a Publication of GDS Associates, Inc.

TransActions

Developing On Call Energy & Capacity Security

2023 Q3

This article is the second of a three-part series. Part 1 introduced the need for industry proven power project development and asset management processes that can be utilized by organizations to effectively develop, own, and manage natural gas fired generation resources or to do the same via a power purchase agreement. Part 1 detailed the phases of power project development and discussed the required implementation functions needed to successfully develop the project.

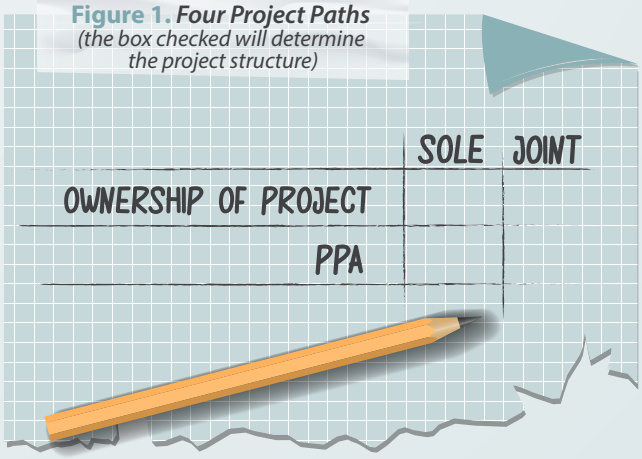
DEVELOPMENT STRATEGY DETERMINES PROJECT STRUCTURE

A project's development strategy will determine the organizational approach or project structure that will be required to implement the project. Projects can be pursued individually or jointly and through either ownership or power purchase agreement (PPA) approaches, resulting in four possible paths. The resulting structures will generally include the same types of technical and commercial resources, but the level of engagement of these resources will differ.

A project ownership strategy, sole or jointly, will require a higher level of resource engagement and time commitment than an off-taker strategy under a power purchase agreement. In a PPA scenario, depending upon the term and ongoing resource planning, some degree of internal resource capabilities or outside services should be in place to proactively track and manage the contract and as needed ongoing asset-based power supply decisions. A long term PPA for a power project to be developed will have greater complexity than a shorter term PPA from an existing power plant.

This article will focus on sole project ownership and the third article in the three-part series will explore joint ownership, saving PPA arrangements for another time.

Figure 1. ***Four Project Paths***
(the box checked will determine the project structure)



GDS Associates

is excited to announce our

NEW

office location in **California**

850 Iron Point Road, Suite 154
Folsom, CA 95630

&

RELOCATION

in **New Hampshire**

15 Constitution Drive, Suite 1E
Bedford, NH 03110

LOOK FOR US

Upcoming Conferences

AUGUST 13-16
UAMPS (Utah Associated Municipal Power Systems) Annual Member Conference
Jackson Hole, WY

AUGUST 14-16
Electricities of North Carolina Annual Conference
Myrtle Beach, SC

UPCOMING WEBINARS

Hi-Line Engineering is excited to once again offer ***12 webinars throughout 2023*** all geared toward keeping you up-to-date on industry issues and standards!

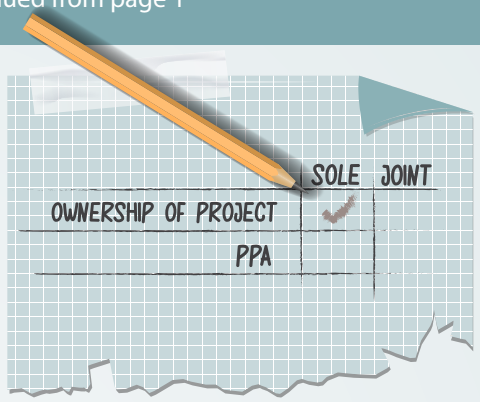
AUGUST 8
Three-Phase, Pad-Mounted Transformers

SEPTEMBER 12
Harmonics and Effect on Power Quality

OCTOBER 10
Overhead Conductor Characteristics

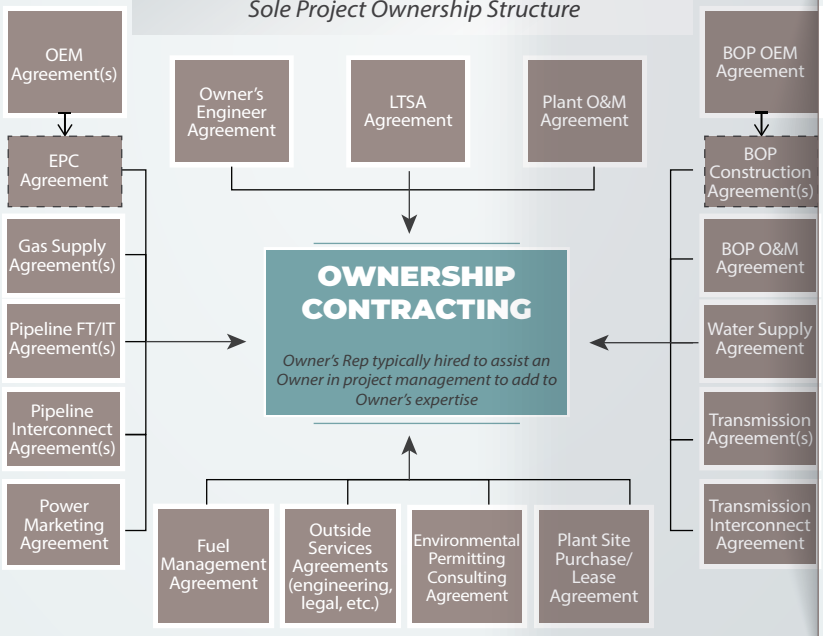
Note *All webinars are recorded & available for viewing post-presentation*

SOLE PROJECT OWNERSHIP



Power project development requires the same types of technical and commercial support regardless of the development strategy. But a sole ownership and development strategy and structure will require a higher level of resource engagement and commitment. This concept is best illustrated by noting the various agreements that will need to be sourced, negotiated, and administered to complete the power project's development and eventual operation (***Figure 2***). The remainder of this article will emphasize four major areas of focus: ***project management, engineering/technical focus areas, support focus areas, and incremental internal staffing.***

Figure 2. ***Project Ownership Required Agreements:*** *Sole Project Ownership Structure*



PROJECT MANAGEMENT

It is best practice for an owner not experienced in power project development and with limited internal project development resources, to engage an owner's representative to assist the owner's project development team. Critical owner's representative qualifications not only include experience in all the development contracting and implementation activities mentioned in Part 1, but also experience in providing this assistance to an owner with limited internal expertise. The owner's representative can also assist in developing the project's overall risk management plan and project risk register. After the commercial operation date (COD), the project management functions will unwind, and the focus will shift to an operations management function.

ENGINEERING/TECHNICAL AREAS

There are several areas of Figure 2 that are of an engineering or technical aspect for which outside support may be appropriate. These areas include engineering and construction, fuel and energy management, transmission and compliance, and plant operations and maintenance.

ENGINEERING & CONSTRUCTION. Power project best practices require the formal engagement of an owner's engineer under an ownership strategy where an engineering, procurement, construction (EPC) contract or a developer arrangement is to be bid. The support of this resource is usually required by lenders. Depending upon the project development strategy, the owner's engineer will develop and oversee the project's specifications, performance, and engineering documents that will be relied on to support the array of bidding packages, especially the EPC or developer request for proposals (RFP), in addition to balance of plant, permit filings, loan application, and regulatory approvals. The owner's engineer will also work closely with the project team and legal resources engaged to support the EPC contracting negotiation efforts.

The owner's engineer role is primarily an "inside the fence" function, meaning those resources will govern the project's technical requirements associated with the plant that exist within the plant footprint or fence. However, the owner's engineer will actively collaborate with all other subject matter experts.

Post commercial operation date (COD), the owner's engineer should continue to play a role in the operations and performance of the plant. The experience of the owner's engineer during plant development and construction will be valuable knowledge to be leveraged during the initial operating years so carryover of some of the development and construction personnel should be planned.

FUEL AND ENERGY MANAGEMENT. Given the importance of natural gas transportation capacity acquisition, an experienced fuel consultant that has related power project development experience should be retained. This effort will necessitate focus on pipeline sourcing and engagement, FEED studies, rates and regulatory, pipeline open seasons, contracting, and construction. Prior to the project being completed, a contracted energy manager may need to be sourced and contracted to administer the project's fuel supply and transport contracts along with the plant's energy scheduling and dispatch.

TRANSMISSION AND COMPLIANCE. Depending on the project's transmission capacity requirements and situation, an experienced transmission interconnect and services consultant may be needed to assist in the securing and implementation of the interconnection and transmission requirements and agreements. This assistance will include technical input, transmission modeling, and regulatory and NERC compliance issues. These services may be retained post project COD to assist in the operations management of the project's transmission requirements.

continued on page 3

PLANT OPERATIONS & MAINTENANCE. There are multiple providers of outsourced power plant operations and maintenance services contractors, so sourcing is not difficult, and selection can be bid or sole-sourced. The keys to a successful operation are contractor experience and the final negotiated terms of the plant operations contract. The level of liability acceptance by the contracted provider should be fully understood and defined. This resource should be engaged and fully contracted in sufficient time prior to COD to provide start up assistance and day-one operations support.

SUPPORT AREAS

There are several areas of Figure 2 that are less technical than the engineering functions but for which outside support is likely appropriate. These areas include environmental, funding, analysis, legal, and public relations.

ENVIRONMENTAL. A key resource needed early in the project is an environmental consulting firm that has power project experience and a local presence. Local presence comes with a thorough understanding of the power project permitting requirements and a working relationship with the state's permitting agency. The engaged environmental consulting firm will also be a key participant in the development of an EPC contract. This resource will likely remain engaged, though to a lesser degree, to support permitting compliance and other environmental issues during post COD plant operations.

FUNDING. A consultant experienced in obtaining funding sources and arranging financing for power generation projects should be added to the development team, particularly one familiar with the anticipated source of funding. Seeking and obtaining funding can be a rigorous and time-consuming process. There will be funding implications from early in the project development phase to the eventual closeout of the EPC contract. This resource, along with legal, provides significant benefit by helping navigate the processes and streamlining the preparation and ultimate processing of the array of borrowing documents. The resource engaged to assist the project's owner will unwind post COD and the organization's financial function will rely on such support only as needed.

ANALYSIS. Expertise and experience with power project modeling, resulting life of project costs, and impact on the organization's rates is required on the development team to maintain the project's modeling and decision-making tools during the project's development phases. A strong matrix reporting channel to the organization's leadership to ensure the ongoing integrity of modeling and decision tool results is critical. After COD, similar expertise would be necessary to effectively audit the financial performance of the project and its expected cost and rate objectives.

LEGAL. To prepare the required project documents and agreements as shown in ***Figure 2***, including the EPC RFP and contract or developer arrangement, legal resources that have power project development experience is a must. And depending on the source of the project funding, legal experience in both is very helpful to ensure the contract terms dovetail with the lending requirements. It is common for more than one law firm to be engaged during the development process given the various complex issues that arise in such a project. It is also beneficial to have local counsel near the project site to assist and help deal with local matters including site acquisition, neighboring landowners, local taxes and ordinances, and other related matters including relationships with area governing boards and officials. Local counsel can help source a real estate appraiser/broker that will assist with project siting and purchase of the project site. Post COD, best practices would be to retain the project's outside legal resources to assist as needed in addressing project legal matters as they arise in the early years of the project's operation.

PUBLIC RELATIONS. Outreach support in the form of an experienced local public relations consultant should be secured to manage the organization's messaging related to the project. This function's importance has grown in recent years and should be sourced sooner rather than later. Post COD, outreach support will be needed to assist in area relations and with issues that may arise during plant operations.

INCREMENTAL INTERNAL STAFFING

As already seen, sole project ownership requires a variety of experts for successful execution and operation of the project. Under the ownership scenario, it is industry practice to have some number of internal experienced power operations resources. If not already in house, these resources will need to be added. At a minimum, an experienced plant manager or plant engineer and a mid-level operations resource should be included. ■

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

Paul Wielgus, *Managing Director*
GDS Associates, Inc. - Marietta, GA
770.799.2461 or
paul.wielgus@gdsassociates.com

...SOLE PROJECT OWNERSHIP REQUIRES A VARIETY OF EXPERTS FOR SUCCESSFUL EXECUTION AND OPERATION OF THE PROJECT

ENHANCING PHYSICAL SECURITY

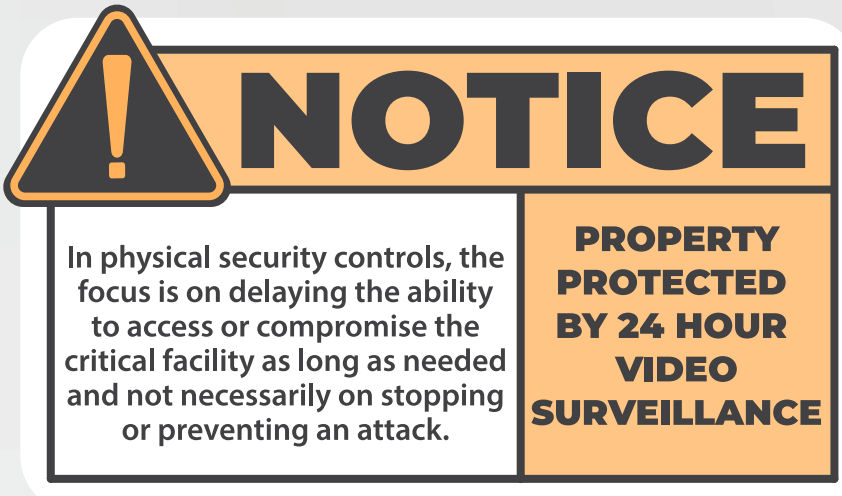
for your

Critical Electric System Facilities

In the electric utility industry, we have spent recent years focusing on cyber threats against our facilities, but now physical threats seem to be making a comeback. Many electric utilities have spent large amounts of money developing and deploying cyber security protections at their critical facilities, including control centers and major substations. Some of the utilities have also focused on increasing their physical security controls, but that has not been the major push from FERC and NERC until recently and, even then, only for the major high voltage substations and control centers (NERC CIP-014). Most companies use standard physical security deterrents that are good enough to meet the minimum requirements for compliance and safety, which may not be good enough in the new physical security threat landscape that we are now facing. Some examples of the changing physical threat landscape are shown in the ongoing war in Ukraine and the substation attacks in North Carolina.

On the international front, Russia has been attempting to destabilize Ukraine for years, by using cyber-attacks against the power grid. Since the start of the war, the Russian forces are actively attacking the Ukraine power grid using both cyber and physical methods. The news headlines show how many articles there are about Ukraine's struggles to keep the lights on from Russia's constant attacks. Domestically, in North Carolina, extremists targeted multiple substations and other power facilities with physical attacks in an attempt to cause major blackouts and potentially create a panic in the area. We have also seen similar tactics used for physical attacks on electric system facilities in Oregon and Washington. ***Attacking the electric grid is often seen as one of the easiest ways for an adversary to destabilize a country.***

When compared to cyber security, physical security encompasses a different thought process. In cyber security, the overall goal is to prevent cyber-attacks and to be able to restore that cyber asset after a critical failure, but for physical security, the main goal is to delay the attacker's ability to compromise your facility long enough for law enforcement to respond and stop the attack. *In physical security controls, the focus is on delaying the ability to access or compromise the critical facility as long as needed and not necessarily on stopping or preventing an attack.* That being said, good physical security controls can be a preventive measure to discourage would-be attackers.



For many, when we think of physical security, we think of locks on doors, fences, sensors, or security cameras, but there are many more facets to a strong physical security program.

Facility design and landscaping can both be key components of physical security. For example, if you build a server room that is critical for your organization and you deploy a Physical

continued on page 5

Access Control System (PACS), the room seems to be physically secure, but if the walls of the room are made of only sheetrock, the PACS will not provide adequate security. Some physical security experts conduct what is called the kick test, if the expert can kick a hole in the wall, they fail the test. Attackers could simply break through the wall with little effort and access the room without even needing to touch the door. One way to prevent this physical security weakness is by adding additional wall protection, such as steel mesh or ballistic paneling. In many cases, physical security is not considered during the initial design process of a facility and then the utility is forced to make modifications to a critical facility to add new physical security controls. The post construction modification can be very costly and, in many cases, would have been much more economical and efficient if they were considered during the design phase.

When devising a physical security program, the designer should consider the facility location, the law enforcement response time, and the criticality of that facility. A remote critical facility may seem to be at a lower risk for a physical attack, but the law enforcement response time may be much longer than for a facility that is in a city. Physical security experts recommend that you take into consideration the average response time of law enforcement may be roughly 1.5 times greater than anticipated, especially if the facility is in a remote location. For example, if you have a major substation located inside the city limits, the law enforcement response time may within 30 minutes of receiving the notification of an event, but if that substation is located in a rural part of the county the repones time maybe hours and not minutes.

Utilities should coordinate with local law enforcement to assess realistic response times to their critical facilities. If you have a critical facility that has a 30-minute response time for local law enforcement, building in at least 30 minutes of delays is crucial. Coordination with local law enforcement is vital to ensure all parties understand the level of importance for physical security as well as understanding the proper way to respond to an event at the facility. This may include training for the law enforcement partners on how to safely access and respond to physical attacks at dangerous high voltage facilities, such as Bulk Electric System substations.

In addition to potentially delayed law enforcement response times, there are other easily identified weak points in most substation physical security controls. ***The first control that can be a weak point is the substation fence.*** Most facilities us a standard fence of 2-inch links with 9-gauge wire it which meets the minimum requirements for a safety and security but can easily be cut through in less than a minute. If the substation uses thicker gauge wire and a smaller link, such as a 6-gauge and 5/8-inch link, the delay in cutting through the fence can be increased by 6 minutes. Those 6 minutes could be vital to maintain the integrity of that facility and add more time for law enforcement to respond.

A second physical security control that can be a weak point is the locks that are used on the facility gates. Unfortunately, most standard pad and door locks are not very secure. The standard padlock that is commonly used throughout the United States can be compromised by anyone who has watched a YouTube video and spent 30 minutes learning how to lock pick. Many standard locks can also be broken or cut though. The best option for critical facilities is to use high security locks with pick resistant pins or a digital signature, such as smart locks. The high security locks can slow down an attacker and provide for more time for a law enforcement response.

A third control that can be both an enhancement and a determent to the physical security of a critical facility is landscaping. If utilized properly, landscaping can both add security controls to the facility and make the facility look aesthetically pleasing. For example, hard to walk on boulders or spikes around the facility will slow down a potential attacker and allow more time for the law enforcement response. Strategically planted bushes can be used to hinder line of sight attacks by gunfire. Landscaping can also be a problem for physical security as it can allow attackers to hide and avoid security cameras or even provide an easier way to climb a fence and enter the facility if it is not well maintained. Clearing trees and brush from around a facility removes the possibility of an attacker using the brush as cover or a method of breaching the physical security perimeter.

A key component to a good physical security program is coordination with neighboring utilities to jointly protect and monitor for security events at critical facilities. The neighboring utilities' security controls also matter to your utility for multiple reasons: 1) electric utilities are part of the interconnected electric grid and damage to a neighbors' facility may also cause outages for your customers; 2) many utilities have shared facilities and want to ensure that both entities have equally as strong security controls; and 3) strong coordinated physical security controls can help deter attackers from either entities' critical facilities. The electric utility industry needs to continue to have conversations between entities about security events that have happened, the responses to those events, and security measures that they put into place to deter future events. Having industry wide transparency of threats and events allows for a better picture of what is happening in the broader scope. For example, there could be a pattern of multiple security events that was not noticed until all the information from multiple entities is gathered and analyzed.

A good way to stay knowledgeable about both physical and cyber security threats to the electric industry is through participation in the North American Energy Reliability Corporation (NERC) and Department of Energy (DOE) Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC is open to all electric utilities and provides a secured platform form sharing information regarding potential and actual physical and cyber security events. Water and gas utilities have similar Information Sharing and Analysis Centers. The Department of Homeland Security launched the Cyber and Infrastructure Security Agency (CISA) in 2018 to assist critical infrastructure entities in protecting their facilities and systems. All of these industry and government groups provide information on ways to protect your entity from physical and cyber security threats and ways to coordinate with fellow utilities as well as local, state, and federal law enforcement entities.

To summarize, here are some key take aways that will be helpful in deploying an effective physical security program:

01 Law enforcement response times can vary based on location of the critical facilities. It is good to plan for a response time 1.5 times longer than anticipated.

02 Locks, cameras, sensors, and fences serve as deterrents but cannot stop physical security incidents from occurring.

03 Priority in developing physical security controls should be given to the utilities most critical facilities.

04 A key goal of physical security is to delay the intruders/attackers for as long as you can to allow law enforcement to respond.

05 Landscaping is an often unthought of part of an effective physical security program.

06 Coordination with neighboring utilities and through the E-ISAC and CISA is critical to having a strong physical security program.

07 A physical security program is only as strong as its weakest link.

Enhanced physical security of your facilities not only protects you and your customers from potentially long outages but also helps take steps to secure the overall North American interconnected electric grid. In many cases the investments that are made for physical security enhancements to protect transmission facilities can be recovered through your Transmission Tariff or your Regional Transmission Organization (RTO) Tariff. Additional security enhancements on the critical facilities on the interconnected electric system are a win for all parties involved. ■

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

Dex Underwood, *Analyst*
GDS Associates, Inc. - Marietta, GA
770-799-2395 or
dex.underwood@gdsassociates.com