SONECON

VALUING FUEL SECURITY: RECOMMENDATIONS ON STUDY SCOPE AND SIMULATED DISRUPTIONS

Paul Stockton
June 8, 2018

PJM's study on *Valuing Fuel Security* is timely and urgently needed. PJM and its member companies serve many thousands of facilities vital for national defense, the U.S. economy, and public health and safety. That makes the region's grid – and the fuel supplies on which it depends – potential targets for cyber and physical attacks.

The study provides a strong foundation to assess these threats to fuel supplies. In an April 30, 2018 message outlining the study, PJM President and CEO Andrew L. Ott noted that the study will "simulate disruptions to fuel systems that could be the result of credible extreme events such as coordinated physical or cyber-attacks, extreme weather, etc."[1] Developing weather contingencies to study will be easy; ample historical data is available to help do so. No equivalent basis exists for developing contingencies for cyber or physical attacks. Moreover, as PJM has previously emphasized, RTOs face obstacles in acquiring the government data they need to assess cyber threats.[2]

But it would be a grave mistake to do what is easy and focus the study solely on extreme weather. Coordinated cyber or physical attacks can create fuel disruptions far more catastrophic that those caused by the 2018 bomb cyclone or any other severe weather events to date. The Department of Energy (DOE) warns that cyber threats are becoming increasingly severe, and that the risks of physical attacks on natural gas systems merit special concern.[3] PJM is making a unique (and uniquely valuable) contribution to national security and grid resilience by structuring the study to encompass manmade threats.

This letter offers three recommendations to support the study. First, to support Phase I of the study, I propose specific disruption scenarios for the study to employ. It is not credible that a potential adversary such as Russia or China will attack a single pipeline and/or storage facility. If those nations are going to strike the U.S. energy sector, and risk incurring an overwhelming military response, they are much more likely to attack as many pipelines and/or storage facilities

[1] Andrew L. Ott (letter to PJM Members), April 30, 2018, http://www.pjm.com/-/media/committees-groups/committees/mrc/20180508-special/20180508-ott-fuel-security-member-letter.ashx.
[2] PJM Interconnection, L.L.C, "COMMENTS AND RESPONSES OF PJM INTERCONNECTION, L.L.C.," *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators* (AD18-7-000), March 9, 2018, p. 52.
[3] Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*, March 2018, p. 3.

as possible to disrupt the flow of power to defense installations and other national security-related assets. Nor is it credible that disruptions caused by manmade threats will last 14 days or less. If adversaries conduct coordinated high explosive attacks against critical gas infrastructure, many months could be required to repair pipelines and restore the flow of gas. Consistent with the study's proposed structure, PJM should use two disruption scenarios to assess manmade risks to fuel security:

- Reduction of a realistic percentage of delivery capability on particular constrained portions of pipelines and disruption of storage facilities in the PJM region: assume that adversaries interrupt the flow of gas on two major pipelines for three months, including in the coastal region. This scenario constitutes a limited threat to fuel supplies.

- Realistic but extreme contingency: assume that adversaries disrupt 80 percent of the gas pipelines in the PJM region as a whole for six months. This scenario represents the severe threat that a major state adversary might pose, reflecting the outcome of combined high explosive and cyberattacks on all major pipelines in the region, potentially combined with attacks on gas storage facilities and other critical gas infrastructure components.

The most likely way that adversaries could create an 80 percent disruption would be to exploit common failure modes in the natural gas systems that serve the PJM region. As will be discussed later in this study, adversaries may be able to disrupt widely-distributed gas system components in a single cyberattack, by exploiting supply chain vulnerabilities and related threat vectors which DHS recently attributed to Russian actors.[4] PJM may also want to adopt a sub-regional approach to model realistic but extreme contingencies. For example, in certain coastal portions of the PJM service area, physical attacks on a small number of major pipelines could disrupt 80 percent of that sub-region's pipeline capacity and potentially cause disruption of storage for extended periods.

PJM may find it useful to model additional contingencies as well. However, given the critical military installations and other national security facilities in the PJM service area, this area will be *ground zero* if Russia, China, or other potential adversaries launch comprehensive attacks to disrupt the flow of natural gas for power generation. Such attacks could also spread disruptions to New York and other regions that are densely populated and vital to the U.S. economy. The realistic but extreme scenario proposed in this paper will be essential to assess fuel security against such threats.

Second, the PJM study approach notes that Phase I will incorporate locational variations in system infrastructure, such as the proximity of generators to gas production facilities co-located with gas fields in the Marcellus. This granularity will greatly improve the accuracy of company-specific models. However, we should also assume that in a comprehensive attack on gas flows, adversaries will target all types of infrastructure components that might be vulnerable to high-consequence cyber or physical attacks, ranging from key nodes in gathering and refining

[4] "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *United States Computer Emergency Readiness Team*, last revised March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

facilities to storage facilities. Modeling initiatives in Phase I should account for the risk of such multi-component attacks.

My third recommendation is that PJM launch Phase III of the study ("Ongoing Coordination") at the same time that it begins executing Phase I. The first phase involves identifying system vulnerabilities and developing fuel security criteria to assess them. Given the severity of threats to fuel resilience and the length of time the government requires to identify security needs in the PJM footprint, PJM should not delay work on this first phase of the study until such information is available. The third phase calls for collaboration with government agencies to address concerns related to cyber and physical security. However, precisely because so much time may be required to reach government-industry agreement on threat data priorities and sharing mechanisms, PJM should immediately reach out to FERC and other appropriate agencies to begin that consensus-building process. The analysis that follows offers specific recommendations on how to structure that coordination.

I. DISRUPTION SCENARIOS FOR PHASE I

PJM defines fuel security as "the ability of the system's supply portfolio, given its fuel supply dependencies, to continue serving electricity demand through credible disturbance events, such as *coordinated physical or cyberattacks* or extreme weather that could lead to disruptions in fuel delivery systems, which would impact the availability of generation over extended periods of time."[5]

Manmade and weather threats to fuel resilience are not mutually exclusive. Indeed, as Phase I goes forward, PJM may want to consider adding a dual-disruption scenario: i.e., cyber or physical attacks occurring in the midst of a severe, extended winter freeze, when heating demand and risks of gas curtailment to power generators would be most extreme.

Initially, however, PJM should develop manmade disruption scenarios that help scope fuel security vulnerabilities against high-capability nation states (Al-Qaeda and other terrorist organizations will constitute lesser included cases). Two factors will be most important in developing disruption scenarios and assessing their impact on power generation: the number of pipelines and/or storage facilities that adversaries will be able to disrupt, and how long fuel interruptions will last.

A. NUMBER OF PIPELINES DISRUPTED AND STORAGE FACILITIES CONSTRAINED

Threat assessments by the Transportation Security Agency (TSA) provide the starting point for scoping the threat to pipelines, storage facilities, and other gas infrastructure components in the PJM region. TSA has regulatory authority for pipeline security under P.L. 107-71 and P.L. 110-53 (though TSA relies on voluntary industry compliance with the agencies' security guidance, versus the mandatory relatability standards that NERC issues for the bulk power system) and provides a Pipeline Threat Assessment (For Official Use Only).[6] However, TSA has not updated

[5] PJM Interconnection, LLC, *Valuing Fuel Security*, April 30, 2018, p. 1.
[6] Aviation and Transportation Security Act, Public Law 107-71, *U.S. Statutes at Large* 115 (2001); Implementing

that document since 2011. DOE and the Department of Homeland Security have provided more recent assessments. Both Departments have found that cyber threats to electric and natural gas systems are rapidly intensifying.[7] My May 10, 2018 testimony to FERC examines these threats.

U.S. reliance on natural gas for power generation has been increasing along with adversary capabilities to attack pipelines and storage sites in the PJM region and beyond. The net result: according to Bruce Walker, Assistant Secretary of Energy for Electricity Delivery and Energy Reliability, this "increased dependency on our pipelines" has "effectively doubled and tripled the amount of critical infrastructure that is necessary for us to protect predominantly on a cyber front but also from a physical security front."[8]

The expansion of natural gas infrastructure in the Marcellus and other areas can benefit fuel security. Where redundant pipeline systems exist to serve power generators, the loss of a single pipeline may have little or no effect. But other portions of the PJM region have much less gas infrastructure redundancy. In coastal regions of New Jersey and Maryland, for example, the loss of even two major pipelines and/or storage facilities could have major effects on power generation. Accordingly, as PJM already envisions, it will be important to employ disruption scenarios to identify fuel security risks that could affect specific locations of the system.

The question remains of how many disruptions of pipelines and other gas system components these scenarios should entail. It is (barely) conceivable that in an escalating crisis, Russia or another potential adversary might attack a single pipeline or storage site to demonstrate their ability to hold the gas transmission system at risk, and/or threaten further attacks unless the United States acceded to whatever demands they were making. But it is far more likely that adversaries will attack on a larger scale. If a crisis with the United States is so dire than an adversary will launch cyber or physical attacks on gas systems, despite the risk of provoking an overwhelming response by U.S. forces, we should expect that the enemy will seek to deal us a crippling blow.

For cyberattacks, the actual number of pipelines in the PJM footprint that adversaries will be able to disrupt will vary with their ability to exploit common modes of failure, and conduct simultaneous attacks on multiple pipelines in the region. Supply chain corruption poses an especially significant challenge in this regard.[9] If adversaries are able to corrupt the development

---

Recommendations of the 9/11 Commission Act, Public Law 110-53, *U.S. Statutes at Large* 121 (2007); Peter Behr and Blake Sobczak, "TSA to expand gas pipeline cybersecurity oversight," *E&E News*, December 22, 2017, https://www.eenews.net/stories/1060069743; Transportation Security Agency, *Pipeline Threat Assessment*, January 18, 2011.

[7] Department of Energy, *Multiyear Plan for Energy Sector Cybersecurity*, March 2018, p. 3; Transportation Security Administration, *Pipeline Security Guidelines*, March 2018, p. 1.

[8] Bruce Walker, (speech delivered at the GridWise Alliance 2018 Spring Group Meetings, Chicago, IL, May 11, 2018).

[9] In July 2016, FERC directed NERC to develop a Supply Chain Risk Management reliability standard for BES entities, which is currently available (Standard CIP-013-1). NERC intends the standard to "mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems." See: North American Electric Reliability Corporation, *CIP-013-1 – Cyber Security - Supply Chain Risk Management*, July 2017, p. 3, https://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/CIP

and production process for widely-used gas system software and hardware components, they could gain the ability to later sabotage or covertly control those components, and attack multiple pipelines at the same moment. Doing so would cause common mode failures, disrupting power generation over wide areas. Conducting special forces-type physical attacks on multiple compressor stations, storage facilities, and pipelines would entail greater coordination and pre-attack planning challenges.[10] However, because of the massive damage that vehicle-borne improvised explosive devices (VBIEDs) or other kinetic attacks could create,[11] adversaries seeking to maximize disruption to power generation will have strong incentives to conduct such attacks against critical gas infrastructure nodes.

Given the variations in adversary capabilities to conduct such large scale cyber and physical attacks, PJM should consider employing credible high- and low-threat scenarios of cyber and physical attacks. At the low end, the disruptive scenario should assume that adversaries interrupt the flow of gas on two major pipelines. At the higher end, reflecting the risk of common mode failures *combined* with carefully targeted attacks using high explosives, a "realistic but extreme" contingency should reflect the disruption of 80 percent of major pipelines in the PJM region, as well as severe disruptions in gas storage.

B. DURATION OF FUEL INTERRUPTIONS

The impact of pipeline system attacks on power generation will also depend on how long gas interruptions last. From a cyber perspective, a primary threat for extend-duration interruptions will come from Advanced Persistent Threats hidden in gas system networks and components, which – unless entirely eradiated – will launch repeated attacks based on timing or system conditions.[12] However, physical attacks offer special risks of extend gas supply disruptions. Attackers have frequently used high explosives against gas pipelines in the Middle East and elsewhere to halt gas flows and require extensive, time-consuming repairs.[13] Fortunately, no such attacks have yet occurred in the United States. But terrorists have employed truck bombs with tons of explosives against other U.S. targets in Oklahoma City and beyond all too often.

Even corrosion-induced pipeline failures can take many months to repair. In the case of the 2016 Spectra pipeline explosion, for example, repairs took six months to complete.[14] Gas companies would no doubt seek to accelerate the restoration of service if the United States were in the midst

---

-013-1_Clean_071117.pdf. FERC issued a Notice of Proposed Rulemaking proposing to approve this standard with some additional requirements. *See* Supply Chain Risk Management Reliability Standards, 162 FERC ¶ 61,044 (2018). Without similar strategies for natural gas systems, however, potential supply chain vulnerabilities that could have cascading effects in the Bulk Power System remain.

[10] Mark Galeotti, "The Three Faces of Russian Spetsnaz in Syria," *War on the Rocks*, March 21, 2016, https://warontherocks.com/2016/03/the-three-faces-of-russian-spetsnaz-in-syria/.

[11] Department of Homeland Security and National Academy of Sciences, *IED Attack: Improvised Explosive Devices*, July 8, 2015, https://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf.

[12] Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*, June 2016, p. 7.

[13] "IS-linked militants claim attack on Sinai pipeline to Jordan," *Middle East Eye*, January 8, 2016, http://www.middleeasteye.net/news/linked-militants-claim-attack-sinai-pipeline-jordan-2114845158.

[14] Debra Erdley, "6 months after Salem Township explosion, Spectra Energy has gas pipelines running," *Tribune Review*, November 18, 2016, http://triblive.com/local/westmoreland/11496039-74/pipeline-spectra-explosion.

of a national security crisis. However, multi-point physical attacks would create unprecedented challenges for restoring gas flows. The Spectra repair operation took place in blue sky conditions. Efforts to repair gas systems after attacks by Russia or China would need to go forward in a much more challenging environment, especially if the electric grid and communications systems were affected as well. A truck bomb carrying tons of high explosives would create damage far more extensive than in the Spectra incident or any previous U.S. pipeline failure – potentially over multiple, carefully-selected sites in the PJM region.

As with assumptions on the number of pipelines and/or storage facilities that an adversary will attack, PJM should consider adopting low- and high-end estimates of gas interruptions, and combine those risk factors into two consolidated disruption scenarios. The low could assume that adversaries will halt the flow of gas on two major pipelines for 3 months. The higher end "realistic but extreme" scenario would posit the disruption of 80 percent of the major pipelines including storage facilities in the PJM region for 6 months.

C. ATTACKS ON MULTIPLE TYPES OF SYSTEM COMPONENTS

PJM's proposed study approach for Phase I emphasizes the need for the stakeholder process to account for local variations in gas infrastructure and the resulting implications for fuel security. The proposal notes that generation located "on top of a Marcellus shale field does not face the same fuel security issues as a generator more distant from supply and connected to a lateral pipeline served by a single natural gas distribution company."[15] Accounting for such variations will greatly improve model accuracy.

However, as these system-specific modeling efforts go forward, it would be a mistake to assume that adversaries will only attack pipelines and the compression stations that serve them. The NERC *Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System* (November 2017) notes that gas storage facilities and other gas infrastructure components are critical for enabling the electric industry to meet its load-serving obligations.[16]

Industrial control systems and other network-connected electronic devices and control mechanisms are embedded across many of these gas system components, from production, gathering, and processing facilities to local distribution company infrastructure. All such connected systems may be vulnerable to cyberattacks or supply chain exploitation (including the introduction of corrupted software though Russian threat vectors recently identified by DHS).[17] Depending on the configuration of specific gas systems, physical attacks against crucial but

[15] PJM Interconnection, LLC, *Valuing Fuel Security*, April 30, 2018, p. 3.
[16] North American Electric Reliability Corporation, *Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruption on the Natural Gas System*, November 2017, p. *vii*.
[17] "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *United States Computer Emergency Readiness Team*, last revised March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

unprotected system components could also produce long-term disruptions to fuel supplies for power generation.

The net result: factors such as generator proximity to the Marcellus shale field may not automatically translate into reduced vulnerability. As location-specific modeling goes forward, Phase I should account for the risk of attacks on multiple types of gas system components, especially if they offer adversaries alternative and more efficient means of interrupting fuel flows than by attacking pipelines alone.

II. ONGOING COOPERATION: ADVANTAGES OF AN EARLY LAUNCH FOR PHASE III

The study overview notes that "PJM anticipates overlap between phases" as the initiative goes forward. While Phase I should be initiated as soon as possible, PJM should also consider a rapid start for the "Ongoing Coordination" called for in Phase III.

PJM has already found that "There are obstacles to obtaining information necessary to assess cyber security threats because RTOs can only base their threat assessments on open source information and certain classified intelligence, but the information from classified sources is limited and does not provide a full and complete understanding needed to detect and respond to cyber-attacks."[18] PJM similarly emphasized the need for Federal support on identifying and assessing risks: "there needs to be a process for vulnerability threat verification. The Commission needs to provide intelligence and metrics to apply to resilience vulnerability and threat analyses, such that they can then guide and anchor subsequent RTO planning, market design, and/or operations directives. Overall there needs to be better information made available to the RTOs on the above-identified risks to enable the RTOs to assess the risks. This information could be supplied from a wide range of federal agencies and interdependent systems."[19]

Phase III should be structured to fill these gaps to support fuel security assessments for both cyber and physical threats. Ideally, PJM could reach out to FERC, DOE, and other Federal partners for a near-term review of the disruption scenarios provided in this paper. However, over the longer term, PJM should collaborate with these partners to develop a more holistic design basis threat to assess and mitigate gaps in grid resilience.

Government assistance in developing a design basis threat will be especially important for incorporating national security considerations into fuel security assessments. Assistant Secretary Walker recently stated that "I don't know that the RTOs or NERC have the visibility or proposer information to determine if something is a national security issue." Indeed, "with the various

[18] PJM Interconnection, L.L.C, "COMMENTS AND RESPONSES OF PJM INTERCONNECTION, L.L.C.," *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators (AD18-7-000)*, March 9, 2018, pp. 52-3, http://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx.

[19] PJM "COMMENTS AND RESPONSES OF PJM INTERCONNECTION, p. 32

intelligence agencies we have throughout the federal government" as well the Department of Defense, "we have different information" than RTOs and NERC.[20]

As PJM moves forward in the Phase III process, it will be essential to build a secure process so that this government information can help guide PJM fuel resilience assessments. PJM and its member companies serve a broad array of military installations and other facilities vital to national security, and are already taking aggressive measures to ensure these facilities have the power they require. The Valuing Fuel Security study offers a timely and much-need opportunity to further reinforce such resilience. Basing PJM's analysis on realistic, credible assessments of the threat is a prerequisite for ensuring that the initiative succeeds.

[20] Gavin Bade, "DOE's Walker: National Security Assessment Broader than Grid Reliability, Utility Dive, April 20, 2018, https://utilitydive.com/news/does-walker-national-security-assessment-broader-than-grid-reliability/521852/