



Smart Security for Smart Grid Programs

By Mark Cioni, Executive Consultant,
Enspira Solutions, Inc. , A Black & Veatch Company
Greenwood Village, Colorado USA

The strong industry focus on Smart Grid security over the past few years has resulted in a substantial evolution of the standards and guidance from relevant influencers including DOE, NIST and others. In essence, the industry has made very significant progress in the “What” and “Why” aspects of Smart Grid security. And, as most people who have been involved in a Smart Grid project will attest, it’s equally important to understand and execute on the “How” aspects of that security guidance. This article, based on a substantial number of AMI and Smart Grid implementations, attempts to focus on several key areas of program execution relative to Smart Grid security from an implementation perspective.

Although seemingly obvious and pragmatic, the areas that follow are too often marginalized to some degree during the Smart Grid program due to many contributing factors. Timing constraints on Smart Grid funding, internal resource constraints and even ignorance have been contributory on past programs along with other factors. Faced with the extremely small probability that any given Smart Grid program will occur under optimal circumstances, it pays to be aware of the following focus areas and to consider how to apply their lessons, regardless of where in the lifecycle a Smart Grid program currently resides.

- Choose More Security Involvement
- Nominate A Security Liaison Role
- Build and Deploy Securely From the Start
- Identify What Needs to Change

Choose More Security Involvement

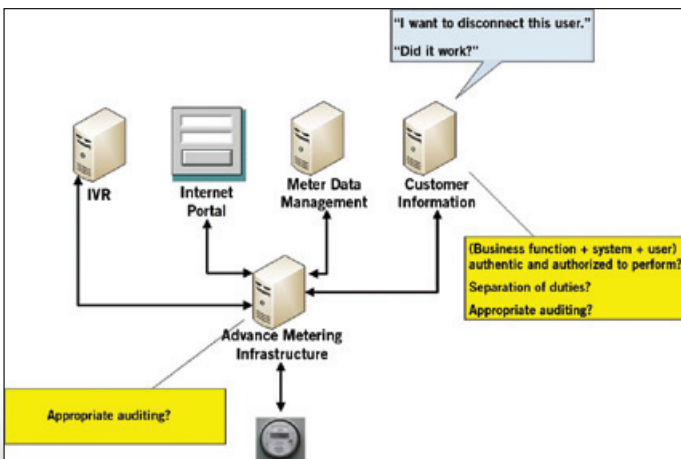
Engage security resources early and often. Although elegant in its simplicity, too often this practice is not applied and the appropriate security resources are not involved as broadly or often as necessary. Security casts a large footprint on a Smart Grid implementation program, and even though some critical areas are obvious, others may not be as straightforward. Smart Grid implementers don’t just need their security

resources to review firewall configurations, but rather to take an active role in a broad range of activities. Some of the most important of these are addressed in the following.

- **Business Case Development** – Security will most likely add a number of costs to the Smart Grid business case, including but not limited to acquisition costs for hardware, software, services and training, as well as ongoing costs associated with these items and others. Additionally, funding restrictions and other potential regulatory constraints mean the business case will likely need input and guidance from security resources relative to procurement and even cost allocation to the program and larger enterprise.
- **Cyber Security Planning** – Smart Grid investment funding is based on a number of core application criteria, the Cyber Security Plan being one of these that must be accepted before such funding is granted. Although fairly straightforward that security resources would be involved in the development of the Cyber Security Plan, the key takeaway is that these same resources would optimally apply that knowledge base to activities such as Conceptual Architecture, Vendor Selection, etc.

- Solution Architecture** – Even before Vendor Selection, a Smart Grid program would optimally start to develop a solution architecture that presents a series of aspects or views as to how that solution would interact at a logical level, the candidate platforms on which it will be deployed, how integration will occur, candidate Electronic Security Perimeters (ESP) and network enclaves, instrumentation points and management components, and many other architectural facets that must align with and incorporate security controls. The solution architecture will help to frame and codify the organization's vision, as well as to communicate that vision to vendors and partners.
- Process Refinement** – The instantiation of a Smart Grid solution will likely require the development of new business and operational processes, and refinement of existing processes as well. These processes may have both automated and manual elements that span multiple new systems. Security has an important role to play in these activities. Consider a simple example, yet one that causes worry for nearly every AMI implementer: Remote Disconnects.
- Vendor Selection** – A key engagement area for security resources, their expertise will help the organization to evaluate the security posture of candidate vendors and their offerings, as well as how well aligned their proposed solution will be with the organization's solution architecture vision. For example, whether candidate vendors follow a formalized Security Development Lifecycle, perform regular third-party testing and certification, and other best practices are important assessment criteria.
- Program Documentation** – Throughout a Smart Grid program, formal documentation is usually required that reflect the decisions and rationale around security designs, compensating controls, disaster recovery and resiliency mechanisms, security practices and other core solution aspects. Not only does such documentation need to be developed, but this information must also be protected appropriately both internally to the organization as well as relative to outside entities.

Although the implementer may already have an existing disconnect process, the ability to perform this operation remotely changes the landscape from a security perspective. Given this new capability, security resources should help the organization to evaluate which of their business and operational entities should be able to initiate this process, how to ensure separation of duties so that one entity (person) cannot shed load en masse, and alternatives for ensuring transactional closure (i.e. "We wanted to disconnect these 10 endpoints; how can we be sure that the operation completed correctly in a manner we can audit and prove, or if not what remedial action should we take?"), among others.



Your Source for High Voltage Test Equipment

...a wide range of test systems available!

AC Hipots
3 kV to 1 MV

Aerial Lift Test Sets

DC Hipots/ Megohmmeters
6 kV to 160 kV

Rubber Goods Test Systems

High Current Test Sets
up to 7,500 A frame breakers

Transformer Test Systems
Distribution or Power

Resonant Test Systems

On-Site GIL/GIS, Cable, Transformer Induced Test Systems

HIGH VOLTAGE

HIGH CURRENT

HIGH POWER

Contact us at
301-746-8118
INFO@phenixtech.com

75 Speicher Drive
Accident, MD 21520
USA

www.PhenixTech.com

30+ Years Experience

ISO 9001
CERTIFIED

Nominate A Security Liaison Role

Since security concerns and activities will likely influence broad areas of a Smart Grid program, ensuring consistent oversight is a key requirement. Very often, the organization's existing security resources cannot devote significant amounts of their time to the program, making consistent oversight challenging at best. The security liaison role doesn't necessarily need to be a full-time activity, however it needs to be engaged consistently throughout the program and fully involved during critical activities. This role should help to facilitate – relative to security – communication and cooperation

among vendors, individual project managers, application and business function owners, technical staff and program executives.

Build and Deploy Securely From the Start

Key areas of security concern are too often overlooked or buried in different project plans with little coordination. Although often unwieldy to place every program management activity in a single plan, there needs to be cohesion between individual plans within the Smart Grid program, where the detailed activities and tasks are in one plan and appropriate touch points and milestones are incorporated into other plans. Some

of the most important of these areas that usually span multiple project plans include:

- **Develop and Integrate the Security Project Plan** – The security project plan should be the central point for all security related activities – from firewall acquisition and configuration to creating enterprise directories – with logical touch points from and into other project plans within the Smart Grid program. For example, acquiring and configuring additional firewalls should articulate its activities, dependencies, resources and milestones within this plan, and incorporate appropriate influence and interdependent milestones from other project plans in the program. Likewise, those project plans should also reflect relevant milestones and interdependencies from the security plan.
- **Plan Multiple Environments** – Having multiple environments (e.g. Production, Disaster Recovery, Test, Development) for a Smart Grid deployment is nothing new and is a best practice in general. The key takeaway here is to ensure, with respect to pragmatic organizational constraints of budget, resources and others, that these environments can help to facilitate security posture and deployment in the solution. In other words, as much as feasible, make appropriate provisions to have Disaster Recovery, Test and Development environments that can accurately model the same security architecture (albeit perhaps at a reduced capacity in some cases) as Production.

Conserve your energy, let CPS protect your property.



CPS is your Green Security Technology Provider

- Live Video Surveillance
- Alarm Monitoring
- Fiber Optic Fence Line
- Structured Cabling



- Solar Options
- Time Lapse & Archiving
- Intelligent Video Analytics
- Security Officers & Trailers



Call for a FREE site survey/evaluation!
800-520-1742
sales@cpssecurity.com | cpssecurity.com

CA C7 825688 | ACO 6119 | C10 865761 | PPO 11094 | GA P5C001921 | NV 741 | AZ 1003939 | FL B2100148 | UT P1C2088 | TX C09819 | LA 531 | AR B2005-0080 | NM 2328

Additionally, provisioning a “Sandbox” environment has become increasingly common as an area for IT resources, including security, to perform certain types and levels of testing and proof of concept.

- **Harden First, Then Relax With Reason** – A fundamental best practice in security is to harden systems, networks and other infrastructure components first, and grant permissions only after that hardening is complete and tested. In many cases, there are several factors that may work against this practice within a Smart Grid program, including everything from vendor hardware and software installation to compressed timeframes. For example, the inability for product vendors to communicate simple requirements such as port numbers, protocols, source and destination systems and other hardening information is still much too common an occurrence.
- **Test Security Controls and Monitoring Early** – The design, deployment and testing of security controls, instrumentation components, and subsequent monitoring and management will be absolutely critical to long term solution viability. Unfortunately, these items are often deferred or reprioritized during project execution when in fact the opposite should happen. Not only do Smart Grid implementers want to have these items in place as early as possible in order to be able to appropriately test them, these items in fact can help facilitate the security development and testing of the rest of the solution.
- **Processes** – Probably the biggest area for potential change due to the influx of new processes and the extension of existing processes over multiple disparate systems. For example, with the potential advent of new field tools and platforms for AMI, does the organization need to refine its Mobile Device Lifecycle process and infrastructure such as mobile device security?
- **Organizational Capabilities** – A common area for change is the organization itself. What new or expanded roles will need to be created, and will those roles need specialized training such as CIP awareness, Linux administration and security, and others? Relative to process changes, what organizational security changes should support potential changes such as separation of duties, field service, key management and others?
- **Partners** – What changes are needed with respect to existing outside partners? For example, will the organization need to restrict permissions and expand auditing in various domains due to integration with new Smart Grid components? What changes, such as new systems and protocols, might be needed with security partners such as logging/scanning services, vulnerability/pen testers and others? Will the organization need to add new partners due to changes in policies, processes and capabilities?

The continuing evolution of standards and guidance relative to Smart Grid security is necessary and contributory to the entire industry. Smart Grid implementers should remember, however, that guidance is only as effective as the execution that accompanies it.

Identify What Needs to Change

The advent of a comprehensive security posture for a Smart Grid program will very likely give rise to the need to refine or instantiate changes in many areas of the enterprise. Although not a complete list of questions for consideration, some of the most common security changes driven by a Smart Grid program include:

- **Policies** – In many cases, security influences on existing policies drive appropriate refinements. For example, policies for several areas from subcontractor hiring and work to mobile devices to remote access could be affected. The enterprise may also need to enact new policies in some cases.

About the Author

Mark Cioni is an executive consultant with Enspira Solutions, a Black & Veatch company. He has over 26 years of experience with particular expertise in Information Security, Enterprise Architecture, and Systems Integration. He is a contributor to NIST's Cyber Security Coordination Task Group, and holds a BS in Electrical Engineering with concentrations in Computer Science, Physics and Economics.