

Constant Vigilance

A holistic approach to smart-grid security.

BY MARK CIONI

The smart grid has gained solid traction in many respects, and it encompasses a broad and interrelated ecosystem of technology, processes, information and concerns. While the smart grid has the potential to enable many desirable outcomes articulated by government, industry and consumers, it also presents significant potential risks to our power generation, transmission and distribution systems in ways perhaps not even imagined just a few years ago.

A number of smart-grid security concerns have been expressed in recent mainstream discussions. Many laypeople and experts believe the smart grid might be widely vulnerable to cyber attacks. For example, hackers or insiders could cause massive blackouts or other disruptions. There's also significant concern and media attention around the idea that utilities, hackers or other entities could use new smart meters and other methods to spy on consumers or control their homes without consent. Underlying these concerns is a relative lack of perceived experience and predictability regarding how the smart grid will react to intrusions and compromise, coupled with newly evolving standards for smart-grid security from the National Institute of Standards and Technology (NIST) and other influencers. In light of the myriad security concerns, some experts even advocate that smart-grid deployment should slow down.

The presentation of these concerns is sometimes sensationalized, even to the point of being comical; however, the potential risks are very real. Industry stakeholders are starting to recognize the paradigm shifts engendered by smart grid, with security being a core concern for the future. Additionally, the relatively recent advent of smart-grid funding and the associated need for standards compliance around new critical cyber assets

Security isn't a destination. It requires ongoing investments across core areas of the enterprise.

are driving utilities' security diligence like never before relative to themselves, smart-grid solution vendors and other broad areas of infrastructure.

As smart-grid security continues to evolve, the critical areas of discussion should include the approaches by which utilities and solution vendors can help to mitigate security risks within smart-grid implementations. Smart-grid security isn't a destination, it's an ongoing process. Smart-grid security shouldn't be about slowing down, but rather mitigating risk and limiting exposure as intelligently and as quickly as possible.

AMI: A Common First Step

As utilities evolve their smart-grid implementations, a common foothold is an advanced-metering infrastructure (AMI) solution. Although AMI systems are just one component of the smart-grid ecosystem, their functionality, characteristics and confluence with the larger grid impart an array of interesting security challenges.

AMI systems have evolved rapidly over the last several years to include a wide range of business and technical features that have served to differentiate AMI vendors and advance the state of the industry. Functionality such as remote connect and disconnect, segmenting endpoint populations for mass control, message buses for integration, remote firmware updates and many other functions embody the ways by which these systems are striving to meet, or create, customer and market needs.

Unfortunately, this rapid pace of product evolution often is driven by individual customer demands, marketing strategies, acquisitions and other factors, without sufficient consideration of potential security threats presented by new business or technical functionalities. Remote firmware updates, as one example, provide great potential benefits to an organization, yet without sufficient capabilities—for separation of duties, source authentication, code signing and encryption, completion checks and rollback functions—a significant risk could be introduced into the AMI system.

The inherent characteristics of many AMI systems present a significant threat surface for security vigilance. A majority of AMI endpoint assets are physically dispersed over wide areas with few, if any, physical controls. The fact that these endpoints might provide functionality beyond metering (*e.g.*, appliance control), and also might be manufactured and supplied by a variety of sources, means that AMI providers need to ensure that their own infrastructure is as secure as possible and resilient to potential threats they can't predict

Mark Cioni is an executive consultant with Enspira Solutions, a Black & Veatch company. He also is a contributor to NIST's Cyber Security Coordination Task Group.

from sources over which they have little or no influence.

Intermediate field-deployed assets, such as collectors and extenders, as well as the pervasive integration of head-end systems, also may present their own vulnerabilities and introduce potential risks for malicious endpoint and system control, including systems outside the immediate AMI sphere of concern, such as meter-data-management systems and outage-management systems.

Modern AMI systems have incorporated, to varying degrees, sophisticated software development, middleware and integration capabilities into their fabric. This means AMI systems now can provide usage information for meter data management and billing, as well as low latency, bi-directional interfaces to such operational systems as outage management, demand response and others. These capabilities hold huge potential for making the grid smarter, and they also radically increase the threat surface, not only for AMI, but also for the entirety of the interconnected systems and their associated business processes.

It isn't difficult to imagine an attack that takes malicious control of other operational systems connected to AMI because the systems didn't incorporate sufficient security controls at their integration points. Even the potential effects of an inadvertent AMI load shed, potentially initiated *en masse* and by accident from an existing customer-service system process, should be enough to make utilities, vendors and other grid stakeholders think very seriously about their security posture and controls. The expanding role that AMI systems play in the smart grid demands a holistic and equally evolutionary approach to security.

Solution Security

As security imperatives have ramped up over the past few years, providers of AMI and other solution offerings and services have faced intense scrutiny from



existing and potential utility clients around their security controls and features. Although the conversations between vendors and utilities have become much more constructive and extensive, the typical view of solution security is often too limited.

Too often, utilities hold solution providers to standards they don't emulate themselves.

Utility focus often is skewed toward discovering how solutions have implemented specific controls versus the provider's overall approach to security in the solution. For example, it's important to ask if a provider uses a virtual private network (VPN) in the solution and what kind of VPN, but probably more important is discovering the roles of all communications channels being used throughout the solution, the options for securing those channels, and what the vendor enables.

When utilities explore candidate smart-grid solutions, they are particularly concerned around the security controls

and features of the solution—and rightly so. Often left unexplored, however, are the processes and practices that the solution providers are living and breathing every day. It's important to understand the penetration tests that have been done for a particular solution, but even more important to understand how the provider has instantiated a repeatable security development lifecycle as part of a larger product-development lifecycle.

Utilities justly are concerned about these and many other security aspects in the candidate smart-grid solutions they explore. The question is: Can they shine the same bright light on themselves? Too often, utilities will hold solution providers to standards they simply don't emulate themselves. For example, using the corporate directory infrastructure to provide authentication and authorization services to an AMI solution, without sufficient controls on that directory infrastructure itself, could present a significant risk of attack to critical cyber assets.

Secure Smart-grid Implementations

To implement smart-grid solutions that incorporate core principles of layered, reinforcing controls providing in-depth defense, utilities and solution providers

must share the responsibility of achievement. A number of key aspects, if viewed as mutual responsibilities, will help to enable utilities and their solution providers to mitigate security risks and exposures (see Figure 1).

Utilities and solution providers should begin by embodying a proactive security stance, evaluating and addressing the principles of smart-grid security across both individual solutions and their entire spectrum of initiatives. Objectives of such a security stance may include preventing data theft, minimizing manufacturing and maintenance costs, preventing malicious uses, and logging and auditing all modifications, among many others.

An evolvable security roadmap is needed to guide the organization's strategic intent relative to security, as well as the other aspects of the organization's security stance including policies, processes, product development, features and functions, *etc.* Analogous to a good business case in many respects, the security roadmap provides greater granularity in the near- and medium-term timeframes. Inputs to the roadmap include business drivers, regulatory constraints, current and emerging standards, competitive landscape, and potential system vulnerabilities and risks. The roadmap: 1) expresses the business case for security investment including expected return on investment (ROI); 2) conveys formal security requirements; 3) plans for appropriate certifications from recognized organizations; and 4) defines assessment, remediation, verification and prevention of vulnerabilities.

The roadmap should set forth an information assurance process (IAP) to guide internal and external security governance with rationale, objectives, metrics and priorities. The IAP includes supporting processes, artifacts and other substantive framework. The IAP guides internally focused security processes such as confidentiality and protection of

FIG. 1 SECURE SMART-GRID IMPLEMENTATIONS	
Embody a Proactive Security Stance	
Understand and proactively address security principles in AMI and smart-grid implementations.	Objectives include preventing data theft, protecting confidentiality, minimizing manufacturing and maintenance costs, preventing unauthorized and malicious uses, and logging and auditing all modifications.
Develop An Evolvable Security Roadmap	
Formalize the drivers, decisions, rationale and key performance indicators (KPI) that define the organization's view of success relative to security.	Inputs to the roadmap include business drivers, regulatory constraints, current and emerging standards, competitive landscape, and potential system vulnerabilities and risks.
Develop an Information Assurance Process (IAP)	
Guide internal and external security governance with objectives, metrics and priorities.	The IAP includes supporting processes, artifacts and other substantive framework for internally facing and externally enabling initiatives.
Instantiate A Security Development Lifecycle (SDL) Framework	
The SDL provides a measurable, repeatable and evolvable approach for developing and delivering secure products and services.	SDL guides manufacturing, development and testing standards for hardware, firmware and software—enabling best practices, knowledge management, and process maturity.
Perform Ongoing Testing and Remediation	
Establish measurable, repeatable and evolvable approaches for performing internal and external security testing across multiple fronts and threat surfaces.	Approaches span remediation, validation and future prevention, and include passive and active testing (internal and third party) as well as detailed reports of vulnerabilities discovered, contingent and remedial actions, and validation of closure by vulnerability occurrence and class, preventative actions, <i>etc.</i>
Look Outside The Industry	
Develop an infrastructure that has undergone rigorous testing, will evolve to meet an ever-changing threat matrix, and exhibits the same or better security, resiliency, monitoring and other aspects as more well-established, battle-tested infrastructures that currently convey critical resources and information.	
Become Mutually Trusted Security Advisors	
Utilities and solution providers must actively consider the future of smart grid-security.	Collaborate to identify solutions to common security concerns and encourage continued development of, and adherence to, security principles and standards industry-wide.

intellectual property, trade secrets and other critical information. It also ensures coherence and alignment with externally enabling initiatives such as the security development lifecycle (SDL) framework, testing and others.

The SDL framework provides a measurable, repeatable and evolvable approach for developing and delivering secure products and services. It encompasses the design and implementation of

processes, information and technology, the goal of which is to enable the realization of objectives and measures codified in the security roadmap and IAP. SDL includes instrumented and measurable quality gates, enabling artifacts to support the processes and practices, and maturity assessments and certifications. It guides manufacturing, development and testing standards for hardware, firmware and software—enabling best

practices, knowledge management, and process maturity.

A measurable, repeatable and evolvable approach for performing internal and external security testing is a core SDL component. Secure solution development depends on vulnerability assessment and testing incorporating both internal and external third-party approaches—and including active and passive black, gray and white box-focused penetration testing, automated code profiling, physical and low-tech penetration testing, social engineering and many other aspects.

Utilities and smart-grid solution providers often hear permutations of the following imperative from their own stakeholders: “Be as secure as the ATM and ACH networks.” Regardless of any perceptions or reality about the security of these networks, especially in light of the high-profile breaches in recent years, the message in the industry is clear: “Develop an infrastructure that has undergone rigorous testing, will evolve to meet ever-changing threats, and exhibits the same or better security, resiliency, monitoring and other aspects as more well-established, battle-tested infrastructures that currently convey critical resources and information.” A look outside the utility industry is one of the key aspects of smart-grid security.

In addition to addressing immediate concerns, utilities and solution providers must actively consider the future of smart-grid security. While challenging to enact, a meaningful dialog is a key enabler of ongoing long-term success. Utilities and solution providers can become mutually trusted security advisors by:

- Exchanging security expertise and lessons learned in order to drive improvements in solution and services offerings as well as utility implementations;
- Assessing available security technology and best practices to better mitigate risks, reduce costs and

CAREER OPPORTUNITY

Electric Power and Public Policy:

Carnegie Mellon’s Department of Engineering and Public Policy seeks PhD candidates to work on technical/policy issues in the electricity industry in areas such as variable renewables, time of use pricing, distributed resources, etc. Details at: www.epp.cmu.edu


Gas-Fired Power Plant Optimization Model

Features include tolling optionality and a dynamic programming optimization algorithm.

Inputs: Ramp tables, heat rates, duct data, prices/volatilities, down times etc.

Outputs: The optimal operating schedule, intrinsic/extrinsic values and price sensitivity.

Contact information:



Website: www.cygnetriskgroup.com
Phone: 713-668-8170
Email: info@cygnetriskgroup.com

Cygnets Risk Group, Ltd.

maximize efficiencies; and

- Encouraging a focus on, and sharing of, new technology ideas or developments with broad industry applicability.

These key aspects of successful and secure smart-grid implementations represent a core subset of an evolutionary and holistic security approach. By definition, this approach must continue to evolve in order to address the equally dynamic landscape of smart-grid needs, capabilities, standards, and of course security threats.

Business-Case Considerations

Smart-grid security exerts a range of influence on the typical touch points of business-case development and enterprise architecture. Many times, these influences aren’t properly recognized and addressed, potentially impacting the realization of business outcomes and enterprise initiatives.

Some of the key considerations include ensuring that enterprise architecture, risk management, facilities, and information security resources are involved in all aspects of business-case

development, smart-grid architecture, solution evaluation and, of course, solution implementation and business-case realization.

Utilities should make a concerted effort to consider the range of influences of smart-grid security. For example, when developing an AMI business case it's important to account for the acquisition and recurring costs of additional security infrastructure, services and testing. Further, the utility will want to account for ongoing security services, infrastructure, training and industry participation in its fiscal planning, project planning and other key enterprise processes. Security isn't a snapshot in time and it isn't a destination. Security requires ongoing investments across infrastructure, processes, knowledge and other core areas of the enterprise.

Investments in marketing and communications to utility customers and other key stakeholders around smart-grid security also should be recognized. Many utility customers, for example, are concerned by mainstream media reports of hackers shutting off their power, the utility spying on how they use electricity and resultant privacy concerns, and many other aspects of the paradigm shift to smart grid. Utilities must proactively cultivate stakeholder buy-in as capital to offset situations ranging from implementation challenges to the ongoing FUD factor (*e.g.*, fear, uncertainty and doubt) introduced by mainstream media.

The granting of funds for smart-grid investment comes with the potential for security and operational audits of the utility plans on which the funding is predicated. With this in mind, preparation for future audits should address resources, remediation costs and even damages and capital.

Security Fabric

Smart-grid security likely will drive a wave of changes to policies, processes, technology, organizational constructs

AMI holds huge potential for making the grid smarter, and also radically increases the threat surface for inter connected systems and associated business processes.

and other areas including the supporting data, information and knowledge value chain. These changes will impact a range of stakeholders including customers, staff, external partners and others, and will present operational and organizational challenges.

Smart-grid security will require the development or redesign of organizational processes, with one classic example being remote disconnect and reconnect. Utilities will need to think broadly and deeply around triggering events, separation of duties, throttling and other aspects of a remote disconnect process. This process likely will be one that spans the white space between discrete system domains such as AMI, CIS, customer self-service and others.

New integration paradigms also will need to be developed to support smart-grid capabilities. Typically, this involves a much better understanding of the process, application, and data integration points, both extant and required, as well as the mechanisms ranging from manual to file-based to service-based integration. For example, using the remote-disconnect scenario, not only do organizations have various security aspects to consider, but they also must ensure that only authentic and authorized entities—including users, systems, processes and others—are able to inter-

act in a meaningful way with the infrastructure implementing remote disconnect. Since the process context may span multiple system domains, it's crucial to ensure that remote disconnects have a transactional context (*i.e.*, an operation was requested, executed and verified across the entire process domain, versus just sending out 100 remote disconnect commands from the customer-service system to the head-end system).

Compliance policies, processes and information will need to be instantiated or extended relative to smart-grid investment. Funding constraints may proscribe using existing infrastructure, such as IT assets, for AMI initiatives, and many funding recipients have adopted a net-new infrastructure policy. Obviously, this directly would affect business-case inputs relative to acquisition, licensing and support costs, among others.

A secure smart grid also requires changing the processes, policies and interactions involving external partners such as billing and other infrastructure and service providers. In many cases, these entities have not dealt with stringent security constraints to their access and usage of relevant information and processes. With the increased focus and requirements around security, external entities may need to engage differently in many areas, such as using multi-factor authentication and VPN access.

In order to realize the smart grid's potential, security must exist in every fiber of the smart-grid's fabric. Smart-grid security threats will become more challenging and pervasive in the foreseeable future, and both utilities and solution providers will need holistic, proactive and mutually enabling security approaches to address those threats. To paraphrase Thomas Jefferson, the price of smart-grid security is constant vigilance, and that vigilance is everyone's responsibility. ■