A Description of PJM's Work Under Phase 3 of the PJM Fuel Security Analysis: Summary of Current Discussions with the U.S. Department of Energy and Requested Analyses – PUBLIC VERSION[1]

Executive Summary

In April 2018, PJM Interconnection announced that it would begin to study an important aspect of resilience: fuel security. That effort has been broken into three phases. In Phase 1, PJM has identified assumptions and inputs to create credible fuel security risk scenarios, which it will then simulate and analyze. In Phase 2, PJM will work with stakeholders to identify solutions to any material risks identified in Phase 1. For Phase 3, PJM has consulted with federal agencies to define a set of scenarios based on restricted information about credible risks to the fuel supply chain that could have impacts on the bulk electric system. Information gathering for Phase 3 has been taking place concurrently with Phase 1. The analysis of these scenarios will take place after Phase 2 is complete.

While much of the information was given to PJM in classified meetings, this document provides a public version of the summary of the risk scenarios provided by federal agencies. The scenarios supported by information provided by federal agencies are separate from the PJM-identified fuel security scenarios.

Introduction

In PJM Interconnection's original document outlining its fuel security analysis,[2] "Valuing Fuel Security," released on April 30, 2018, PJM indicated that it would reserve the review and coordination of certain results with specific security scenarios to Phase 3 of its analysis. More specifically, Phase 3 would feature the results of scenarios identified by various federal agencies, including the U.S. Department of Energy (DOE) and U.S. Department of Homeland Security (DHS), as well as the Federal Energy Regulatory Commission (FERC).

PJM intentionally separated this set of federally advised analyses into a separate phase in order to clearly differentiate between resilience challenges specific to the PJM region that PJM identified based on its knowledge of system conditions, and those identified by relevant federal agencies. Although this federal agency input is separate from PJM's own identification of contingencies, this separation does not necessarily mean that work cannot occur in parallel with the other analysis as identified in "Valuing Fuel Security."

[1] A confidential version of this paper will be provided to those entities owning and operating critical fuel supply chain infrastructure, such as natural gas pipelines, provided that the individual entity has signed a nondisclosure agreement with PJM to allow for the exchange of reliability-based confidential information.

[2] This paper can be accessed at http://www.pjm.com/-/media/library/reports-notices/special-reports/2018/20180430-valuing-fuel-security.ashx.

As part of its preliminary work under Phase 3, PJM contacted the DOE to obtain DOE's input concerning cyber or physical risks that could result in service impacts or delivery disruptions to fuel supply infrastructure that may have a potential "downstream" impact to the bulk electric grid.[3]

PJM met with DOE subject matter experts in July 2018 to better understand these risks. The meeting focused on cyber and physical threat actors to provide greater insight into the capabilities and potential attack vectors used by foreign and domestic adversaries and the challenges to U.S. critical infrastructure based on classified information available to the federal government.

The information from the DOE meeting is a key input into Phase 3 of PJM's fuel security study to analyze a range of risk scenarios and determine the potential impact on PJM's ability to continue to provide reliable electricity in the PJM service territory.

In Phase 3, the impacts of these scenarios will be analyzed using estimates of duration and scale (based on the number of companies/pipelines or the amount of cyber or physical infrastructure) informed by input from the pipeline industry. PJM will be seeking input from the pipelines on duration and scale of impact.

Background: Types of Threat Actors and Risk

The types of threat actors have been generally identified as falling into three primary "classes" that may pose risks to fuel supply infrastructure:

1) Nation-State Actors. Nation-State Actors work for a government to disrupt or compromise target governments, organizations or individuals to gain access to valuable data or intelligence and can create incidents that have international significance. Nation-State Actors often have close links to the military, intelligence or state control apparatus of their country, and a high degree of technical expertise.

   A Nation-State Actor would have the resources and capabilities of their government behind them and take instruction from other government employees or members of the armed forces. They also influence other suspects, introducing new tools, insights, tactics and attacks that are copied by others.[4]

   There is significant open-source intelligence to indicate persistent cyber reconnaissance and presence of these actors in U.S. critical infrastructure sectors. Their motivations are largely geopolitical in nature, indicating that while they possess high levels of capability, they are less likely to perform attacks due to the political and military ramifications of doing so.

[3] Additional discussion with DOE in this area is ongoing so that PJM may receive federally advised scenarios on other fuel supply-chain risks such as those involving fuel oil, coal and other supply sources.

[4] https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor

2) Non-State Threat Actors. Non-State Threat Actors, including terrorist organizations, have the ability to operate in cells and coordinate attacks at multiple locations for ideological or political goals. They have a demonstrated physical attack capability to destroy infrastructure and a more limited cyber capability primarily used for financial or ideological gain.

   Non-State Threat Actors are rarely backed by formal government financial or material support and as a result have lower levels of skill and capability than Nation-State Actors do. The likely impact of their actions is significant, although not as extensive as Nation-State Actors, and the likelihood of Non-State Threat Actors to execute an attack is higher due to their motivations.

3) Lone Wolf Actors. A Lone Wolf Actor is someone who prepares and commits violent acts alone, outside of any command structure and without material assistance from any group. He or she may be influenced or motivated by the ideology and beliefs of an external group and may act in support of such a group.

   The capabilities and resources used by a Lone Wolf Actor to execute a physical or cyberattack are much more limited than in the previous two categories of threat actors, making attacks from Lone Wolf Actors far less likely to result in a significant impact. However, their independence of operation makes a lone wolf attack more likely to occur.

In order to develop credible risk scenarios, each of the three primary threat actors needs to be aligned with known or anticipated tactics and capabilities. A plausible sensitivity analysis requires establishing a range of impacts to create upper and lower boundaries of both scale and duration, in order to avoid single-use case events that make it more difficult to reach conclusions.

For the purposes of this analysis, PJM sought from the DOE only the impacts that would challenge the resilience of the electric system and the critical fuel supply chains on which the electric system is dependent (i.e., impacts whose scale and/or duration would be significant).

When considering the spectrum of risk using this lens, there are three types of attacks that fall into this category and three that, arguably, do not. An explanation is provided below for those scenarios PJM considers out of scope.

	Nation-State	Non-State	Lone Wolf
Cyber	Credible Risk (In Scope)	Credible Risk (In Scope)	Out of Scope
Physical	Out of Scope	Credible Risk (In Scope)	Out of Scope

It is generally understood that a nation-state physical attack is entirely capable of producing a resilience-scale impact; however, the circumstances that would bring about this event (e.g., a nation-state conducting physical attacks on U.S. critical infrastructure) are consistent with open warfare, and the national security implications of such a situation are beyond the scope of this document.

Lone Wolf Actors' comparative lack of resources and sophistication are likely to produce impacts that fall within the capability of infrastructure operators to recover using current operating procedures, including contingency analysis.

Details of Phase 3 Analysis

PJM's Phase 3 analysis, supported by information provided by the DOE, is focusing on the attack categories capable of producing system impacts that extend well beyond local geography and single infrastructure systems. It is important to note, however, that under the PJM analysis, the specific driver or cause of the service interruption is not crucial. Rather, PJM's analysis will focus on the ability of the system to withstand outages of extended duration irrespective of their cause.

The scenarios informed by PJM's DOE discussions are described below. As part of the public version of this document,[5] the following scenarios are described in broad terms. In the confidential version of this document, to be shared with the specific infrastructure owners being analyzed, additional information on potential scale and impact is provided.

As part of its Phase 3 analyses, PJM will seek information from the gas pipeline industry on the potential duration and impact on delivery of natural gas to generators should one of these events occur.[6] Moreover, since some of the DOE-advised scenarios involve the potential for cyberattacks on fuel suppliers, PJM's Phase 3 work, although starting with a focus on natural gas pipeline infrastructure, will also seek to address the impact of these wide-scale risks on other suppliers in the fuel supply chain. Although some of the specifics outlined below are focused on pipeline infrastructure, this should not be read as excluding analysis of other fuel supply chains for non-gas-fired resources.

Phase 3 Scenarios

1) Nation-State Large-Scale Cyberattack: Cyberattack (Nation-State Actor)

   - The duration is driven by the length of time needed to address the impact of the attack.
   - Information is being sought from pipelines and generators on the potential impact of such an attack on the continued ability of the pipeline to deliver gas to generation on their system.
   - Information is broken down separately as: generators with firm service, generators with a primary delivery point purchased from a holder of capacity in the secondary market, and generators with IT service.

2) Nation-State Small-Scale Cyberattack: Cyberattack (Nation-State Actor)

[5] See Footnote 1.

[6] The specifics of the request and the pipeline response will be treated as classified information and will not be publicly released given the nature and expected detail of the information provided.

- Under this scenario, the focus will be on damage to critical infrastructure needed to ensure system pressure and safety.
- The duration is determined by the speed/efficiency of manual pipeline operation, as well as the number/extent of damaged pipeline components and the availability of replacements and the time needed to complete repairs.
- Information is sought from pipelines and generators on the potential impact of such an attack on the continued ability of the pipeline to deliver gas to generation on their system.
- Information is broken down separately as: generators with firm service, generators with a primary delivery point purchased from a holder of capacity in the secondary market, and generators with IT service.

3) Non-State Threat Actor Physical Attack: Physical damage to critical infrastructure needed to ensure system pressure and safety including electronic valves, compressor stations, motors and similar components (Non-State Threat Actor)
   - The duration is dependent on the time needed to repair or bypass the damaged pipeline infrastructure.
   - Information is sought from pipelines and generators on the potential impact of such an attack on the continued ability of the pipeline to deliver gas to generation on their system upstream and downstream of the break.
   - Information is broken down separately as: generators with firm service, generators with a primary delivery point purchased from a holder of capacity in the secondary market, and generators with IT service.
4) Non-State Threat Actor Cyberattack: A cyberattack that affects control systems and corporate networks (Non-State Threat Actor)
   - The duration is tied to the ability to operate the affected pipelines manually and the speed of cyber remediation.
   - Information is sought from pipelines and generators on the potential impact of such an attack on the continued ability of the pipeline to deliver gas to generation on their system.
   - Information is broken down separately as: generators with firm service, generators with a primary delivery point purchased from a holder of capacity in the secondary market, and generators with IT service.
5) Nation-State Focused Cyberattack: A cyberattack that could involve damage to equipment critical to maintaining pressure on targeted pipelines (Nation-State Actor)
   - Repairs are likely to be more extensive, and IT recovery from a persistent attack is longer.

- Information is sought from pipelines and generators on the potential impact of such an attack on the continued ability of the pipeline to deliver gas to generation on their system.
- Information is broken down separately as: generators with firm service, generators with a primary delivery point purchased from a holder of capacity in the secondary market, and generators with IT service.

PJM looks forward to working with DOE and other federal agencies, as well as the gas pipeline industry and other fuel suppliers, in order to analyze these DOE-advised scenarios as part of Phase 3 of PJM's fuel security analysis.