Introduction to Jetstream

PJM Interconnection

October 28, 2017

This page is intentionally left blank.

Introduction to Jetstream

Many assets participating in PJM markets are widely distributed making individual private network connections infeasible. Still, it is often necessary for these assets to have direct data communications to PJM. In these cases, the public domain Internet is used. PJM employs a string of technologies called the Jetstream system to enable the safe, secure and convenient transaction of data.

The network to convey the data is the public domain Internet. Any standard Internet service with acceptable levels of reliability, latency and bandwidth will be sufficient. In general, land lines tend to be less problematic than cellular, satellite and to a lesser extent DSL services, because of reliability and latency issues.

Security for PJM and members must include features for authenticity, integrity and confidentiality.

Authenticity is the capability of one party to be sure about who they are communicating with on the other end of an unsecure line. In this case, the Internet is the unsecure line. PJM makes provision for two-way assurance, which simply means both PJM and the PJM member is able to have high assurance about the identity of the party they are communicating with.

Integrity is the assurance that the data received from a party hasn't been compromised or altered while in route. Integrity is achieved with the use of something called hashes, where the correct data is distilled down into a small unique piece of data which is practically impossible to replicate with incorrect data.

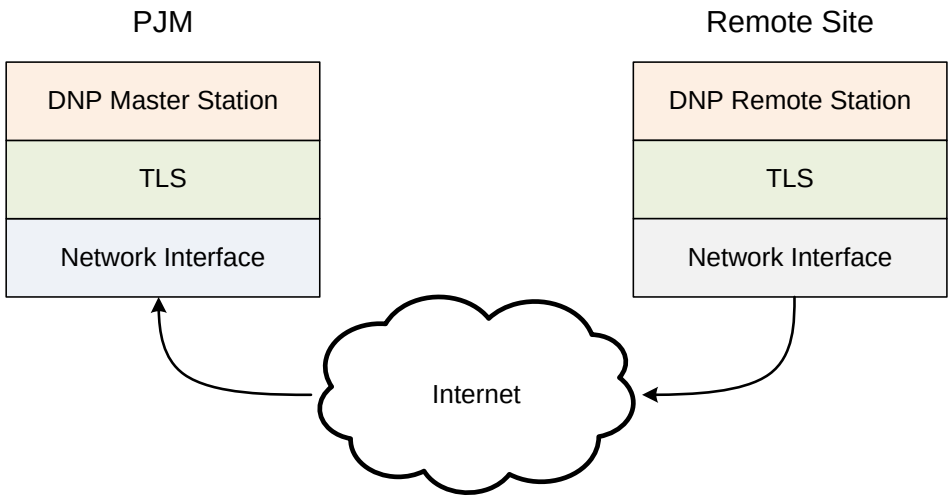
Confidentiality is the capability for two parties to exchange data without any other unauthorized parties being able to read the data while in route; this is achieved by encrypting the data.

The security protocol chosen to provide these features is Transport Layer Security.

Over the secured network connection, the PJM and remote site electronic devices must speak the same language to convey useful information. PJM uses the Distributed Network Protocol to communicate with remote sites.

Transport Layer Security

TLS, which is closely related to Secure Sockets Layer, is one of the most common protocols for securing Internet data exchanges. It is most commonly used when performing personal banking or other sensitive transactions online, and the Web server connection changes from http: to https:, which indicates the generic http Web traffic has been secured with TLS or SSL. Similarly, PJM uses TLS to secure standard DNP3 traffic.



Public Key Infrastructure

Fundamental to understanding everything TLS can offer is the idea of a Public Key Infrastructure. For simplicity of illustration, PJM may be considered a server, since many remote stations will be making connections to PJM. A connecting remote site may be considered a client. Another entity, the Trusted Third Party, completes the PKI.

The primary device of a PKI is a certificate. A certificate is a digital document that, among other things, testifies to the identity of a party. A certificate can be checked with the authority that electronically signed it. Both PJM and the connecting site will use a certificate to complete the data link.

PJM has chosen Open Access Technology International, Inc. to act as the TTP, in that they will be the Certificate Authority and Registration Authority in the PKI. That means OATI will sign and issue certificates to parties that register with them. OATI has been chosen because of their unique position to serve electric industry companies.

When a site connects to PJM to initiate DNP communications, it uses its trust in OATI to check the PJM certificate and be sure it has legitimate identification. Likewise PJM will use its trust in OATI to verify the remote site's certificate. During the initial "TLS handshake" when the data link is started, this verification and the technical details of the link will be settled between PJM and remote site devices. Ultimately, this will result in a secure channel for communications between the remote site and PJM.

Distributed Network Protocol

DNP is one of the most common electric utility industrial protocols. Many vendors have products with built-in support for DNP and it is an open standard so user implementations are also possible.

DNP is based on simple transactions between a master station and a remote station. PJM is the master station and therefore sends command data and requests input data. The remote station replies in kind.

The data transacted in DNP is defined by specific data types but has no contextual meaning. In other words, an out-of-band list of the data must be shared and agreed upon by PJM and a connecting member. This usually takes the form of a simple spreadsheet document. The Data Map will be used to locate where the command data and input data is for both parties use.

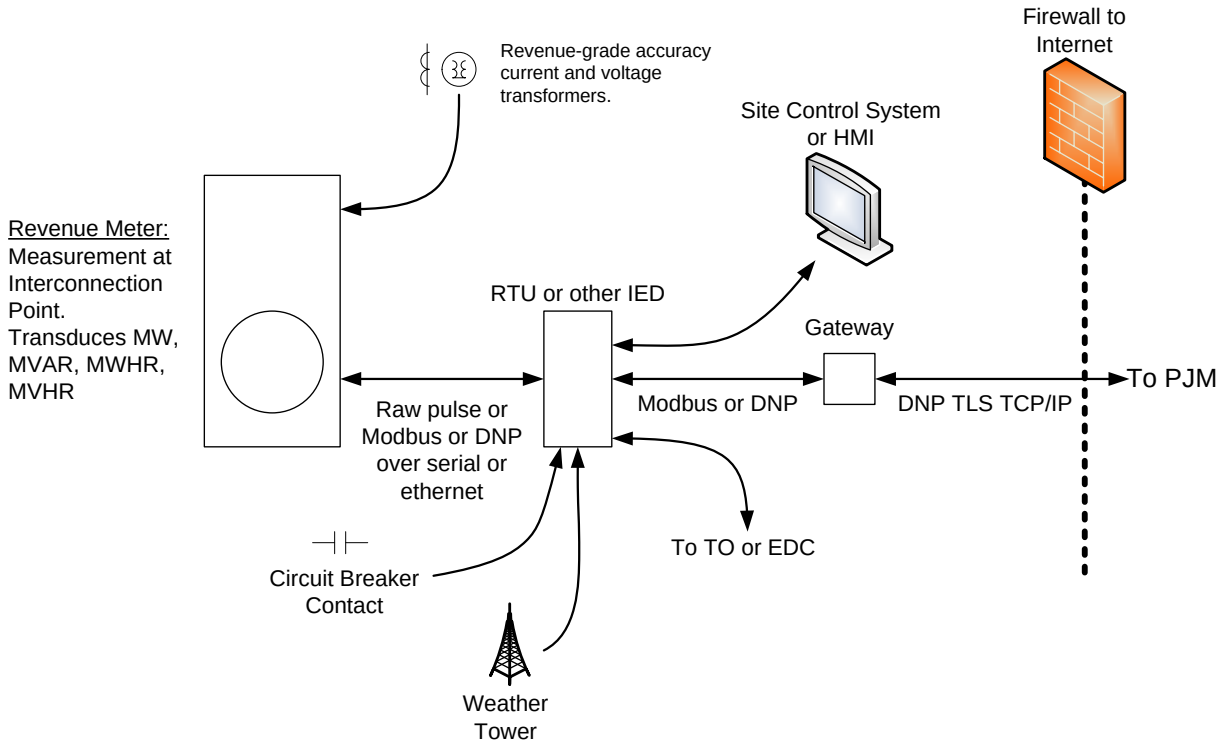
Behind the DNP Device

The design and installation of the telemetry services at a facility has many determining factors. PJM, the local Transmission Owner, and the facility itself will each have requirements that need to be met.

PJM Manuals and the project Interconnection Service Agreement will both contain specific guidelines of what kind of data is to be delivered. There are relevant standards for accuracy and reliability as well.

Basically, PJM needs to transact enough data to support the asset in the markets it is intended for, and to support the PJM model of the transmission system for reliability. Therefore, the markets the asset enters, and how the unit is modeled by PJM, largely determines the required data exchange. Each site and project is to some degree unique.

The data exchange requirements then will determine what data needs to be available on the site DNP device, and therefore what is behind the device. Some common examples are revenue meters, circuit breaker contacts or higher level devices like control systems.



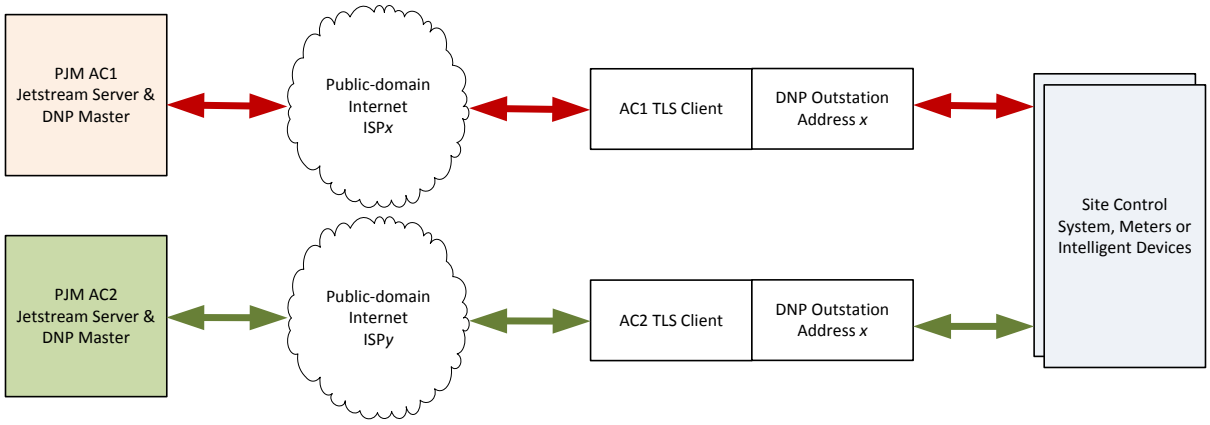
Remote Intelligent Gateway

The device or software that provides the TLS software to interface with PJM servers may be referred to as the Remote Intelligent Gateway or RIG. To better serve members PJM has chosen layers of technology that are open source. It is possible and intended for there to be options regarding how a member can procure or create a RIG.

PJM has published certification and testing documents that can be used to verify a device is capable of interfacing with PJM Jetstream servers. Devices or software that has been vetted by PJM through the prescribed tests are also published. In this way, there is a small market from which members can procure the best device for their circumstances. In some cases a member may be able to develop their own RIG, but decision to undertake the effort will have to be weighed against the associated risks and costs to all parties.

Dual-Connecting

All Jetstream links are dual-connected. The site will connect to and communicate with the PJM AC1 control center and PJM AC2 control center simultaneously. A high degree of redundancy and reliability is provided. PJM receives data from the site and the site receives setpoints from PJM from two independent data paths. Any interruption or failure specific to one of the data paths will not have operational or market impacts. The site has many options in regards to how and to what degree the redundancy should be implemented.



Steps for Establishing a DNP Internet Data Link with PJM

1. Confirm you need a link. There must be data you are required to send to or receive from PJM. Assets or aggregations representing greater than 100 megawatts of generation or load response capacity are usually designated to use a private network called PJMnet rather than the Internet. The project's PJM Client Manager or Interconnection Coordinator should be consulted.

2. Include telemetry in your project schedule and design. Establish the source for each data point and the data requirements of all parties. Particularly pay attention to boundaries between devices owned or installed by different parties, making sure all devices have a common way to interoperate. Select and include a RIG in the overall design.

3. Plan for installation and testing. PJM can generally create a link within three to six business days of finalizing the DNP data exchange, assuming the remote site is prepared. Testing can be done in phases: initial RIG testing for network and authentication testing, initial DNP testing to exchange simulated data, and finally actual telemetry tests including real asset operational performance. Each test phase may take considerable time, depending on the complexity and quality of the resource.

4. After commissioning, the asset telemetry should be supported 24/7 according to the site owner's and operator's policies and PJM guidelines. This process at minimum would include protecting the physical and electronic perimeter around telemetry equipment, keeping a 24/7 contact person or persons for technical response, maintaining network health and similar activities.