a Publication of GDS Associates, Inc.

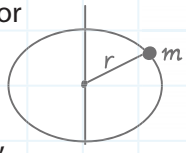
TransActions

2021 Q2

REACTIVE POWER COMPENSATION

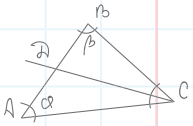
& non-synchronous generators

INTRODUCTION. The past few years has seen a surge in reactive power compensation filings for solar and wind-powered projects, with a high concentration of filings for facilities in MISO and PJM. There are several factors contributing to this trend. Spurred on by decreasing costs, state and regional renewable energy goals, and investment tax credits (ITC), solar leads all other technologies for new electric generation capacity additions. Together solar and wind outstripped all other technologies 4:1 in new U.S. capacity additions in 2020. Until recently, reactive power compensation for wind and solar was not an achievable revenue opportunity, but technological advancements and changes in the regulatory landscape created new revenue opportunities for non-synchronous resources. And since PJM and MISO are the most lucrative markets for reactive compensation, it is not surprising to see the number of solar and wind projects seeking reactive compensation at the Federal Energy Regulatory Commission ("FERC" or the "Commission").



HISTORIC PERSPECTIVE: REACTIVE POWER REQUIREMENTS FOR SYNCHRONOUS AND NON-SYNCHRONOUS GENERATION

Order Nos. 2003 & 2003-A In Order No. 2003 Standardization of Generator Interconnection Agreements and Procedures, the Commission adopted standard procedures and a standard agreement for the interconnection of Large Generating Facilities, which included the reactive power requirement. Under this requirement, facilities must be designed to provide 0.95 leading to 0.95 lagging reactive power at the Point of Interconnection. Subsequently in Order No. 2003-A the Commission recognized the pro forma interconnection agreement was designed around large synchronous generators, and determined that generators relying on newer technologies with unique electrical characteristics (i.e., wind generators) would be exempted from this reactive power requirement.[1]



Order No. 827 The next signifcant Commission order for non-synchronous generators' requirements for reactive power came with Order ***No. 827, Reactive Power Requirements for Non-Synchronous Generation***. In this order, the pro forma interconnection agreement were revised to require new non-synchronous generators to provide dynamic reactive power, recognizing that the equipment needed to provide reactive power had become more commercially available and less costly.

GDS ASSOCIATES

was excited to attend the

2021 APPA National Conference

Being among the first conferences to be held ***live and in-person*** in over a year, it was not only refreshing but a huge success!

LOOK FOR US

Upcoming Conferences

JULY 26-28
TPPA Annual Meeting
San Antonio, TX

AUGUST 15-17
UAMPS' 2021 Member Conference
Olympic Valley, CA

AUGUST 16-18
Electricities of North Carolina Annual Conference
Hilton Head, SC

UPCOMING WEBINARS

JULY 13
How to Place Capacitors on a Distribution System

AUGUST 10
NESC Clearances on Poles

SEPTEMBER 14
Application and Coordination of Overhead Fuses

Note *All webinars are recorded & available for viewing post-presentation*

However, acknowledging the differences in technologies between synchronous and non-synchronous generators, Order No. 827 altered the point of measurement of reactive capability for non-synchronous generators from the Point of Interconnection to the high-side of the generator substation.

COMPENSATION FOR REACTIVE POWER.

Generally, compensation can be categorized as either "pay for capability" or "pay for performance". *Figure 1* presents a summary of the compensation models throughout the United States.

Although ISO-NE, NYISO, PJM and MISO all pay for capability, compensation in PJM and MISO are most lucrative since the compensation is an individual cost-based revenue requirement, based on the AEP Methodology. That is the higher the costs to provide the service, the higher the compensation. Additionally, several markets also compensate generators providing reactive service for variable costs, such as lost opportunity costs, cost of energy consumed, and/or cost of energy produced, when called upon to produce MVArs instead of MW.

AEP Methodology & Adaptation for Non-synchronous Generators. While the Commission has not required a uniform approach to compensation for reactive power, the FERC-approved AEP Methodology is the precedent for calculating cost-of-service reactive service compensation in a "pay for capability" compensation model, such as in MISO and PJM. This oft-cited method originated with AEP's 1993 FERC rate case to determine an annual revenue requirement for its fleet of thermal (coal) generators.

The method depends in large part upon the FERC Uniform System of Accounts ("USofA") to allocate investment in specific components supporting production of reactive power based on the accounting treatment for that plant, and applies an annual fixed charge rate to that investment to arrive at the annual reactive power revenue requirement.

The AEP Methodology has since been adapted for non-synchronous resources. In doing so, applicants liken the function of key components addressed in AEP to the specific components characteristic of non-synchronous generators, such as solar panels, AC and DC collection systems, wind turbines, and inverters.

However, the adaptation of AEP for non-synchronous generation is not without criticism or controversy. Common objections to the interpretation of AEP to non-synchronous generation include:

1. ***Proper accounting for wind and solar plant costs, which is now the subject of a rulemaking before the Commission;***
2. ***Attribution of non-synchronous components by function to that of typical synchronous generator components supporting reactive production;***
3. ***Allocation of components to Accessory Electric Equipment supporting production of reactive power, i.e., the "AEE Allocation Factor;" and***
4. ***Demonstrated reactive capability vis-a-vis use of nameplate Power Factor ("PF") of the invertors in calculating the Reactive Power Allocation Factor.***

Reactive Revenues Paid to Solar and Wind Generators. Current practice at FERC is, with limited exceptions, to set all reactive filings for hearing and settlement proceedings. Most reactive filings are settled without going to litigation at some reduction to the filed rates. For wind and solar filings, the settlement process typically results in a significant reduction to the as-filed annual revenue requirement ("ARR") (see ***Figure 2***).

Two key objections to continue using AEP as precedent for determining revenues for non-synchronous generations are that (1) the reasonableness of paying reactive compensation based on a method that does not account for the intermittency of non-synchronous generation (no wind, no sun, no power); and (2) the as-filed ARRs for non-synchronous resources resulting from the modified AEP approach are notably higher than that of comparably sized synchronous generation. Despite the reductions taken in settlement, MISO and PJM solar and wind revenues are nevertheless on average two to five times greater than those paid to steam, combustion turbine or combine cycle generators on a $/MW basis, based on Q4 2020 data for reactive revenues paid in MISO and PJM.

Figure 1 ***US Compensation Models Summary***

RTO/ISO	PAY FOR CAPABILITY	PAY FOR PERFORMANCE
ISO-NE	Fixed $/kVAr-year	
NYISO	Fixed $/MVAr-year	
PJM	Individual revenue requirement, based on AEP method	
MISO	Individual revenue requirement, based on AEP method	
SPP		Fixed $/MVArh, only compensated outside of obligation bandwidth when called upon by SPP
CAISO		Based on LMP
ERCOT		Paid the avoided cost of reactive support resources, $/MVArh, only compensated outside of obligation when dispatched by ERCOT

RECENT EVENTS DRIVING CHANGE

Spurred by the exponential rise in renewable generation, particularly from the independent power production sector over the past several years, stakeholders in both MISO and PJM are investigating alternative rate designs for reactive power.

continued on page 3

A common element to both the MISO and PJM rate designs is there is no cap on the amount of reactive capability for which the ISO/RTO will compensate. That is, regardless of need for additional reactive service, if a generator's compensation request is approved by the Commission and it meets the ISO/RTO technical requirements then the applicant recovers the approved revenue requirement.

Figure 2 *Wind & Solar Reactive Compensation in PJM and MISO*[2]

	WIND		SOLAR	
	Filed	*Settled*	*Filed*	*Settled*
# Filings	57	45	28	12
Total Capacity (MW)	9,292	7,304	1,369	352
Avg. Revenue ($/kW-mo)	$0.47	$0.29	$1.30	$0.48

As previously discussed, the adaptation of the AEP method used by several expert witnesses in this field yields as-filed ARRs significantly higher on a dollar-per-MW basis compared to synchronous generation. Protesting parties routinely identify the general inapplicability of AEP and specifically the criticisms described previously as key issues in the filing.

In an attempt to resolve some of these issues, on April 28, 2020, Locke Lord LLP filed a request for confirmation from the Chief Accountant at the FERC that the cost of specific wind and solar generating equipment is properly booked to FERC Account Nos. 343 - Prime Movers. 344 - Generators, and 345 - Accessory Electric Equipment, in Docket No. AC20-103-000.

On January 19, 2021, the Commission rejected Locke Lord LLP's request, but concurrently opened a Notice of Inquiry (NOI) on the accounting and reporting treatment of certain renewable energy assets under Docket No. RM21-11-000. The NOI solicited comments on (1) whether the Commission should create new accounts for non-hydro renewable generating assets in the USofA, (2) revisions to FERC Form No. 1 to reflect any such new accounts, (3) whether the Commission should codify the proper accounting treatment of renewable energy credits, and (4) the rate implications of these potential accounting and reporting changes (i.e., impact on reactive power rates).

As an electric utility, it makes sense to consider the repercussions of all reactive rate filings within the transmission zone which may require intervening in reactive revenue dockets to express specific concerns.

EVOLVING LANDSCAPE & CONSIDERATIONS

Owners of renewable generation will continue to optimize revenue streams and to seek those revenues in the most lucrative markets. There is growing momentum in both MISO and PJM to address the current reactive power compensation construct, and that, coupled with activity at the Commission with the NOI, other non-ISOs/RTOs will likely follow suit and/or look to the outcome of RM21-11 to decide the best model for their ratepayers. That said, no formal proceedings have begun to initiate a change to Schedule 2 in MISO or PJM.

The Commission may propose changes to the USofA that include new account categories to address new technology and the accounting treatment thereof, but it is likely that this will take more than three years to finalize.

As an electric utility, it makes sense to consider the repercussions of all reactive rate filings within the transmission zone which may require intervening in reactive revenue dockets to express specific concerns. It's also helpful for electric utilities to identify opportunities to optimize potential reactive revenues from the utility's generation resources to lower transmission cost for retail customers. ■

For more information or to comment on this article, please contact:

Michele Slater, *Senior Project Manager*
GDS Associates, Inc. -
Marietta, GA
407-563-4461 or
michele.slater@gdsassociates.com

References

1 *Order 2003 and 2003-A refer to wind generation, but are interpreted to be equally applicable to solar generation as a non-synchronous generator.*

2 *Data set based on single facility filings, mostly IPPs.*

What Does the Ransomware Attack on COLONIAL PIPELINE mean for the Future of Critical Infrastructure Protection?

On May 7th, Colonial Pipeline was forced to shut down operations as a result of a ransomware attack. The shutdown lasted until May 12th and the effects of the shutdown were felt long after. Colonial Pipeline supplies 2.5 million barrels of fuel daily to the southeastern US. This accounts for about 45% of the fuel for the region and resulted in massive fuel shortages which lasted for weeks.

The gas industry, as well as others who are part of the critical infrastructure, are extremely vulnerable to cyberattacks. Many of the different industries that make up the critical infrastructure do not have any regulations in place to protect against these kinds of attacks. The attack on Colonial Pipeline was not even trying to disrupt pipeline operations. The group that targeted Colonial Pipeline saw them as an easy target, and just wanted to make money. However, Colonial Pipeline did not have their operations network properly segregated from their business network and an attack on the business network resulted in a complete shutdown of their operations network.

Many critical infrastructure industries, including the natural gas industry, do not have the same regulations as the electric power industry. The electric power industry has an entire set of cybersecurity standards, the NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) Standards, that they must follow in order to prevent this type of occurrence. These standards exist today as a result of the 2003 northeast blackout, which left over 55 million people without power. It is only a matter of time before similar measures are going to be put in place across all industries that make up our critical infrastructure.

Natural gas and electricity go hand in hand and If something effects the gas supply, it will also affect electricity generation. The February 2021 events that unfolded in the South-Central region of the United States were caused by cold weather and drastically affected the ability of natural gas suppliers and pipelines to deliver gas to electric generation. But if a cyberattack were to impact the gas pipelines in the same way, that in turn would similarly cascade into additional critical infrastructure, such as the electric grid. If we want to protect our electric grid, then it makes sense to protect our gas pipelines as well since these systems do not work in isolation and are all co-dependent.

On May 12th, ***President Biden signed an executive order designed to improve the nation's cybersecurity in order to protect critical infrastructure and the Federal Government networks underlying the nation's economy and way of life.***

continued on page 5

The goals of the executive order are as follows:

- ***Improve threat information sharing between government and private sector***
- ***Increase and improve cybersecurity standards in the Federal Government***
- ***Improve supply chain security***
- ***Create a cyber safety review board***
- ***Create a standardized process for responding to cyber security incidents***
- ***Improve measures for detecting and mitigating potential threats***

From this executive order, we can see that the increase in recent cyberattacks warrants additional measures to be taken in cybersecurity, specifically surrounding supply chain and incident response. This is the second time President Biden is addressing supply chain, following the previous executive order signed on February 24th. NERC's most recent additions to the CIP Standards included adding in a Supply Chain Risk Management Standard and improving the current Incident Response Standard. Additional agencies within the Federal Government are also starting to see an increase in cybersecurity regulations.

The executive order targeting supply chains calls for two separate reviews of supply chain vulnerabilities. The first, targeting vulnerabilities related to semiconductors, batteries, strategic minerals, and pharmaceuticals. The second, targeting vulnerabilities in critical sectors, including defense, public health, information technology, energy, transportation, and agriculture. The goal is to eventually limit reliance on products from competitor nations.

Over the past few years, the world has seen a dramatic increase in both cyberattacks and more specifically, ransomware attacks. Just recently, Kaseya, an information technology firm, was hit by a ransomware attack. This single attack has affected around 800 to 1,500 businesses around the world. Back in 2020, SolarWinds, an information technology and software development firm, was also hit with a major cyberattack. This attack affected around 18,000 SolarWinds customers, including the US Department of Homeland Security.

The US was hit with over 65,000 ransomware attacks in 2020, and that number is only expected to continue rising. The rise in popularity of Bitcoin and other cryptocurrencies is also making it easier for attackers to demand and receive ransom payments outside of the traditional financial institutions. Colonial Pipeline paid its attackers around $4.4 million in order to get their systems back under their operational control. The group behind the Colonial Pipeline cyberattack, Darkside, specifically targets hospitals, schools, non-profits, and governments. They are not alone, these targets typically have less cybersecurity protections in place, have neglected IT staff and infrastructure, and can afford to pay out larger sums in order to regain control of their systems.

The continued proliferation of ransomware attacks will hopefully push other industries classified as critical infrastructure protection to implement cybersecurity regulations. The NERC CIP Standards, which were developed for use to regulate the electric power industry were based around the NIST SP 800 series. NIST is the National Institute of Standards and Technology. It is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. For entities looking to increase their cybersecurity protections, this is a great place to look for guidance. Specifically, the NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations, provides a good baseline catalogue of security and privacy controls to follow.

NIST SP 800-53 was originally created in order to help improve the security of the information systems used within the federal government but has since been expanded to include non-federal information systems. The controls are broken up into low, medium, or high classes based on impact level. These controls are placed in 20 different families within cybersecurity. ***The control families include:***

- ***Access Control***
- ***Awareness & Training***
- ***Audit and Accountability***
- ***Assessment, Authorization & Monitoring***
- ***Configuration Management***
- ***Contingency Planning***
- ***Identification & Authentication***
- ***Incident Response***
- ***Maintenance***
- ***Media Protection***
- ***Physical & Environmental Protection***
- ***Planning***
- ***Program Management***
- ***Personnel Security***
- ***PII Processing & Transparency***
- ***Risk Assessment***
- ***System & Services Acquisition***
- ***System & Communications Protection***
- ***System & Information Integrity***
- ***Supply Chain Risk Management***

continued on page 6

Implementing even the low impact controls across all of the control families will drastically improve cybersecurity protections.

Another great resource for preventing these kinds of attacks is GridSecCon. GridSecCon is an event put on by NERC every year to help entities with their incident response and recovery procedures. They put on a simulated widescale event that emulates a cybersecurity attack against the critical infrastructure in the US. Entities are supposed to coordinate and work together with one another, working through their individual incident response processes and eventually recover from the simulated event. This event started out as a tool for electric utilities to better know their incident response procedures, but has since expanded into a more widescale event that encompasses more critical infrastructure and also includes the addition of gas industry participants.

Some commonsense activities also include:

(1) spending additional funds on IT and Cybersecurity infrastructure, systems, and incident response training;

(2) providing protocols for the company's IT and operations staff to work together on cybersecurity related problems and solutions;

(3) ensuring the company's business networks and operations networks are properly separated;

(4) develop a cybersecurity program (if you do not already one) or look for areas of improvement within the existing cybersecurity program.

COMMONSENSE ACTIVITIES

(1) spending additional funds on IT and Cybersecurity infrastructure, systems, and incident response training;

(2) providing protocols for the company's IT and operations staff to work together on cybersecurity related problems and solutions;

(3) ensuring the company's business networks and operations networks are properly separated;

(4) develop a cybersecurity program (if you do not already one) or look for areas of improvement within the existing cybersecurity program.

James Fenstermaker is the Cyber Security Lead Project Consultant at GDS Associates. He works with Clients thoughout the United States to develop and assess their cyber security programs and practices. ■

For more information or to comment on this article, please contact:

James Fenstermaker,
Project Consultant
GDS Associates, Inc. - Marietta, GA
770-799-2480 or
james.fenstermaker@gdsassociates.com