

a Call to Action



A Call to Action

Realizing the U.S. Smart Grid

Imagine 25 years from today a world where the Smart Grid exists everywhere. There will be literally hundreds of millions of smart electric meters installed as well as thousands of micro grids developed in our communities all across the country with local grid controllers. An entire generation of children will have grown up with plug-in hybrid electric vehicles in their garages. In fact, they are probably driving the family “clunker” PHEV.

THESE AND OTHER INTERMITTENT resources such as photo voltaic arrays, wind farms, etc. have sprouted up all over the landscape to help mitigate the ever rising cost of energy. Imagine all these new devices, all with microcontrollers at their core, harmoniously communicating and interacting with each other keeping the Smart Grid functioning.

Even with all these new technologies in place on the electric power grid, it is credible to believe that substations probably will still exist and protection and control devices will still be in place to provide operational safety and security just as they do today. Imagine more sophisticated devices than today, and probably more autonomous, but still there performing a similar function. So we end up with more devices on the grid, controlling the operation, millions of them, with microcontrollers operating at their core.

A different scenario

If you don't believe this scenario, consider the implications of the Energy Information and Security Act 2007 – Title XIII – Smart Grid

and the various state public utility commissions that have encouraged rate recovery for advanced metering installations that are providing utilities significant motivation to move forward with the smart grid.

Now imagine the challenges in managing the smart grid. The Eastern Interconnection is often touted as the largest machine in the world. Just think of the massiveness of the smart grid communications network that will ultimately connect all the devices in the east along with the west and all of North America. It is simply mind boggling.

Security issues

Now think of the playground this communications network provides for hackers that enjoy playing around in this kind of space to see what they can do. This new and vast communications network that will be necessary to handle the data, information, microgrid control signals, metering, customer turn on / off, outage information, demand response signals, etc., all moving around this network.

With so many devices listening for actions to respond to and other devices constantly issuing

commands for other devices to act upon the need for security, authentication, trust, etc will be paramount.

Security of this network will need to be extremely tight. Today's hackers get enjoyment out of messing up your desktop PC or overwhelming a corporate e-mail system. This results in lower productivity for a day or two.

The smart grid network, if not properly secured, will provide hackers with a much more widely visible end result if they are successful and consequences much more dramatic than a video display acting peculiar of an e-mail server overloaded (I'll let you imagine these consequences on your own). Network and system management tools will need to be developed to provide smart grid operations staff the ability to monitor, configure and manage these devices similar to how PCs are managed today with the utmost attention paid to the entire security spectrum.

Today, when a microprocessor based relay needs to have its firmware upgraded a field engineer typically needs to visit the site, take

Paul Myrda is a technical executive at the Electric Power Research Institute. He is a graduate of the Illinois Institute of Technology with a MSEE in Power Systems and an MBA from Northwestern University – Kellogg Graduate School of Business. He joined EPRI in 2007 and is responsible for activities related to the transmission system including smart grid, protection and synchrophasors. Previously, he was employed at major US utility companies.

New smart grid network management tools should be developed.

the device out of service, connect a laptop to the relay and upgrade the firmware, re-test the device and then return the unit to service. This is an unlikely scenario 25 years from now for a long list of reasons but the manpower requirements alone would be unrealistic.

So what does this smart grid look like in the future?

First there will be a vast communications network, probably IP based but heterogeneous in physical makeup. This is not very

challenging and exists in many areas today but the security aspects and service level requirements of different devices will be. The mix of critical control signals and non-critical data streams coming out of the same device and flowing over the same communications path will greatly impact the business processes needed.

For example, suppose you have a multi-function relay that has synchrophasor and protection capability in a single IP connected device. It may easily provide critical data to control systems such as an EMS or a wide area protection scheme and also various asset management or maintenance management systems.

Planning a device outage will entail not only the power system operations staff but also the smart grid operations IT staff to make sure the loss of data to other devices

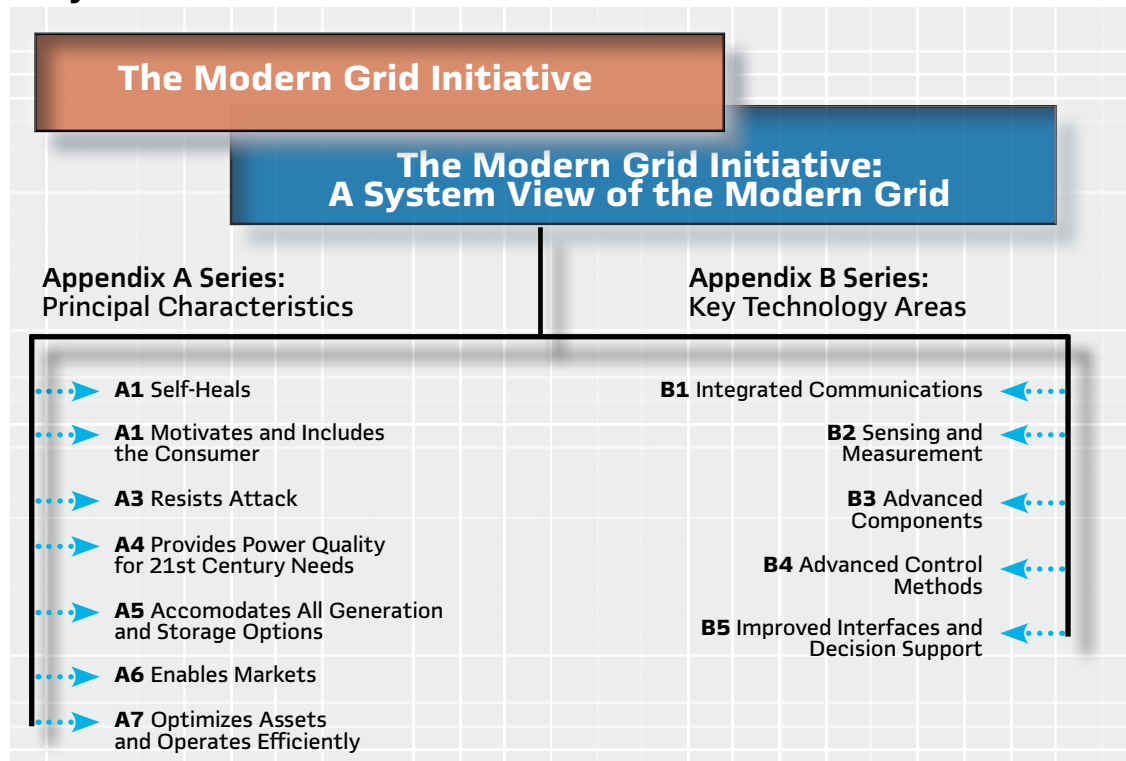
or systems does not impact them adversely. Also, the mixing of critical control signals and non-critical data streams would require messaging prioritization capability and reliable network latencies to assure that control signals get through the traffic successfully.

New smart grid network management tools will need to be developed that are similar to the tools used to manage the IT network today such as HP Openview or IBM's Tivoli. These tools provide the visibility, control, and automation necessary to manage the smart grid network.

Key functions of this tool set are:

- Device, network and server management – provides for efficient provisioning, configuration and monitoring of the smart grid infrastructure and ensure critical services are operating per service level agreements

1 v2.0 A Systems View of the Modern Grid



Note: v2.0 A Systems View of the Modern Grid
 Conducted by the National Energy Technology Laboratory for the U.S. Department of Energy.
 Office of Electricity Delivery and Energy Reliability
 January 2007.

The Smart Grid will be a large and complex system and everyone involved will need to work together to make sure that the entire system is safe and secure to operate.

■ **Security management** – establishes and controls access to smart grid resources and ensures compliance with established security policies

■ **Storage management** – backup and restore resources for smart grid storage devices that include both transactional and temporal data sources

■ **Asset management** – identifies and manages all smart grid device configurations, settings, maintenance schedules and performance history

■ **Application manager** – ensure smart grid applications are optimally performing and in accordance with service level agreements

Action plan

To effectively accomplish the functions described above the smart grid devices will need to be enhanced to handle capability similar to Simple Network Management Protocol (SNMP) agents. It is through these agents that services, like those described previously, get accomplished today in the IT community.

At the recent T&D Exposition held in Chicago, IL, a paper was presented by Frances Cleveland on IEC 62351-7 where she highlighted the recent work in the area of Network and System Management of the information infrastructure being done under IEC TC 57. She pointed out that SNMP Management Information Base (MIBs) data is used to monitor the health of network systems but each vendor must

develop their own set of MIBs for their equipment. This is unlike common network equipment like routers, where standard MIBs can be applied.

Network issues

The lack of network tools is only one of the issues facing the smart grid. Let's get back to that vast communications network supporting the smart grid. It will most likely be heterogeneous in its makeup. In order to define what exactly it will look like, we need to answer many questions:

■ What will the interfaces need to look like?

■ What technology works best where?

■ How do I monitor this network to know that it is working?

■ What are the security requirements and how are they implemented and monitored?

■ Do end point devices need to be encrypted?

■ Should they be encrypted?

■ How does one know who did what when to any device on the smart grid.

■ How is the audit trail maintained?

■ How do we know if a device is configured properly?

■ How is configuration verified, by whom, how often?

■ How do I know if the end point device is authentic and not a fraud, replaced by another device?

This is just a brief list of questions that need to be answered in the future smart grid world. The good

news is that we do not have to start from scratch.

Where do we go from here?

Many of these questions have processes that can address them from other industries or even within our own. For many years now the information security world has abided by the core principles of confidentiality, integrity and availability. By leveraging the years of security development work in encryption such as AES128/256, authentication with public and private keys, assuring that no one person has the entire key and other such measures, secure environments are achievable. Securing this massive control network is not trivial and the impact of intrusions into the network will potentially have a more wide spread impact on people's lives.

The Smart Grid will be a large and complex system and everyone involved will need to work together to make sure that the entire system is safe and secure to operate.

The call to action though is now; before we have massive deployments of devices that will not comply with the future requirements or smart grid network management tools.

Other issues

So how do we attack these and other smart grid implementation issues?

One way is by working together to develop the solutions through the various standards bodies and industry forums. The smart grid will require teams of people from utilities, vendors and consultants

For many years the information security world has abided by the core principles of confidentiality, integrity and availability

Securing this massive control network is not trivial.

working together to address the issues. With pressure from our customers, regulators and the industry, time to develop solutions to the host of issues will require an uncanny level of collaboration and commitment. The not invented here syndrome will need to take a back seat and reaching across to other industries and internationally will be critical to our success. There will not be a more exciting time than now to get involved.

EPRI's efforts

In an effort to facilitate the issues related to implementing a smart grid, EPRI is developing a multi-site laboratory that will include microprocessor based

protective relays, synchrophasor measurement units (PMU), wide area communications network, historians, servers, GPS clocks from multiple vendors.

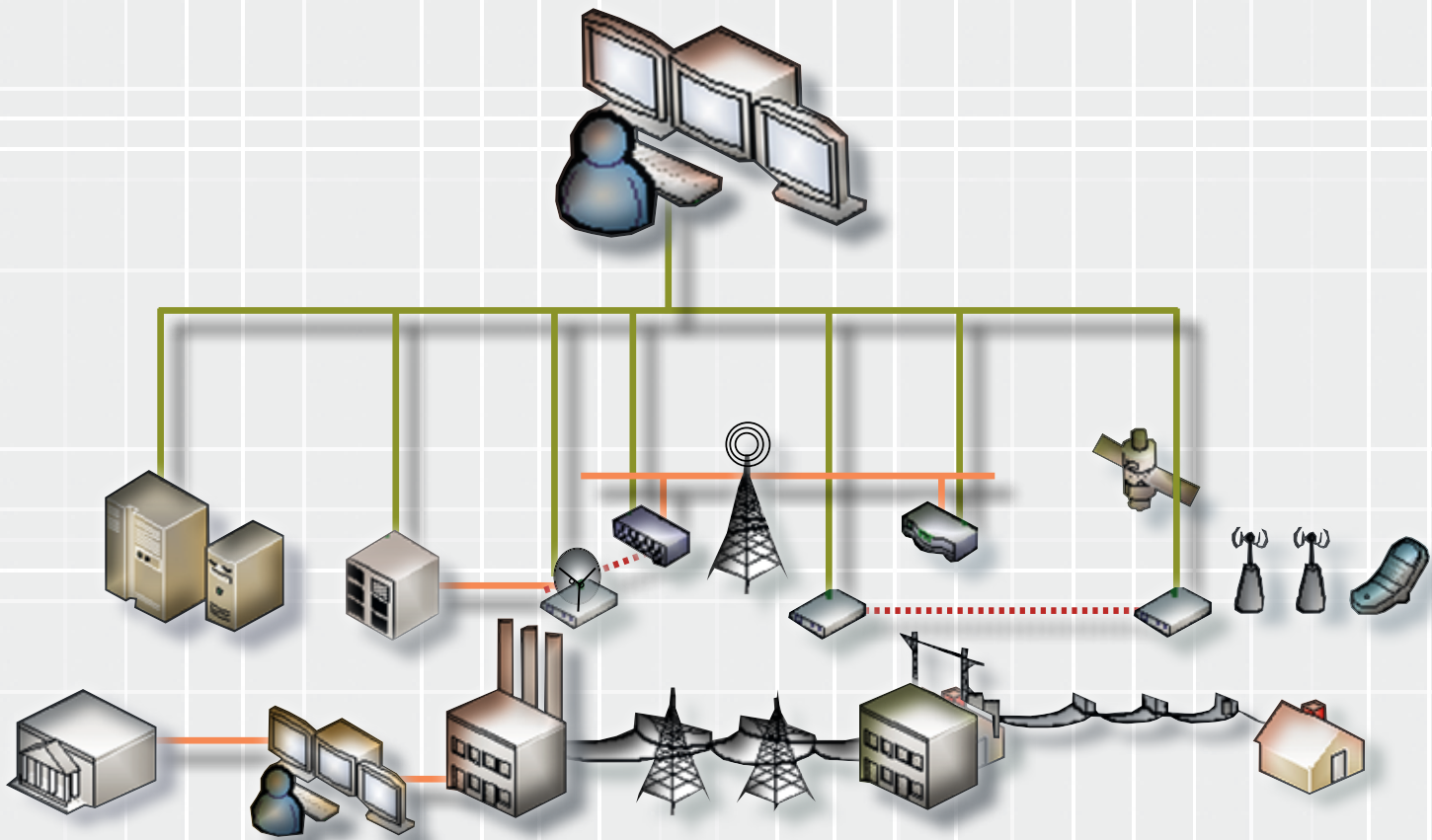
The labs will be located at our existing facilities in Knoxville, TN; Charlotte, NC, and Lenox, MA. The multi-site geography will provide some unique capability including wide area PMU measurement, wide area communications challenges especially for transmission class protection schemes and other geography induces issues.

The purpose of the laboratory is to provide a test bed for new ideas to address the many issues facing the smart grid. We expect to ultimately

Reaching across to other industries and internationally will be critical to our success.

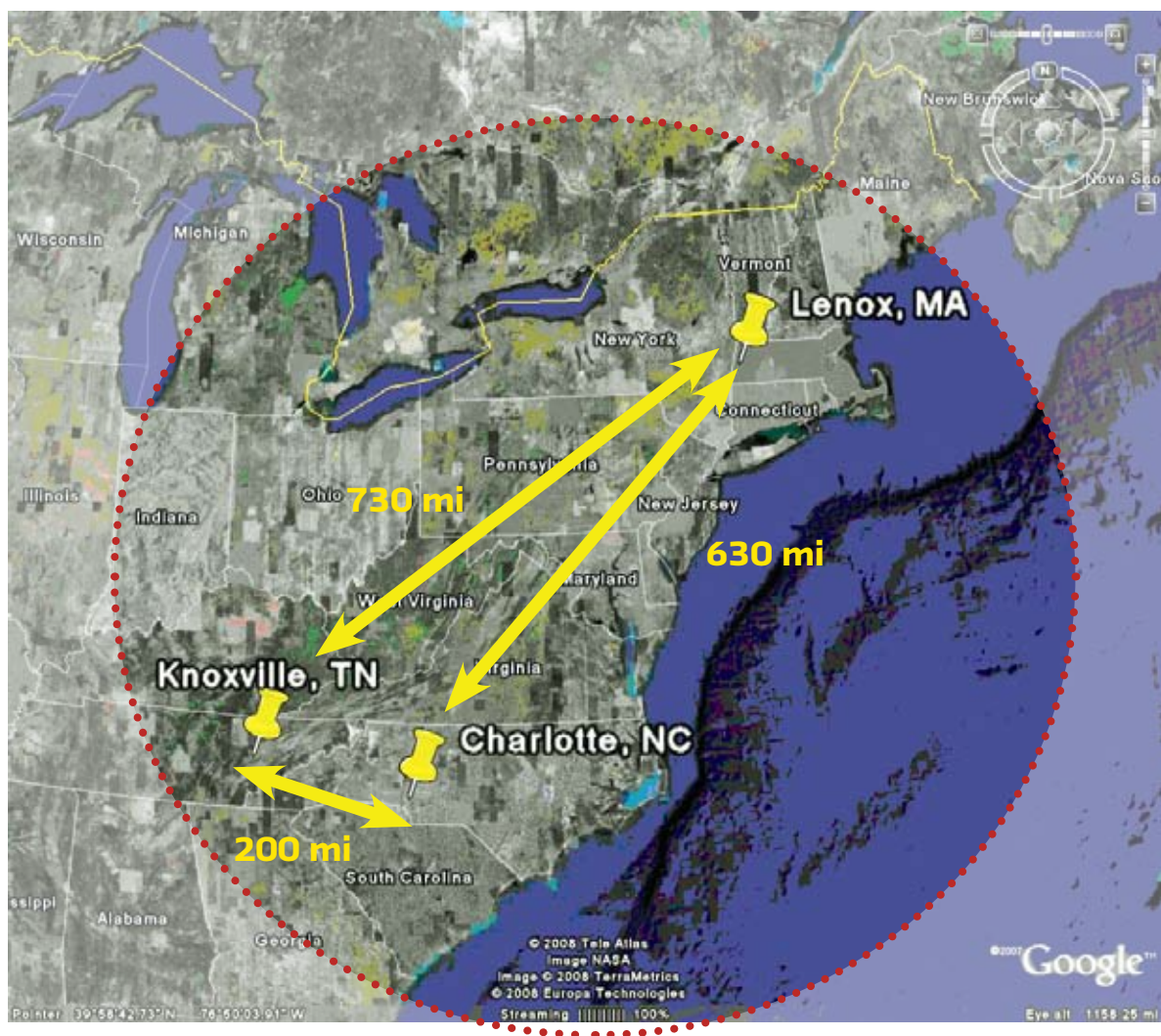
couple this facility with the existing "living lab" that primarily deals with end use devices. We expect to work jointly with both utility and vendor representatives on a variety of issues at the multi-site lab.

2 Smart grid communication and network management



Multifunctional Intelligent Electronic Devices, communications equipment and different software tools will be tested.

3 Multi site laboratories locations



Wide area phasor measurements and communications challenges can be addressed by the distributed laboratory.

EPRI's existing facilities in Knoxville, TN; Charlotte, NC, and Lenox, MA., USA.