

Successful Smart Grid Architecture

Even as the smart grid comes together, utilities must consider factors such as data sources, models and security to ensure long-term success.

www.UtilitiesProject.com

The smart grid is progressing well on several fronts. Groups such as the Grid Wise Alliance, events such as Grid Week, and national policy citations such as the American Recovery and Reinvestment Act in the U.S., for example, have all brought more positive attention to this opportunity. The boom in distributed renewable energy and its demands for a bidirectional grid are driving the need forward, as are sentiments for improving consumer control and awareness, giving customers the ability to engage in real-time energy conservation.

On the technology front, advances in wireless and other data communications

envisioned it would be proud. But to avoid making a gooey mess in the oven, an overall architecture that carefully considers seven key ingredients for success must first exist.

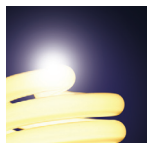
SOURCES OF DATA

Utilities have eons of operational data: both real time and archival, both static (such as nodal diagrams within distribution management systems) and dynamic (such as switching orders). There is a wealth of information generated by field crews, and from root-cause analyses of past system failures. Advanced metering infrastructure (AMI) implementations become a fine-

devices (IEDs) and other smart grid devices. In an era of renewable energy sources, grid connection controllers become yet another data source. With renewables, micro-scale weather forecasting such as IBM Research's Deep Thunder can provide valuable context for grid operation.

DATA MODELS

Once data is obtained, in order to preserve its value in a standard format, one can think in terms of an extensible markup language (XML)-oriented database. Modern implementations of these databases have improved performance character-



ON THE TECHNOLOGY FRONT, advances in wireless and other data communications make wide-area sensor networks more feasible.

make wide-area sensor networks more feasible. Distributed computation is certainly more powerful – just consider your iPod! Even architectural issues such as interoperability are now being addressed in their own forums such as Grid Inter-Op. It seems that the recipe for a smart grid is coming together in a way that many who

grained distribution sensor network feeding communication aggregation systems such as Silver Springs Network's Utility IQ or Trilliant's Secure Mesh Network.

These data sources need to be architected to be available to enhance, support and provide context for real-time data coming in from new intelligent electronic

istics, and the International Engineering Consortium (IEC) common information/generic interface definition (CIM/GID) model, though oriented more to assets than operations, is a front-running candidate for consideration.

Newer entries, such as device language message specification – coincidence-ordered subsets expectation maximization (DLMS-COSEM) for AMI, are also coming into practice. Sometimes, more important than the technical implementation of the data, however, is the model that is employed. A well-designed data model not only makes exchange of data and legacy program adjustments easier, but it can also help the applicability of security and performance requirements. The existence

WRITTEN BY

Jeffrey S. Katz – IBM

Jeffrey S. Katz is the chief technology officer for the Energy and Utilities industry at IBM. He is involved with the application, development and innovation of IBM products, services, technology and research for electric power companies and related organizations. Katz has worked on the industry's strategic growth case, the IBM Innovation Jam workshops, the IBM Intelligent Utility Network initiative and is the primary industry liaison with IBM Research.

of data models is often a good indicator of an intact governance process, for it facilitates use of the data by multiple applications.

COMMUNICATIONS

Customer workshops and blueprinting sessions have shown that one of the most common issues needing to be addressed is the design of the wide-area communication system. Data communications architecture affects data rate performance, the cost of distributed intelligence and the identification of security susceptibilities.

There is no single communications technology that is suitable for all utilities, or even for all operational areas across any individual utility. Rural areas may be served by broadband over powerline (BPL), while urban areas benefit from multiprotocol label switching (MPLS) and purpose-designed mesh networks, enhanced by their proximity to fiber.

In the future, there could be entirely new choices in communications. So, the smart grid architect needs to focus on security, standardized interfaces to accept new technology, enablement of remote configuration of devices to minimize any touching of smart grid devices once installed, and future-proofing the protocols.

The architecture should also be traceable to the business case. This needs to include probable use cases that may not be in the PUC filing, such as AMI now, but smart grid later. Few utilities will be pleased with the idea of a communication network rebuild within five years of deploying an AMI-only network.

Communications architecture must also consider power outages, so battery backup, solar recharging, or other equipment may be required. Even arcane details such as “Will the antenna on a wireless device be the first thing to blow off in a hurricane?” need to be considered.

SECURITY

Certainly, the smart grid’s purpose is to enhance network reliability, not lower its security. But with the advent of North American Reliability Corp. Critical Infrastructure Protection (NERC-CIP), security has risen to become a prime consider-

ation, usually addressed in phase one of the smart grid architecture.

Unlike the data center, field-deployed security has many new situations and challenges. There is security at the substation – for example, who can access what networks, and when, within the control center. At the other end, security of the meter data in a proprietary AMI system needs to be addressed so that only authorized applications and personnel can access the data.

Service oriented architecture (SOA) appliances are network devices to enable integration and help provide security at the Web services message level. These typically include an integration device, which streamlines SOA infrastructures; an XML accelerator, which offloads XML processing; and an XML security gateway, which helps provide message-level, Web-services security. A security gateway helps to ensure that only authorized applications are allowed to access the data, whether an IP meter or an IED. SOA appliance security features complement the SOA security management capabilities of software.

Proper architectures could address dynamic, trusted virtual security domains, and be combined not only with intrusion protection systems, but anomaly detection systems. If hackers can introduce viruses in data (such as malformed video images that leverage faults in media players), then similar concerns should be under discussion with smart grid data. Is messing with 300 MegaWatts (MW) of demand response much different than cyber attacking a 300 MW generator?

ANALYTICS

A smart grid cynic might say, “Who is going to look at all of this new data?” That is where analytics supports the processing, interpretation and correlation of the flood of new grid observations. One part of the analytics would be performed by existing applications. This is where data models and integration play a key role. Another part of the analytics dimension is with new applications and the ability of engineers to use a workbench to create their customized analytics dashboard in a self-service model.

Many utilities have power system engineers in a back office using spreadsheets; part of the smart grid concept is that all data is available to the community to use modern tools to analyze and predict grid operation. Analytics may need a dedicated data bus, separate from an enterprise service bus (ESB) or enterprise SOA bus, to meet the timeliness and quality of service to support operational analytics.

A two-tier or three-tier (if one considers the substations) bus is an architectural approach to segregate data by speed and still maintain interconnections that support a holistic view of the operation. Connections to standard industry tools such as ABB’s NEPLAN® or Siemens Power Technologies International PSS®E, or general tools such as MatLab, should be considered at design time, rather than as an additional expense commitment after smart grid commissioning.

INTEGRATION

Once data is sensed, securely communicated, modeled and analyzed, the results need to be applied for business optimization. This means new smart grid data gets integrated with existing applications, and metadata locked in legacy systems is made available to provide meaningful context.

This is typically accomplished by enabling systems as services per the classic SOA model. However, issues of common data formats, data integrity and name services must be considered. Data integrity includes verification and cross-correlation of information for validity, and designation of authoritative sources and specific personnel who own the data.

Name services addresses the common issue of an asset – whether transformer or truck – having multiple names in multiple systems. An example might be a substation that has a location name, such as Walden; a geographic information system (GIS) identifier such as latitude and longitude; a map name such as nearest cross streets; a capital asset number in the financial system; a logical name in the distribution system topology; an abbreviated logical name to fit in the distribution management system graphical user inter-

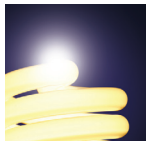
face (DMS GUI); and an IP address for the main network router in the substation.

Different applications may know new data by association with one of those names, and that name may need translation to be used in a query with another application. While rewriting the applications to a common model may seem appealing, it may very well send a CIO into shock. While the smart grid should help

data coming into the utility will be increasing exponentially. As more meter data can be read in an on-demand fashion, data analytics will be employed to properly understand it all, requiring a sound hardware architecture to manage, back-up and feed the data into the analytics engines. In particular, storage is needed in the head-end systems and the meter-data management systems (MDMS).

memory access speed and range; server and power supply reliability; file system redundancy such as a JFS; and techniques such as FlashCopy to provide a point-in-time copy of a logical drive.

Flash Copy can be useful in speeding up database hot backups and restore. VolumeCopy can extend the replication functionality by providing the ability to copy contents of one volume to another.



HEAD-END SYSTEMS PULL DATA from the meters to provide management functionality while the MDMS collects data from head-end systems and validates it.

propagate intelligence throughout the utility, this doesn't necessarily mean to replace everything, but it should "information-enable" everything.

Interoperability is essential at both a service level and at the application level. Some vendors focus more at the service, but consider, for example, making a cell phone call from the U.S. to France – your voice data may well be code division multiple access (CDMA) in the U.S., travel by microwave and fiber along its path, and emerge in France in a global system for mobile (GSM) environment, yet your speech, the "application level data," is retained transparently (though technology does not yet address accents!).

HARDWARE

The world of computerized solutions does not speak to software alone. For instance, AMI storage consolidation addresses the concern that the volume of

Head-end systems pull data from the meters to provide management functionality while the MDMS collects data from head-end systems and validates it. Then the data can be used by billing and other business applications. Data in both the head-end systems and the master copy of the MDMS is replicated into multiple copies for full back up and disaster recovery. For MDMS, the master database that stores all the aggregated data is replicated for other business applications, such as customer portal or data analytics, so that the master copy of the data is not tampered with.

Since smart grid is essentially performing in real time, and the electricity business is non-stop, one must think of hardware and software solutions as needing to be fail-safe with automated redundancy. The AMI data especially needs to be reliable. The key factors then become: operating system stability; hardware true

Enhanced remote mirroring (Global Mirror, Global Copy and Metro Mirror) can provide the ability to mirror data from one storage system to another, over extended distances.

CONCLUSION

Those are seven key ingredients for designing or evaluating a recipe for success with regard to implementing the smart grid at your utility. Addressing these dimensions will help achieve a solid foundation for a comprehensive smart grid computing system architecture. ■

WEBLINK

More information and additional material can be found online at:
www.utilitiesproject.com