Next-Generation Communications Protocols for Advanced Smart Grid Applications

A GTM Research Whitepaper
# TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 3

2 NETWORKING CHALLENGES BEYOND THE SUBSTATION 4

2.1 Architectural Differences 4

2.2 Automated Metering Infrastructure 5

2.2.1 Smart Meter Data Overload 6

2.2.2 Sizing Network Infrastructure Deployments 6

2.2.3 Metrics for Success: Bandwidth and Beyond 6

2.3 Distribution Automation 7

2.3.1 Prioritization, Accuracy, and Reliability 8

2.3.2 Speed 8

2.3.3 Operator Notifications 9

3 COMMUNICATIONS SOLUTIONS 9

3.1 Standards-Based Communications 9

3.2 Aggregation, Sorting, and Prioritizing Raw Data 9

3.3 Network Monitoring and Self-Healing 10

3.4 Meeting Security Requirements 10

4 DESIGNING COMMUNICATIONS NETWORKS TO SUPPORT MULTIPLE SMART GRID APPLICATIONS 11
1 EXECUTIVE SUMMARY

The number of endpoints on utility-owned machine-to-machine (M2M) networks continues to balloon, reaching from tens of thousands to millions of devices. The constant collection and transmission of information from these points is taxing utilities’ ability to manage networks, utilize data, and ensure cost-effective network access for protection and control applications. Standards-based networking protocols and management software can provide effective means of mitigating this challenge through more efficient routing and prioritizing of real- and near-real-time data to reduce bandwidth constraints, reliably deliver data, create actionable intelligence, and ensure value realization across the electrical system.

A variety of smart grid applications demand robust communications capabilities that span across a wide range of often conflicting requirements. Many utilities are addressing this issue by creating entire networks to operate a single application. At the extreme, GTM Research has even heard of utilities making use of as many as a dozen different communications networks to manage various utility operations. However, this business model will ultimately prove to be too expensive for the bulk of electric utilities. Instead, utilities need to identify communications requirements and challenges in order to determine when certain applications can share a particular utility network to reduce the total cost of ownership (TCO) and increase the return on investment (ROI).

This whitepaper will examine communications challenges that are now facing utilities deploying private communications infrastructure to support automated metering infrastructure (AMI) and distribution automation (DA) applications. It will conclude with a discussion of solutions and best practices that utilities should consider while planning AMI and DA communications deployments.
2 NETWORKING CHALLENGES BEYOND THE SUBSTATION

For decades, utilities have had the ability to communicate to substations through telephone lines, supervisory control and data acquisition (SCADA), and serial connections. Over the last several decades, fiber to the substation and various wireless communications technologies have become increasing popular options. In the past, utilities connected communications to a few devices in the substation. The value proposition and regulatory mandates pushing AMI and DA technologies are forcing many utilities to provide communications beyond the substation, greatly expanding their area and complexity of communications coverage. These networks are also tasked with servicing an ever-increasing number of endpoints and AMI and DA applications to improve utility operational efficiency, each with its own requirements, native protocols, and priorities. Serving these endpoints results in a host of technology and application specific challenges.

2.1 Architectural Differences

Different communications architectures create different challenges for network operators based on network topology, policy, and desire for redundancy. Utilities should base their network choice on factors such as geographic topology, bandwidth, latency, redundancy, and the scope of management activities they expect to carry out.
2.2 Automated Metering Infrastructure

AMI has a variety of specific characteristics that present challenges to the effective management of its communications and head-end systems. The biggest challenges an AMI network faces include controlling and utilizing waves of meter data, building AMI networks to scale, and meeting important requirements including bandwidth, latency, throughput and reliability.
2.2.1 Smart Meter Data Overload

Twelve data points are collected from traditional meters every year. Even the simplest AMI system collects roughly 365 data points for each meter every year. More granular systems can record reads as often as every five minutes, resulting in up to 105,192 meter data points per year for a single meter. Total network traffic generated from a meter communicating every 15 minutes with advanced applications enabled could range 137 Mb-479 Mb per year. Some of this traffic consists of headers, which identify the beginning and the end of a particular message while in transit. Aggregations of hundreds of thousands and even millions of these meters are resulting in utilities being forced to manage a magnitude of data that vastly exceeds their past experience. This data can be utilized to improve ROI through better network management, streamlined billing processes, reduced power losses due to theft, and improved grid planning among other applications. On the other hand, failure to tame this data represents lost value and will significantly lower ROI.

2.2.2 Sizing Network Infrastructure Deployments

Creating and meeting proper requirements to scale AMI communications networks is an important step in network planning. Properly scaling network capacity to meet bandwidth, latency, and read reliability can mean drastically changing a utility’s business case. Anecdotal evidence has indicated that it is not uncommon for utilities to have to install 50% more network infrastructure than originally planned to attain reliable communications. The addition of endpoints to collectors for demand response, distribution automation, or home area network information (as AMI and MDM deployments mature) can further tax AMI networks, requiring additional communications infrastructure.

2.2.3 Metrics for Success: Bandwidth and Beyond

AMI network requirements are a function of a utility’s plans to utilize AMI. A utility focused strictly on streamlining the billing process and eliminating the need for meter readers will require less frequent meter reads, along with less bandwidth and throughput than a utility that wants to leverage AMI networks for Volt/VAR optimization, to aggregate and analyze voltage events or momentary outages, or to populate a customer web portal that updates on a daily or more frequent basis.
Figure 2-2: AMI Network Requirements

<table>
<thead>
<tr>
<th>METRIC</th>
<th>BASIC AMI</th>
<th>HIGH FUNCTIONING AMI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Low compared to telecommunications, but due to millions of endpoints, sizable bandwidth is still required</td>
<td>Additional bandwidth required for on-demand meter reads, load control, possibly home area networks (HAN), and for additional advanced metrics</td>
</tr>
<tr>
<td>Latency</td>
<td>Required latency for AMI is fairly high, as billing processes are not particularly time-sensitive</td>
<td>On-demand meter and voltage reads require response times of 15 seconds or less</td>
</tr>
<tr>
<td>Throughput</td>
<td>Large daily data dumps push network and put the stress of multiple reads on networks during low traffic periods</td>
<td>Additional functionality can require prioritization of messages to ensure timely arrival</td>
</tr>
<tr>
<td>Reliability</td>
<td>High reliability is a requirement to reduce truck rolls, ensure efficient billing processes, and reduce stress on Visualization Estimating and Editing applications</td>
<td>Reliability is more important as utilities lean more on AMI data to accomplish high-level tasks</td>
</tr>
</tbody>
</table>

Source: GTM Research

2.3 Distribution Automation

Distribution automation requirements often vary more widely than do those related to AMI. Latency tolerance, throughput utilization, and security needs vary from application to application. These varying requirements create difficulties when trying to utilize a single network for all of these applications.

Figure 2-3: DA Communications Requirements by Application and Device

<table>
<thead>
<tr>
<th>DA COMMUNICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application/Information Source</td>
</tr>
<tr>
<td>Volt/Var Optimization</td>
</tr>
<tr>
<td>Automated Line Switching</td>
</tr>
<tr>
<td>Advanced Asset Management</td>
</tr>
<tr>
<td>DG/EV on a circuit</td>
</tr>
<tr>
<td>Bellwether Meter for VVO</td>
</tr>
<tr>
<td>Sensors</td>
</tr>
</tbody>
</table>

Source: GTM Research, Department of Energy
2.3.1 Prioritization, Accuracy, and Reliability

Monitoring information and commands from and to automated switching and Volt/VAR control endpoints allows utilities to remotely re-route power away from downed power lines and line workers performing maintenance, to re-energize areas without power, and to reorganize and lower system-wide loading. These actions promote safe utility operations, ensure high service reliability, and help to manage the health of expensive utility assets. Communications from these mission-critical protection and control applications cannot be delayed or corrupted.

2.3.2 Speed

Latency is an important measure in many distribution automation applications. AMI deployments can typically provide significant benefits with latencies far in excess of five minutes. In DA applications, that latency falls below five minutes for almost all applications, but the requirements can be as tight as under 100 milliseconds (ms).

Automated switching requires by far the lowest latencies, demanding that devices in the field coordinate operations of switching devices on critical feeders in less than 100 ms without any action from grid operators to limit the extent of an outage. However, to be considered a momentary outage restoration services must be accomplished in less than five minutes for many utilities in the United States and less than three minutes at many European utilities. Past these periods, outages are deemed permanent rather than temporary. Across most of Europe and in 20 U.S. states, utilities can be assessed penalties for poor reliability most often measured by the frequency and duration of permanent outages.

Other DA applications do not have the same performance requirements as of yet, but the continued growth in distributed generation and electric vehicles will change that in high penetration areas. As these disruptive devices become more popular in local settings, latencies on small bandwidth M2M communications will have to shrink to allow for fast, coordinated action between a variety of line equipment when transient voltage events and major shifts in local supply and demand occur to prevent equipment damage.

2.3.3 Operator Notifications

Managing prioritized alerts that account for conditions reported at individual and multiple sensors will be difficult for utilities familiar with far smaller networks and far less data collection requirements. Parsing out specific negative conditions and prioritizing these alerts to optimize utility management actions will rely on a combination of advanced protocols, analytics, and utility configuration.
3 COMMUNICATIONS SOLUTIONS

Proper networking protocols can provide strong support to help mitigate many of the challenges associated with AMI and DA applications. These protocols can incorporate standards, help perform preliminary processing, help monitor and optimize network reliability, and incorporate varying security features for different applications.

3.1 Standards-Based Communications

By using standards-based communications protocols, the flexibility and longevity of the network can be enhanced. Utility communications should be compliant with TCP/IP and UDP/IP to allow the utility to make use of the widest variety of standards, including IEEE 61850 and DNP3 (whether IPv4 or IPv6). Compliance with IP will also ease developers’ concerns regarding the creation of new applications and process modeling. Providing an IP-based solution also eases concerns about multi-vendor network interoperability for electric utilities.

3.2 Aggregation, Sorting, and Prioritizing Raw Data

The use of protocols and head-end systems to aggregate and filter data can lower data processing requirements, transform data into useable intelligence, and improve network functionality. Filtering aggregate data into smaller representative samples reduces how much stress is applied to servers, as utilities use data for real-time analysis and ad-hoc data mining. Utilities can organize data into a more useful form, using filters to improve network operations. Filters can also be set up to recognize and create alerts for various negative network conditions such as failed meter reads, loss of collectors, or unsuccessful commands.

The critical protection and control aspects of distribution automation applications require either siloed networks to ensure reliability or the ability to prioritize network traffic. Within a network handling multiple applications, critical communications must pass through the network without being lost, slowed, or corrupted. The importance of these communications to ensure the safety of line workers and the public and the protection of the health of key grid systems is paramount.

3.3 Network Monitoring and Self-Healing

Adopting the proper protocols and tools to monitor network performance and allow for rapid network self-healing will be key to maintaining high performance under non-optimal conditions. When equipment fails for natural or mechanical reasons, holes are left in any communications system. Planning and protocols can mitigate the impact of this lost coverage. Redundant infrastructure is costly, but can prevent service loss. Distributed intelligence of centralized communications analysis can shift communications paths, reallocating traffic through active network devices to free up capacity near a communications outage event in order to reestablish communications with at least some of the lost devices. Distributing this intelligence to local nodes can automate the process, leading to less downtime and improved reliability.
3.4 Meeting Security Requirements

Network security is an important consideration in any smart grid deployment. The addition of communications technologies and control functionalities to traditionally isolated grid equipment raises concerns among utilities, regulators, and consumers. The National Institute for Standards and Technology (NIST) has laid out many of these challenges and provided a vision of secure networks for utilities to strive for while designing cybersecurity plans. However, lack of specific directions to get to that goal leads utilities to develop their own plans to secure their utility networks for various applications while keeping the general framework from NIST in mind. The features of these plans must be adjusted to account for differences between applications.

AMI data is non-critical in nature, but confidentiality, accuracy, and customer presentment concerns provide the impetus to limit access. The use of encryption, authentication of operators, authorization of various tasks to various groups, and accounting for any manual changes to AMI data become important security measures to ensure smooth interactions with customers. Authentication can incorporate any combination of username and password identification and physical verification, such as a simple key or fingerprint scan. Restrictive authorization only provides employees access to data relevant to their job function, preventing tampering or accidental corruption of data. Accounting and assigning all actions to particular employees allows utilities to track any changes and determine if a mistake has been made and who is responsible in the event of corrupted data.

DA requires additional security measures, as these protection and control functions alter how distribution networks are configured, as well as the behavior of the electricity that is delivered to the customer. Ensuring the integrity of messages to and from distributed control equipment is paramount to identifying and reacting to incomplete and tampered communications. As with AMI encryption, authentication, authorization, and accounting are also important to be able to limit access and the ability to negatively affect the network.

1 For more information on NIST’s vision of cybersecurity see NISTIR 7628.
4 DESIGNING COMMUNICATIONS NETWORKS TO SUPPORT MULTIPLE SMART GRID APPLICATIONS

Communications requirements are becoming more important as utilities attempt to derive more value from new and existing networks by attempting to carry additional applications. Designing networking requirements to address challenges, including future proofing, data management, real-time analytics, network health, and security, can greatly reduce the operational risk and improve efficiency associated with a new communications network. Addressing these concerns and adopting best practices will be key for utilities that in the United States alone will be spending hundreds of millions of dollars to roll out additional networks for M2M communications.

The use of advanced protocols and improved network management middleware can address and reduce many of these concerns by:

- Utilizing standards based communications
- Prioritizing network traffic
- Performing correlative analytics to simplify alerts, which will improve utility response
- Reducing downtime in the event of device error or other negative network conditions

Robust communications and ease of network management can reduce the cost, the number of operators required, and the headaches associated with increased data from smart grid applications and networks. Over the next five years, the demands on many utilities' communications will increase by more than an order of magnitude as additional communications points are added and additional functionality of hardware, such as smart meters, is enabled. How utilities plan and address these dynamics will shape the ROI of all of their communications deployments.