Smart Grid Operations and Control Center Design – Vision vs. Reality

Stan Pietrowicz, Tom Mazzone, Andrew Mayer

Telcordia Technologies, Inc.
331 Newman Springs Road
Red Bank, NJ 07701

spietrow@telcordia.com

Keywords: Smart Grid Operations, Network Operations Center (NOC), Distribution Management, Smart Meter Management, Energy Management Center (EMC), Advanced Meter Infrastructure (AMI), Smart Meter (SM), Distribution Automation (DA)

Abstract

The Smart Grid, with its explosion of distributed intelligence, field automation, remote sensors and its deluge of new endpoint data, is driving the functional integration of new Distribution Management capabilities into existing Energy Management Centers. Business benefits include greater efficiencies, more productive operations, improved service reliability, better asset management and more insightful system planning. This paper discusses the value of taking a holistic, yet realistic view, of managing intelligent endpoints, communications networks, Smart Grid data and operations. Moreover, it asserts that taking an end-to-end approach to Distribution Automation (DA) and Smart Meter (SM) operations design will better realize Smart Grid benefits. Factors, such as data, systems, processes, people and security, especially at early stages of a project, are given consideration. This paper illustrates the value of exploiting data from seemingly disparate systems for the Advanced Meter Infrastructure (AMI) to support operational needs in security, reliability, safety, network management, theft deterrence, customer service and vendor management. This paper makes six recommendations to help utilities maximize the potential of Smart Grid capabilities: 1) integrate Smart Grid AMI and DA capabilities into current operations by employing a holistic approach, 2) analyze the command and monitoring capabilities of endpoints and network equipment from an operations and security standpoint, 3) plan and integrate AMI and DA operations into existing distribution energy management operations during project deployment, 4) include management of the Field Area Network (FAN) communications infrastructure into the operations center integration, 5) cover the domains of a holistic approach in the Plan-Design-Build-Operate stages of the Smart Grid Lifecycle, 6) exploit the data's potential for improved reliability, safety, efficiency, security and other business benefits.

1. INTRODUCTION

The Smart Grid, with its explosion of distributed intelligence, field automation, new remote sensors, and its deluge of endpoint data is a strong stimulus for functional integration of new Distribution Management capabilities into existing Energy Management Centers. This paper focuses on the need to holistically integrate the management of new Smart Grid capabilities deployed in the electric distribution network into utility operations and control centers. Specifically, this paper focuses on AMI and DA.

2. THE SUPPORT INFRASTRUCTURE

Both AMI and DA introduce a new breed of intelligent devices enabled by a heterogeneous, two-way communication network. Major AMI components include Smart Meters, access nodes, field service equipment and element management systems. DA components include a variety of automated controls and new sensors on feeder lines, pole-based equipment and substations. Examples of DA components include automated reclosures, capacitor banks, sectionalizers and switches, faulted circuit indicators, feeder meters, smart transformer regulators, automatic restoration equipment and substation computers. Other Smart Grid components in the distribution network that may be under the control of utilities include distributed solar and wind generation systems, related wind and solar sensors, direct load control infrastructure and electric vehicle charging/management systems.

In addition to the physical power assets, it is important to recognize that distribution infrastructure also includes the various operations support systems that monitor and control the field equipment. These systems are the Meter Data Management Systems (MDMS), Energy Management Systems (EMS), Distribution Management Systems (DMS) and even micro DMSs.

Linking the physical assets together with the operations support systems are a multitude of FANs. Some FANs

employ wired technologies, such as SONET and traditional telecom transmission systems that are either privately owned or leased from a communications provider. Most new FANs at the edge of the distribution network use wireless technologies. While some wireless FANs are standards-based, the majority employ proprietary radio technologies and protocols. Each device in the FAN needs to be managed, secured, and monitored, presenting new operations and security challenges.

3. THE DATA DELUGE AND EXTRACTING VALUE

In AMI, DA and FAN deployments, each new intelligent device and communications support will generate state, condition, and event information. Each will process commands from back-end systems for control actions affecting the power network or communications network. As the number of devices grows to hundreds of thousands and millions, the result is an unprecedented volume of data not previously encountered or managed by a utility. Today's utility operations processes and control centers are not designed to accommodate this volume of data, nor do they have the capability to process and react to the new types of information being received. New operations management processes and workgroup functions are needed in Energy Management Centers to turn the data deluge into meaningful business and operations information.

Why is this deluge of data important and what's its promised value? The potential to improve network reliability, reduce operations expenses (OPEX) costs, integrate renewable energy resources, offer more flexible energy services, and support emerging energy applications, such as electric vehicles, in an environment that will become increasingly competitive with many new entrants in the energy value chain, is significant and will continue to grow over the decade.

Let's examine AMI as an example to understand what types of data need to be processed. The most obvious category of AMI data are usage measurements. Typically, this is the first to be addressed by a utility's billing processes as part of the meter-to-cash business flow. A second category of data is for automated operations, such as remote connects and disconnects. Both of these data categories are associated with customer support and the meter provisioning process.

A third category of data from AMI systems is the state and state change data about the electrical energy sensed at the meter. This information is valuable to distribution management operations to better understand the operating conditions in the distribution plant and support actions to control power quality, such as circuit tap changes, which has become a frequent operation on circuits with high penetration of photo voltaic systems. AMI state data is also needed by outage restoration management to identify customers who are without power and manage work force activities.

A fourth category of AMI data that is often overlooked is the state and health information of the metering infrastructure itself, such as network connectivity, network performance, latency, network routing, access node utilization, and traffic statistics. This information is valuable to telecom, radio and network planning engineers who need to monitor daily network conditions and track long term trends, optimize network performance, allocate bandwidth or control quality of service, diagnose network or endpoint communications problems, re-engineer field networks to improve coverage, and update their network models for signal propagation. It is also needed by the Information Technology (IT) groups to better schedule application and network traffic to reduce congestion and latency in bandwidth-constrained AMI FANs.

A fifth category of AMI data is security-related information, which includes both information needed to maintain the network's security controls, such as key provisioning and periodic updates, authentication and password management, but also security monitoring information, such as security log reporting and detection of anomalous events. This information needs to be integrated into the cyber and physical monitoring activities of physical and information security.

In general, most of this information is new to organizations and for personnel who may be familiar with it; the huge volume of data is new and often overwhelming. Most utilities are familiar with the rudimentary aspects of these data. For example, SM usage data drives billing and customer services. The usage data must be collected, screened for immediate problems, the proper response provided, and then the data must be forwarded to the billing and customer records processes. The raw data are then stored for future use. There may be value in normalizing the data before parsing it to make the data more easily used by other systems.

Similar categories of data exist for DA data, which reflects how the distribution network is running, its health, and the quality of the electrical service being provided to customers. Because DA equipment is inherently more control and sensor oriented, command automation and monitoring, security, and communications network performance are most critical. Supervisory Control And Data Acquisition (SCADA) and DA data supports distribution network operations centers to monitor systems, open breakers and activate switches, etc. Information about the equipment states, changes in states and predetermined actions taken by the equipment, and health of the equipment should undergo analysis by local control center personnel and systems and

not just stored for the future as is being done by many utilities today.

Who understands what the data are really telling us? What could the data tell us if we knew what to ask and how much more could the data tell us if it is combined with data from other operations processes? Who is skilled enough to know what other data to combine it with? Where do these knowledgeable people work and can we move them and their analyses tasks to an integrated work center or control center so they will have easy access to the various data and more easily discuss ideas with technicians in adjacent operations areas?

If it is impractical to move these personnel, how do we give them access to the DA, AMI and FAN data, or a more important question, how does the utility re-engineer processes and work priorities to give this data analysis activity a higher priority to really make it happen? Work priorities may need to be changed; new tasks and responsibilities may need to be assigned to processes, work groups and individual. Most importantly, it has been long recognized by transformation practitioners that an executive sponsor should be assigned to the project or any such culture change is doomed to struggle for years with inadequate resources.

4. A FEW OF THE CHALLENGES TO ADDRESS

Today, most utilities focus too much on Smart Grid technology itself to the exclusion of other aspects that are just as critical to the success of their Smart Grid vision. It is common today to find AMI operations and its data analysis an orphan looking for a home in which to be accepted and integrated. Similarly, the management of the FAN operations is not well recognized as a critical part of asset management and EMS operations and need to find a home either in EMS centers or IT NOCs, which are typically responsible for the general communications networks. Even if utilities see the value of fully integrating IT and Operation Technology (OT) domains, they may not have the skills or budget to do so at the time of deployment. It is important to build these operations capabilities in a timely manner regardless of where the responsibility is eventually assigned. Telcordia has found through many similar operations center consolidations in several industries that the return on investment from efficient operations and data analysis can be quickly realized.

Several utilities in the latter stages of their Smart Meter deployments have realized that AMI and DA systems are not an "install it and forget it" proposition. AMI systems, for instance, require constant attention to maintain proper system operation, address equipment and communications alarms, support field staff, reconcile failures of automated processes in MDMSs, and handle the unexpected events associated with any new technology that is being deployed in volume for the first time. To address these needs in the short term, some have tactically reorganized work groups outside of their energy management centers to provide support. Typically, these groups report up through an Information Technology organization rather than System Operations. Consequently, AMI operations and management is functionally and often organizationally separate from distribution and energy management operations.

Does the processing of this new AMI and DA data with its high volumes and its correlation with data from other operations domains fit into established work centers? Do existing work centers want the work, see the value in it, and can they add resources to cover the added work load? In many utilities, the answer is no or they are still studying how to best address the opportunities and issues. Inadequate resources are one of the initial challenges faced along with the knowledge and capabilities of the existing staffs. However, process change, or to be more direct, culture change is also a significant challenge.

5. TELCORDIA'S OPERATIONS PLANNING RECOMMENDATIONS

Telcordia makes the following recommendations with respect to planning Smart Grid processes and operations and designing control centers based upon experience working with leading Smart Grid utilities and performing work center re-engineering with clients in other industries.

5.1. Recommendation 1

To properly integrate Smart Grid AMI and DA capabilities into current operations, take a holistic view of the introduction of the new technology early in the planning lifecycle stage before deployment is started or the technology's full potential may be missed. Often utilities will have to expend considerably more resources to integrate the functionality in the later lifecycle stages. There are six critical aspects to introducing new technology that must be addressed to ensure success:

- **Technology** – Understanding the technology's capabilities and limitations are critical for success and generally addressed by utilities. Considering the Total Cost of Ownership and not just the initial deployment costs are critical because equipment deployed in the grid typically has a long lifespan. The technology's OPEX savings potential, ease of interfacing with other systems and the ease of maintenance are as critical as the technology's basic functionality.

- **People** - Understanding the stakeholders involved in the existing and new processes and addressing their responsibilities and needs, are critical to successful Smart Grid deployments. How similar or different are the operations, management and maintenance tasks of AMI and

DA systems from current equipment and how will people have to interact with it? Is leadership and project sponsorship sufficient to effectively introduce the necessary changes? Understanding goals is key because it will drive employees' behavior. Does the change brought about by the new technology have clear goals the employees can understand? What training will work centers and technicians need to truly understand how to operate the technology to its fullest potential?

- **Data** - Data is the language the technology speaks and the data can tell us more about the equipment, its operations and its health over time as we understand how correlate it with data from other operations areas and realize value from it.

- **Processes** - Processes are important to the business and should be addressed and understood by employees before Smart Grid deployment. Much evidence in the electric and other industries shows that process execution acumen is a Critical Success Factor. A structured and comprehensive methodology should be followed to re-engineer processes to the extent needed to exploit the capabilities of the new technology. Changes to processes should be addressed early in the lifecycle. Processes should be documented to a sufficient level for the maturity of the organization. A common refrain from field teams is, "Don't just tell us what we can't do; show us what we should be doing, provide us the guidelines, then let us do it." A well-proven process will minimize work-arounds and produce results that are less likely to circumvent policy.

- **Systems** – Automated systems are a necessity for handling complex activities and the large volume of both operations and security related tasks. Systems introduce their own set of complexities and systems are often interfaced with other systems introducing more complexities. Ideally, management and control systems should be selected to mechanize the processes the utility has designed. Of course, there must be some compromise when selecting Off-the-Shelf systems to avoid customization costs. The key is striking the right process, employee and financial balance. A structured methodology should be used to get it right the first time.

- **Security** – To best implement security, build it in and validate it during the planning and selection phases rather than try to add it during or after deployment. First, define your Smart Grid security requirements, which should cascade down from your information security and physical security policies and support your application and operations use cases. Consider technical, procedural, contractual controls, not only for the technology, but also for your operations, services and vendor-hosted solutions. Specify your security requirements when seeking a vendor solution and evaluate their ability to deliver from day one. Consider defining Service Level Agreements (SLAs) with vendors. Clearly distinguish between present-day versus future roadmap capabilities. Validate claimed security capabilities through hands-on security and vulnerability testing using testing scenarios that are traceable to your security requirements. While paper security analyses are useful, they are insufficient to base a deployment and must be followed by hands-on testing.

Be proactive and realistic about your security needs and policies. Consult standards and monitor industry direction, but do not wait for industry standards to solidify. Each utility who has a security program probably better understands its own security needs than a standards body that is trying to balance multiple interests. Standards often lag behind user needs and industry best practices. While standards may offer a framework, they are not a detailed recipe for a security solution. Security remains both a science and an art that must be customized to achieve both application and business goals. Furthermore, do not stand behind a "culture of compliance." Compliance with North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) requirements does not guarantee security, only that regulation has been met. Instead, adopt a culture of "cyber security responsibility."

5.2. Recommendation 2

Analyze the command and monitoring capabilities of endpoints and network equipment from an operations and security standpoint. Identify important information to monitor and gather from chatter and map each element to one or more operational processes. New intelligent endpoints and network equipment support hundreds of commands and can generate huge volumes of events, but not all of which are meaningful to a particular utility's operations. Bandwidth limitations preclude the "pack rat" approach of reporting and backhauling everything. Even if it were possible, important data may go unrecognized because it is buried deep in the noise. Instead, utilities need to investigate the reporting capabilities of each type of endpoint and each network element. Utilities need to understand what information Smart Meters and other Smart Grid equipment are reporting and decide which of the hundreds of commands, events and information elements are useful and important data sources for its operations.

Furthermore, as part of the system integration process and ongoing tuning of its operations, utilities need to map data to their operational processes. First, data needs to be aligned to support existing processes, replacing older sources of data and redefining portions of existing processes so that normal business operations can continue. But equally important, data needs to be aligned with the planning and definition of new processes to support operations that are enabled by data that was not previously

available. These processes may be driven top-down by new business applications, but they can also be driven bottom-up by those who with the insight of how to apply the data to solve a business need. Utilities can exploit the power of this data by understanding the types of data received by the various FAN devices, what they are telling us and what more they could tell us if we properly designed the processes to receive, correlate and analyze these data with data from other operations processes and to properly assign these operations management and data analysis activities to control centers and work groups. The approach taken by many today to collect data and simply store it in massive and ever-growing databases is a futile attempt to compensate for the lack of proper process and operations integration.

5.3. Recommendation 3

Plan and integrate AMI and DA operations into existing distribution energy management operations during project deployment. If this is not practical, develop a clear roadmap with intermediate objectives, activities and necessary resources to successfully reach each objective. A long-term cost-benefit analysis with realistic and insightful assumptions to achieving intermediate milestones for integrating new functionality and data correlation capabilities into targeted NOCs along with re-engineering processes is key. A well understood, documented and approved technology introduction roadmap is a valuable tool to ensure Smart Grid projects align with the utility's vision.

5.4. Recommendation 4

Include management of the FAN communications infrastructure into the operations center integration. FAN communications needs to be managed like a critical power asset. The primary enabler of Smart Grid is communications and should it fail, a utility's ability to maintain situational awareness and stay in control of a dynamic Smart Grid would be seriously jeopardized. FAN monitoring should be part of a work group in the utility's distribution and energy management centers. While maybe difficult to believe at this stage, there may come a time when priorities shift from getting power restored to first getting communications restored.

Pursue achieving situational awareness not only in the power grid, but in your FANs. This requires planning, selection, and deployment of tools and support systems to obtain visibility into FANs and to manage communications elements. This includes network inventory systems, network monitoring and service assurance software, security management and correlation tools, intrusion detection systems (IDS), and configuration and policy compliance tools.

FANs are now integral to the distribution network and they should not be managed as an adjunct responsibility by a detached organization. FANs should be managed as an integrated Smart Grid asset.

5.5. Recommendation 5

Cover the six domains of a holistic approach in the Plan-Design-Build-Operate stages of the Smart Grid Lifecycle:

- **Plan** – During the planning stage, include not only the technology requirements to properly accommodate the new equipment, but also all the processes, systems, data, security and people requirements. Identify which operations processes will be impacted and plan appropriate changes early. Prepare for downstream testing and integration during the planning stage and account for all interfaces and data flows needed downstream.
- **Design** – Apply a holistic approach when designing the architecture, writing the requirements, engineering the networks and designing the test cases.
- **Build** – Address the six domains while deploying the equipment and its FANs. Test deployments against established acceptance criteria. Introduce the AMI and DA capabilities and data correlation and analysis into the processes and add consider employee training which may be needed.
- **Operate** – "Plan your work and work your plan" is the old adage. Document policies and processes for the Smart Grid clearly and provide adequate guidelines for field personnel to follow and adapt for their environments.

5.6. Recommendation 6

Exploit the power of data – This paper has discussed the value the data being received from the various AMI and DA components and the value of correlating it with other operational areas. To exploit the data's potential for improved reliability, safety, efficiency, security and other business benefits, plan for capabilities to analyze and interpret data early in the Smart Grid Lifecycle. It may require more planning and resources initially but the results promise to be worth the investment. Apply AMI and DA data to support other business areas such as security operations, revenue assurance, asset management and more. AMI data can provide more than usage and billing functionality. For example:

- Build or add capabilities to obtain visibility into FANs, such as AMI networks, to support communications monitoring and analysis, security, diagnostics, meter engineering and telecom engineering, even if the FAN is operated as a Managed Solution. On the very surface, it does appear prudent to deploy a large FAN

for which the asset owner has limited to no means to observe the operation of its network. Such means, if built or sourced independent of the FAN vendor, can help mitigate the growing issue of supply chain cyber security risk.

- Build or add data analytic capabilities that combine AMI data with information from other systems and work centers to address business needs. For example:

  - **Asset Management & Reliability** – Analyzing AMI state information with equipment lot numbers, geographic and environmental information can identify problems and predict premature equi**pment failures. This will assis**t utilities move from a "run-to-failure" asset management approach to a prognostics and conditioned-based maintenance operation.

  - **Security** – Integrate AMI, DA, and FAN condition and state data with security monitoring and intrusion detection work center activities to more quickly detect and assess security anomalies and intrusions in these networks and respond appropriately.

  - **Revenue Assurance** – Detect power theft and illegal activities that harm the network and minimize unpaid account losses through correlating AMI data with billing, customer account and provisioning information without dispatching a technician.

6. CONCLUSION

AMI and DA deployments introduce a large number of intelligent devices with increased operations capabilities and needs. All of these devices are rich with commands and can generate numerous and different types of data. Proper planning and integration of processes and data will help improve operational efficiencies, service reliability, safety, and security. Several recommendations are given to optimize the potential benefits:

- Take a holistic view of Smart Grid infrastructures early in the planning lifecycle stage before deployments begin. If this step is omitted, a utility may miss the technology's full potential and often have to spend considerably more to integrate the functionality post-deployment. Telcordia believes there are six critical domains of the business that must be addressed to ensure success: Technology, Data, Processes, Systems, People and Security.

- Integrate management of Smart Grid infrastructure into distribution and energy management centers to maximize the benefit of an intelligent and flexible electrical system. If full integration is not practical or desired, ensure that all functionality and data analysis is addressed in purpose-build operations centers and interface this new operations center with existing NOCs.

- Manage FAN communications like a critical power asset. Include FAN communications management in your process planning and operations center integration. Communications is the nervous system of the Smart Grid.

- Take a holistic approach in all Lifecycle stages: Plan-Design-Build-Operate.

- Exploit the power of data – AMI and DA devices and their communications FANs provide a wealth of data. Plan for the data analysis capabilities early in the lifecycle. Seek benefit from correlating AMI and DA data with data from other business areas.

Biography

Stan Pietrowicz is a Senior Principal Security Consultant in the cyber security practice of Telcordia Technologies. With 20 years of combined experience in the Communications, Smart Energy, and Intelligent Transportation sectors, he is responsible for business development, project management, technical delivery and research. Working for Bellcore and now Telcordia since 1990, Stan's presents focus is Smart Grid security and operations where he pioneered the security assessment of Advanced Meter Infrastructures and received the Telcordia's first Chief Operating Officer (CEO) Award for Innovation in 2011. Stan also manages security research for FAN security and conducts research in Intelligent Transportation Systems and vehicle communications. Stan received his MSEE from Rutgers University and BEEE from Stevens Institute of Technology.

Dr. Andrew J. Mayer –
Dr. Andrew Mayer is a Principal Systems Engineer in Telcordia Advanced Technology Solutions. With over 24 years at Telcordia, he is a leading expert in service and network management and operations for broadband technologies and Next Generation Network (NGN) services. In the government sector, Andy led teams that formulated the Net-Centric Implementation Guidelines for the integrated enterprise management of the multi-domain Global Information Grid, and most recently on applying Policy Based Enterprise Management to satellite communications (SATCOM) Services and Network Perimeter Defense. He helped drive the development of management standards in the Asynchronous Transfer Mode (ATM) Forum, Digital Subscriber Loop (DSL) Forum, Digital Audio Video Council (DAVIC), International Telecommunications Union-Telecommunications Standardization Sector (ITU-T), Tele Management Forum,

and Metro Ethernet Forum (MEF). He is currently active in the MEF serving as liaison to the TeleManagement Forum (TM) Forum, editor of the Carrier Ethernet Management Information Model, and technical lead for the Dynamic Responsive Ethernet initiative. He is also involved in the TM Forum's Defense Interest Group and Ethernet Service Management Team. Dr. Mayer holds a BS from Purdue University, as well as a MS and Ph.D. from Stevens Institute of Technology.

Tom Mazzone is a Principle Solution Architect with Telcordia Technologies' Advanced Technologies Solutions responsible for project management, customer solution architecture, process design and reengineering for cyber security, utility smart grid, telecom operations process and software development process quality improvement services. Tom has over 30 years experience in telecommunications network management, provisioning and maintenance systems engineering, operations processes and re-engineering, interconnection regulation and global number portability program development. Tom has 5 years experience with Pacific Bell in various network and operations management positions including switching systems and outside plant equipment maintenance operations control centers. Tom holds a Project Management Professional (PMP) certification from PMI and is ITILv3 Foundation Certified.

Telcordia – Telcordia has over 27 years of experience planning, designing and protecting critical infrastructure and large, complex networks. As a leading global provider of engineering and security services, fixed, mobile, and broadband communications software, and cutting-edge research, Telcordia serves a broad spectrum of communications-intensive markets. Working with a broad range of clients in government, communications, military, finance, energy, automotive, and entertainment, Telcordia has a unique perspective on current and future network needs and best practices. In recognition of Telcordia's role in architecting our nation's communications infrastructure, Telcordia is a member and trusted advisor to the President's National Security Telecommunications Advisory Committee (NSTAC). The NSTAC provides technical and policy advice to assist the President and other stakeholders who are responsible for our nation's critical national security and emergency preparedness services.