAERM tools will be used by the National Laboratories in conjunction with utility and other energy sector partners to conduct regional and national scale resilience analyses. Similarly, NAERM will provide DOE, Federal Government partners, and private industry with extreme event planning and ultimately operational capabilities, by identifying the most promising avenues for asset hardening and strategizing risk mitigation for potential threats with industry and government support functions. In conjunction with threat models, NAERM tools will provide significant value-add to utilities, enabling them to develop energy plans that concurrently address power grid reliability and resilience. Measuring economic risk and impact with defined resilience metrics can enable comparison of investment strategies and enable cost recovery, especially in identified cross-sector risks. Finally, DHS, DOE/NNSA, and DoD will be able to leverage NAERM capabilities in support of their missions, dependent upon coordination with the private energy sector asset owners who supply their respective energy needs.

The NAERM is a significant undertaking, in terms of labor, program management, and—most importantly—modeling and computing. Defensible modeling results are dependent on extensive sources of industrial data, including infrastructure consequences of historical events for purposes of verification and validation of NAERM models. Varying levels of sensitivity surrounding specific data sources necessitate a significant effort to firewall and appropriately protect the various data sources. Particular effort will be required to ensure that aggregated data and results are maintained at the appropriate classification level.

Continental, national, and regional-scale analyses generally require significant computational power, in the form of high-performance computing architectures and advanced parallel algorithms and solvers. Because disparate tools from the National Laboratories and industry will be integrated under the NAERM, the team must deploy and operate in a collaborative development and testing environment. Due to the criticality of decisions based on the NAERM, rigorous and commercial-grade regression testing and validation environments must be procured and leveraged. Finally, NAERM capabilities themselves must be replicated and possibly decentralized across the DOE and National Laboratories complex, to ensure the operate-through ability of NAERM itself. A successful NAERM will survive well beyond the proposed development phases, such that a centralized maintenance and operations strategy will be necessary for sustained impact. NAERM will also serve in the long term as a platform through which advanced analytic capabilities for energy security analysis developed by the National Laboratories and industry will be deployed.

The NAERM has been designed to mitigate risks to accomplish the NAERM objectives of enabling national energy systems planning and operations resilience. Unforeseen difficulties due to the innovative nature of this undertaking could impact cost and schedule. Additionally, success of the NAERM rests largely and critically on the collaboration with industry to build upon their specific area knowledge and situational energy system data. The inability to secure and integrate data from industry to both populate national-scale energy systems models and analyze the grid using real-time data streams is the single biggest risk for NAERM, due to the proprietary nature of much of the source data and classified nature of significant portions of the threat data. A significant portion of the first phase of NAERM will be devoted to mitigating this effort, through close coordination between the Office of Electricity, the National Laboratories, and utility stakeholders. The final deliverable of the NAERM requires advanced computational capabilities and massive data-processing efforts, and the risks in these dimensions is increased as NAERM development proceeds. Therefore, DOE will be conducting extensive industry engagement to ensure that the NAERM will be built on the Nation’s best expertise and housed in secure computing environments to comply with cybersecurity requirements of critical energy infrastructure, market sensitivity, and national security data.

IV. EXPECTED OUTCOMES

NAERM will serve as a critical “what-if” machine to help the Nation answer vexing questions to best protect our energy infrastructure. The potential consequences of not addressing well-known and well-documented threat vectors are enormous, resulting in severe societal impact and wasting money on ineffective solutions. Witness the intense debates around how to address threats, such as high-altitude nuclear weapons detonations, cyber-attacks, and large-scale weather events. The arguments for various solutions are built upon uninformed conjecture and incomplete analysis. NAERM arms the Nation to address such debates with the best science and engineering information.

NAERM is a complex technological endeavor. To assist the reader in better understanding the intent and key questions addressed, we have provided three use cases in Appendix A. These provide a vision for how NAERM would be used in future scenarios to improve our Nation’s resilience. Summarizing, these use cases address how we would use NAERM to prevent the next large-scale blackout, understand dependencies between electric and gas infrastructure, and provide economic justifications for procurement for spinning reserves that support both “blue sky” standard operations and “black sky” catastrophic events. These provide insight into specific outcomes that we believe will be achievable through NAERM.

With the NAERM in place, DOE will be able to quickly and effectively prepare and respond to natural and adversarial events to ensure reliable and resilient energy delivery across the Nation—for example, providing recommendations in coordination with state, tribal, and local governments, FEMA, and the National Guard.

APPENDIX A

NAERM MODELING CASES

To help the reader understand how NAERM could be used to benefit the Nation, three examples (or cases) are provided in this appendix section. Each of these describes an important challenge facing our Nation's energy infrastructure and how DOE envisions NAERM to be used to provide solutions. Once the NAERM system is built, we see these use cases as a subset of the many problems this system can address, specifically by tackling important resilience challenges through modeling and analytics.

A.1. Preventing the Next Major Blackout in the Bulk Electric System

On August 14, 2003, an estimated 50 million people in the Midwest and Northeast experienced a major blackout. The economic impact has been estimated at over $6 billion.[13] On September 8, 2011, an estimated 2.7 million people in the Pacific Southwest lost power, with an estimated economic impact of over $100 million.[14] In both cases, task forces comprised of industry experts investigated the root causes of the blackouts and provided findings and recommendations on how to prevent them in the future. Based on the report findings, industry has taken corrective actions to address these issues.

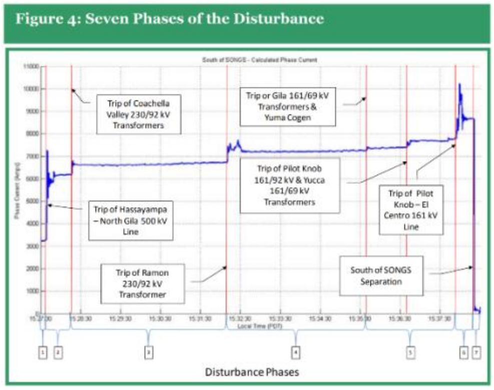
Both blackouts were caused by completely different initiating events, the first by a transmission line contacting a tree due to poor vegetation management and one a switching error caused by lack of system visibility. But the 2012 *FERC/NERC Staff Report on the September 8, 2011 Blackout* identified primary causes that were common between the two blackouts and were independent of the initiating events:

---

[13] "Transforming the Grid to Revolutionize Electric Power in North America," Bill Parks, U.S. Department of Energy, Edison Electric Institute's Fall 2003 Transmission, Distribution and Metering Conference, October 13, 2003.

[14] "San Diego Blackout Economic Impact (September 2011)," National University System Institute for Policy Research, Sept. 9, 2011.

1. *Inadequate Long-Term and Operations Planning* – The reports found that several entities had not properly conducted long-term and operational planning studies to fully understand vulnerabilities and their implications, particularly when related to information regarding neighboring facilities, contingencies, system models, and system operating limits.
2. *Inadequate Situational Awareness* – Operators had limited real-time visibility outside their own systems and did not fully understand how contingencies within their own system might affect their neighbors' systems.
3. *Protection Systems* – While not directly causing the outages, protection system settings impacted the scale of the cascading outage and reduced the operators' window to take mitigating actions.



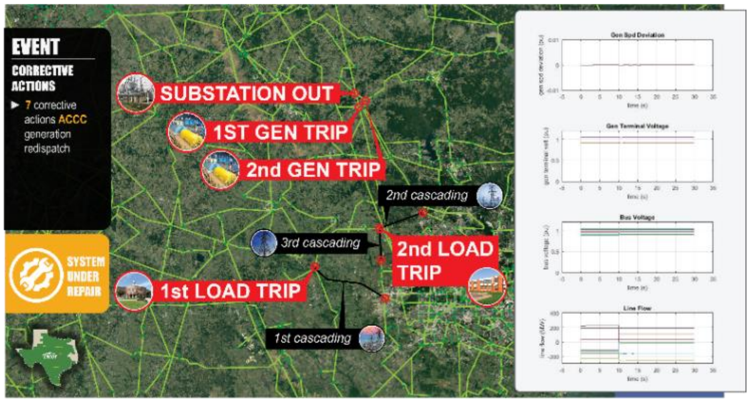
Seven phases of the 2011 Southwest Blackout. Image extracted from Ref [1].

The industry has taken several corrective actions based on the recommendations of the April 2003 report, so it should not be assumed that the industry is not responsive. However, threats are ever changing and reactive procedures were not adequate to avoid additional blackouts, nor were they proactive in identifying new risks. Additional corrective actions were put in place to address the challenges associated with the 2011 blackout, such as increased information and model sharing. However, the main root cause persists: utilities operate separately from each other and neither have nor are required to have the resources to study the impacts of the changes from external networks on their systems. This was a contributing factor in both blackouts, which in turn caused billions of dollars in damages and lost production.

But should we continue to look in the rearview mirror and address these challenges after a major blackout occurs, or can we extend our capabilities and look into the future to predict and mitigate these challenges before they occur? Can we prevent the next $6 billion outage by proactively investing a fraction of this amount, e.g., $100M, to harden critical components? Can a national data and modeling environment provide the global visibility and analysis capabilities necessary to prevent the next major blackout, or least minimize its impact? Do we even know what the next big event might look like and therefore plan for it?

By developing a comprehensive model for the North American energy system, the NAERM and associated tools will be able to study the impact to the entire electric grid when changes are made within an operating entity. This will help the Nation identify *hidden* failures that cannot be identified with the current models, tools, collections of data, and practices, and move us toward a *predictive* capability to prevent or minimize system outages, potentially saving the Nation billions of dollars.

This effort includes collecting and curating industry model data, developing software analysis tools and capabilities, and exercising these capabilities to address questions of national importance. It will model dependencies on critical supporting infrastructures, cascading failure possibilities resulting from extreme events, and other issues of national-scale importance that are associated with national security resilience issues that are above and beyond the current purview and capabilities of industry to address on their own.



DCAT Contingency Analysis Tools

To demonstrate these capabilities, use cases can be constructed to both evaluate the software systems developed and exercise the ability of the models to predict outages. The 2011 Southwest Blackout could be used as a validation case to determine whether the tools can predict an outage, not just replicating it. For example, in after-action modeling and simulation efforts, the causal issues are "scripted" into the simulation to represent what has already happened in reality, sometimes requiring weeks or months to replicate the events. An example use case of a fictional cascading outage in the Electric Reliability Council of Texas (ERCOT) using a lab-developed tool, DCAT, is shown. If successful, the developed tools, along with the requisite system data, will be used to automatically predict outages, allowing stakeholders to identify and quantify the risks associated with large-scale outages and mitigate them before they occur.

A.2. UNDERSTANDING ENERGY COUPLING OF GAS AND ELECTRIC INFRASTRUCTURES

The increasing coupling of the natural gas and electric infrastructure has resulted in new operational and energy planning reliability challenges.[15] Gas-dependent electrical generators can simultaneously experience outages during gas supply disruptions caused by extreme events, such as polar vortexes, hurricanes, and earthquakes.

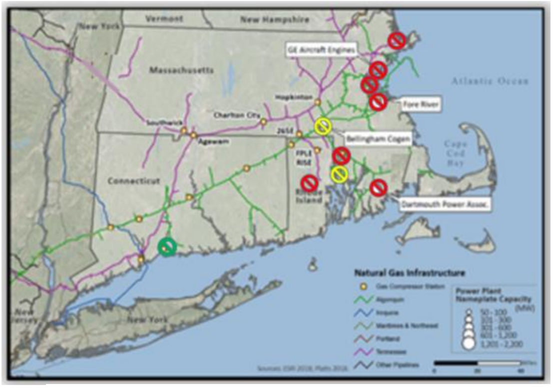
For example, New England experiences significant cold fronts immediately after nor'easters during winter periods when gas consumption for home and commercial heating is at seasonal highs, leaving limited gas reserve capacity for gas-fired electricity generation.

---

[15] For further example on operational and energy planning reliability challenges, see PJM's Grid 20/20: Focus on Resilience (Fuel Mix Diversity & Security), April 19, 2017 ("April 2017 Grid 20/20"), https://web.archive.org/web/20180810192335/http:/pjm.com/committees-and-groups/stakeholder-meetings/symposiums-forums/grid-2020-focus-on-resilience-part-1-fuel-mix-diversity-and-security.aspx

When a failure on the natural gas system, such as a pipeline breach or explosion, occurs under these conditions, system pressure begins to drop, forcing the pipeline operator to issue stop orders to gas-fired generators. Gas supply impacts to each gas-fired generator will vary depending on the nature (firm or interruptible) their contract and their operating status at the time of the gas supply disruption. Some generators will be shut down completely, while others may be put on a hold at current levels and unable to ramp up generation. Idle gas-fired generators will remain idle.

In this use case, as the gas supply decreases, electric utilities throughout the Eastern Interconnection on the eastern end of the pipeline and ERCOT on the western end of the pipeline will be searching to obtain alternate sources of fuel for their gas-fired generators. If liquefied natural gas and other storage facilities are inadequate to fill the need due to limited supplies, pipeline constraints, or limited capacity on other pipelines, the Eastern Interconnect and ERCOT will bring their spinning reserves, a type of reserve provided by online generating resources that can react by providing more or less power to system needs within a short period of time (within 10 seconds and up to 10 minutes), online to replace generation lost due to limited gas supply. If the spinning reserves are not sufficient, rolling blackouts will commence.



Identification of impacts to gas-fired generators

Weather in either or both the ERCOT service area and the Eastern Interconnection may create an unexpected correlated failure despite being loosely coupled at the power grid level (separate interconnections). Generation losses due to loss of gas supply or another bulk electric system (BES) contingency may lead to additional impacts on natural gas pipeline generators who operate processing plants or compressor stations powered by electricity. An iterative, coupled natural gas-BES modeling approach will close on the gas supply impacts and electrical outages.

NAERM, by developing a comprehensive model for North America, will be able to study the impact of disruption of gas supply to multiple utilities at the same time on the entire electric grid and the impact of lost generation on the natural gas supply. This will provide the ability to identify vulnerabilities that could not be identified with the current models, tools, and practices. Identifying and mitigating the vulnerabilities in the coupled natural gas and electric power systems to prevent blackouts is only one of the objectives of NAERM. On real time scales, NAERM will analyze the current gas and electric operating conditions and produce a list of gas components whose failure would have the biggest impact. In this example, NAERM can identify the described pipeline failure as high risk during congested conditions and allow stakeholders to pre-position the power system to survive such a gas disruption (*i.e.* procure non-gas reserves).

A.3. PREPARING FOR EXTREME EVENTS - JUSTIFYING AND IMPROVING ELECTRIC GENERATION RESERVE MANAGEMENT

The balance between adequate electricity power quality and delivery is delicate—constant adjustments, such as spinning reserves, are required to maintain good power quality and reliable service. Traditionally, generators that are online and partially loaded are used to provide spinning reserves. When needed, the generator can increase or decrease power output. There is a cost to reserving a generator for spinning reserves, as it is not operating at its most economical dispatch point and loses opportunity to be compensated for providing energy at its maximum capability. Further, as uncertainty associated with system components (*e.g.*, renewables) and potential damage (*e.g.*, due to extreme weather events) increases, the quantity and cost of spinning reserves increases.

An alternative way to provide spinning reserve is using energy storage, including devices such as batteries, fuel cells, capacitors, and flywheels. The value of energy storage comes from responding within milliseconds or minutes to system needs, and the ability of storage to respond faster than generators can buy time for an offline and less costly generator to come online. This approach will contribute to less cost and generator emissions as resources are called on when needed, instead of idling generators, freeing up generators to run at full capacity and produce more electricity.

By characterizing threats—both natural and adversarial—to the Nation's energy supply and predicting their potential consequences, the NAERM system will be able to study and identify the adequate level of reserve needed, and, as a result significantly reduce the quantity of spinning reserves required to operate the system in nominal (*e.g.*, reliability) conditions, and further provide rigorous analytic guidance concerning the type and quantity of reserves necessary to enhance the resilience of the Nation's electricity supply. As a result, reliability will be enhanced—with costs reduced during nominal operations. Further, the ability to rigorously guide reserve procurement strategies to mitigate the impacts of extreme events will provide a first-of-kind capability for electricity system operators, which are presently struggling with strategies for addressing resilience in the course of operations.

Appendix B provides additional detail on how this system is expected to be used. DOE expects that these details will evolve and be refined with additional planning and technical analysis.

APPENDIX B

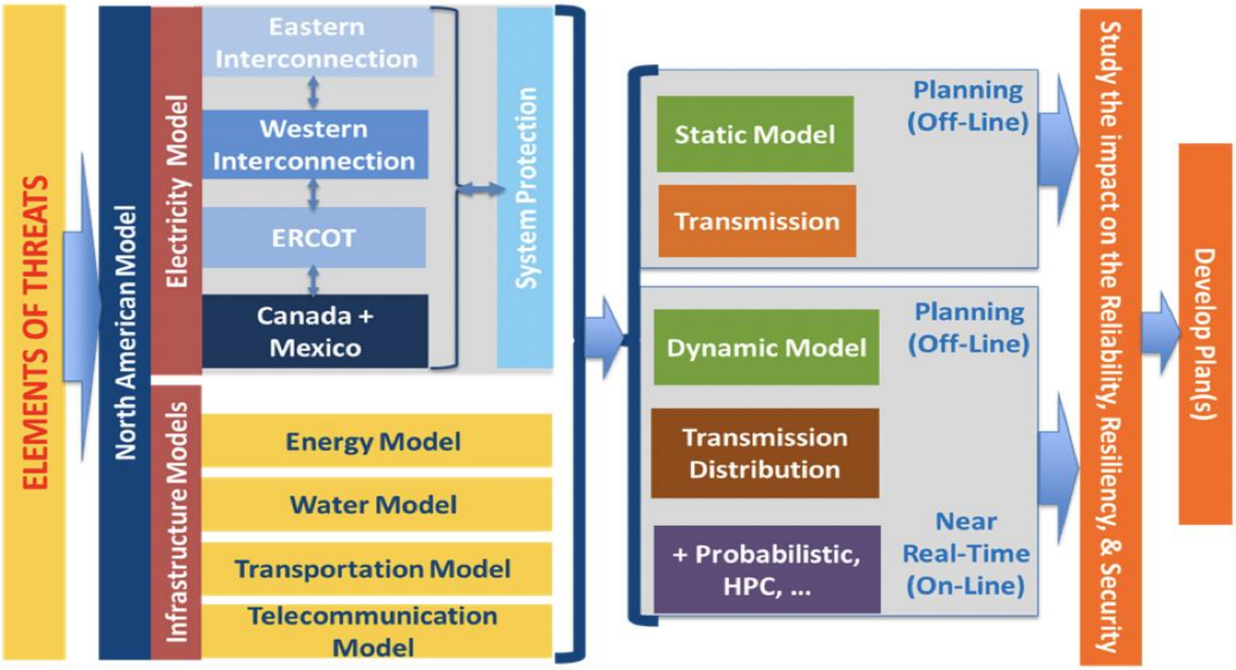


Figure 3. NAERM Workflow Concept

CONCEPT OF OPERATIONS

NAERM could be used by either an individual or a team of subject matter experts to assess the impact of threats to energy infrastructure. A typical scenario might involve a request by DOE leadership to analyze the impact of an important threat event or multiple hazards. Analysts would characterize the threat and then use NAERM to exercise the infrastructure models through various damage scenarios. NAERM would be used to help provide answers to questions regarding extent of outages, damage to equipment, benefits of specific engineering solutions, and improvements to operational playbooks. Figure 3 is a graphical representation of the workflow for how an analyst could potentially use NAERM. Note that this scenario represents just one example of an initial capability. As noted in the body of the report, the NAERM system will be far more flexible and powerful, with a long-term vision of being able to handle multiple infrastructures, identify weaknesses, and recommend courses of action.