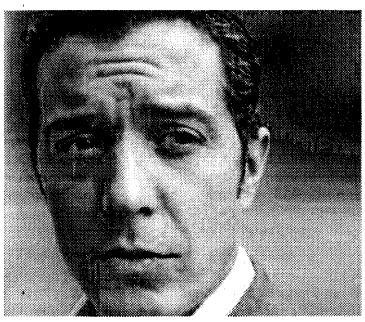
Future. Ready.[SM]

WHITE PAPER

Smart Grid Security: Preparing for the Standards-Based Future

Without Neglecting the Needs of Today

Steve Chasko
Principal Security Engineer,
Landis+Gyr



T.J. LaPorte
Senior Product Manager,
Gridstream Security
Landis+Gyr

Landis+Gyr
manage energy better

Smart Grid Security: Preparing for the Standards-Based Future

Without Neglecting the Needs of Today

The Security Needs of Today and Tomorrow

The importance of properly securing smart grid assets has grown in direct relation to the demonstrated penetration of electric transmission and distribution systems worldwide. Outside of real attacks, test labs have demonstrated the capability to attack home area networks, advanced metering systems and generation facilities. Smart grid security is no longer a theoretical concern.

Yet, securing the smart grid will require electric utilities to take both short-term and long-term views. The immediate focus should be on performing internal risk assessments, implementing continuous threat modeling, and forging partnerships with technology vendors that complement existing internal security policies and procedures. At the same time, smart utility managers will also begin participating in industry security groups with an eye to shaping the development and adoption of comprehensive cyber security standards.

Smart grid networks must have the capability to protect the integrity of data by implementing security controls that detect improper or unwanted modifications. Network components also must have a high degree of confidence that data is coming from a trusted source. Effective smart grid security must be adoptable throughout the utility, adaptable to current and future infrastructure needs, and appropriate to the process or equipment being secured.

Technology vendors are pursuing multiple options for securing network and data assets. Going forward, it will be necessary to develop a true partnership with the utility to integrate a security approach across the utility's personnel and process domains.

At Landis+Gyr, we are building on our long history of helping utilities realize the full potential of the smart grid by working with customers and within the industry to promote a security solution that:

- *Is standards-based*
- *Relies on a proven, open architecture*
- *Addresses every access point in the network*

We believe an end-to-end approach that takes into account today's and tomorrow's needs is the best way to ensure that all utility assets are protected — no matter which communication technologies are deployed. We call this philosophy: *Future Ready.*

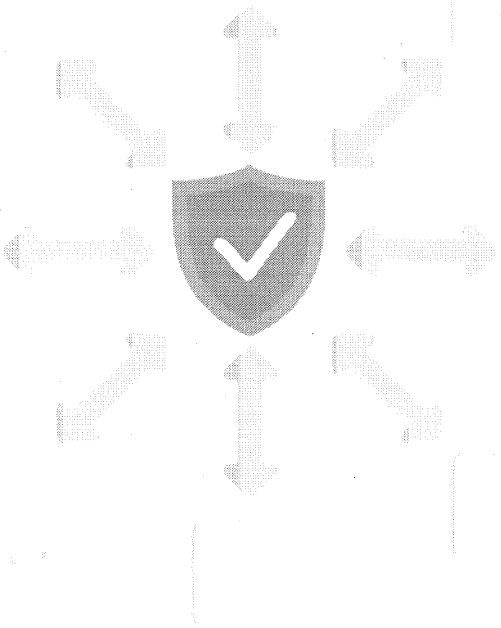
Challenges On All Sides

Modern smart grid networks that are capable of two-way communications with devices across the grid have only been in use for a short time. Previously, utilities have used a variety of communications technologies to communicate with substation equipment, distribution devices, load control switches and meters. In-premise devices, where they existed, were not part of the broader network. Legacy communication devices typically relied on one-way communication and were not part of a singular network or head-end system.

The inherent complexity of the smart grid, along with the concept of multiple interconnected networks with additional entry points, introduces many new security challenges. Utilities must adopt a security solution that provides proven security techniques and strong cryptographic capabilities, not only to protect their network availability and metering data, but also to protect their consumers from malicious attacks affecting operations and potentially compromising their consumer's private data. Adding to these challenges is that, unlike typical IT networks which are upgraded frequently, smart grid infrastructure is expected to have a long service life (often 10 years or longer), meaning security solutions will always need a migration path for legacy systems.

The National Institute of Standards and Technology (NIST) has published an internal report, NISTIR 7628, that states that at some point, all smart grid systems will be targets of an attack. In essence, it is not a matter of if a utility network will be attacked, but a matter of when. With the ever-increasing number of threats (including common hackers, crime syndicates, and terrorists), there is also a significant increase in relatively inexpensive and highly sophisticated hacking tools that could increase the likelihood of a successful attack. Under these circumstances, system security is only as strong as the weakest link.

Landis+Gyr has made security an ongoing priority for over 10 years. This includes practical experience in field applications, as well as developing and maintaining a strong risk-based



methodology for ongoing product development. Systemic security begins with understanding and modeling the various threats utilities may face. Some of the more common risks for distribution utilities include:

- *Endpoints and in-premise devices, such as advanced meters, home area networks, electric vehicles and mobile devices that communicate with the network*
- *Distribution level control systems, such as Supervisory Control and Data Acquisition (SCADA) Systems, Energy Management Systems (EMS), programmable logic controllers (PLCs), and distribution automation (DA) devices that can control the flow of power*
- *The communication networks, both wireless and wired*
- *The head-end system, including servers, applications, databases, web sites and web services*
- *People and process issues, such as attacks initiated by disgruntled or former employees, or a lack of training and awareness for operational personnel who accidentally introduce risk*

One way Landis+Gyr addresses dynamic risk is through ongoing penetration testing of the Gridstream™ smart grid solution for advanced metering, distribution automation and personal energy management. Landis+Gyr engaged Lockheed Martin to perform an objective NERC CIP- and NIST-focused risk assessment of Gridstream system products in an effort to identify critical cyber assets. This is in addition to internal and external risk assessments on these critical assets in an effort to identify, classify and mitigate vulnerabilities that an attacker could exploit.

Compliance with standards such as NERC CIP 002-009 requires a consolidation of utility policies and procedures and vendor technology. Landis+Gyr is committed to continually enhancing product features today and future roadmaps with industry compliance in mind to further complement our customers existing required policies and procedures.

Auditability and Compliance

NISTIR 7628 – GUIDELINES FOR SMART GRID SECURITY

NISTIR 7628 is a set of guidelines or "a reference document" for implementing smart grid security. The information and requirements within NISTIR 7628 provide valuable direction for developing effective cyber security strategies. Landis+Gyr has taken a proactive approach to what we believe will be necessary compliance with future industry standards. Our Gridstream security solution already leverages much of the relevant information provided by NIST, including:

- *Implementing security controls in all phases of the development cycle from the design phase through implementation, maintenance and device/product decommissioning*
- *Developing and performing ongoing risk assessments and penetration tests in order to identify assets, vulnerabilities, threats and impacts that can be used to prioritize and implement necessary mitigating security features*
- *Creating a robust, future ready, systemic feature set leveraging the requirements documented in Volume 1*
- *Implementing appropriate privacy controls based on information provided in Volume 2*
- *Leveraging the vulnerability classes listed in Volume 3 to ensure the Gridstream solution has the necessary controls to mitigate the vulnerabilities listed*
- *Ongoing participation with existing smart grid security bodies including the NIST Cyber Security Working Group (CSWG), the AMI-SEC task force within the UCAIug, and the ZigBee Alliance*

NISTIR 7628 is a tool and reference guide for architecting smart grid security solutions. It is recommended that utilities currently researching prospective vendors with the intention of deploying a smart grid solution utilize the guidelines and requirements as a means of evaluating available solutions.

NERC CIP

The applicability of the NERC CIP standards as they relate to distribution systems and advanced metering is still being debated. However, it is commonly believed that compliance with these standards may become a future requirement. Landis+Gyr has again taken a proactive approach by hiring Tier 1 security vendor Lockheed Martin to perform NERC CIP assessments of the Gridstream product line and the Landis+Gyr Network Operating Center.

The assessment covered all CIP standards including:

- *NERC CIP-002 – Critical Cyber Security Asset Identification*
- *NERC CIP-003 – Security Management Controls*
- *NERC CIP-004 – Personnel & Training*

- *NERC CIP-005 – Electronic Security Perimeters*
- *NERC CIP-006 – Physical Security of Critical Cyber Assets*
- *NERC CIP-007 – Systems Security Management*
- *NERC CIP-008 – Cyber Security – Incident Reporting and Response Planning*
- *NERC CIP-009 – Recovery Plans for Critical Cyber Assets*

Although many of the requirements listed in the NERC CIP-002 through CIP-009 are considered policy and procedural in nature, Landis+Gyr was able to take the results of the assessment, identify the technology-based requirements, and then used this information to architect a solution that allows clear integration within utilities' NERC CIP compliance program.

People and Processes

Each utility faces unique challenges and associated risks relating to network security. Utilities need flexibility to balance risk with the security solution most appropriate for their business needs. Gridstream security is configurable in a way that allows utilities to immediately deploy the desired level of protection necessary to guard against external, as well as internal, threats.

One key area of risk is an attack from within, whether malicious or accidental. External attackers can attempt to breach head-end security in a number of ways, but monitoring employees with legitimate access to systems is just as crucial. Landis+Gyr provides tools within the Gridstream operating software and field tools to guard against unauthorized access and monitor actions as they happen to alert for unusual or improper network applications.

Command Center head-end system software has a variety of security features that can prevent unauthorized employees from accessing functionality. To protect against activity by authorized employees, NIST and NERC emphasize the need to implement strong auditing and reporting capabilities that capture user activity. By following these processes and procedures, utilities can quickly identify suspicious activity and pinpoint who performed the action, the date and time in which the action was performed, and the results of the transaction.

Using role-based access control (RBAC), the designated security administrator is granted the capability to run through a one-time configuration set-up process that establishes the appropriate security settings of the system and the network devices. Once the appropriate security settings have been established, the Gridstream solution ensures a smooth and easy process for network security configuration, device management and network management. The head-end also offers a variety of user-friendly dashboards and reports that guide the security administrator through their day-to-day responsibilities.

Systemic Controls

Landis+Gyr takes an end-to-end approach to security for the Gridstream smart grid network. While some security approaches focus on protecting the transportation of data messages, the Gridstream solution has the capability to go beyond message transportation and offer protocols to validate the origin of a data message, and prevent the spread of unauthorized or malicious code.

Gridstream offers the ability to add third-party components to the IT infrastructure, including a Key Manager from RSA Laboratories and SafeNet's Hardware Security Module (HSM). The Command Center head-end system includes the interfaces needed to connect to these applications, reducing the complexity of the installation and setup process.

RSA Laboratories' security solution is a non-proprietary and scalable solution with a proven track record of securing network transactions in a variety of industries. The main components of the RSA solution include providing cryptographic functionality at the endpoint using the BSAFE crypto-library, and at the head-end using the RSA Key Manager. In this system, network devices have the capability to generate keys during the registration process. These keys are securely passed to the Command Center and stored in the key manager. Each network device or endpoint generates its own key, eliminating the possibility the key could be stolen or compromised during manufacturing.

Gridstream RSA SafeNet

The SafeNet Hardware Security Module (HSM) establishes a strong root of trust by providing a secure storage medium for network keys. This FIPS 140-2 validated solution ensures integrity of encryption throughout the network, and provides confidence that network activities and commands are legitimately initiated within the network.

Enabling Gridstream security does not affect the endpoint installation process. As a matter of fact, there are no additional steps required by the installer to deploy endpoints in the field, as all the security parameters and keys are exchanged between the endpoint and the head-end server via the endpoint "plug-and-play" auto-registration process.

The Importance of Being *Future Ready*

The future of smart grid security depends on a clear roadmap for all technology developers to follow. Landis+Gyr participates in industry cyber-security initiatives such as the NIST Cyber Security Working Group and the SG Security Working Group, formed by the UCAIug OpenSG Technical Committee.

Landis+Gyr strongly believes in establishing an open and mature security process. The Gridstream security solution is based on industry accepted security protocols and standards. It is built on the premise of openness: open architecture, open collaboration and open standards to bring the strongest security mechanisms for protecting the interests of utilities and end users.

Landis+Gyr continues to seek strong partnerships with world-renowned security companies, and has developed a security competency criterion to rank multiple security organizations. Through partnerships with world renowned security vendors, Landis+Gyr has been able to successfully bring to market a best-in-class security solution that utilizes open, non-proprietary, future ready cryptography and key management capabilities that are not only validated by U.S government agencies, but relied upon by the U.S. Department of Defense and many other government agencies because of their reputation for quality, reliability and adherence to FIPS 140 and Suite B cryptographic standards.

Landis+Gyr has performed, and will continue to perform, internal and external penetration tests with security industry experts, such as Lockheed Martin and IBM in an effort to stay on top of the increasing number of threats and new attacks vectors. This allows us to identify and mitigate potential vulnerabilities that utilities face right now, which could be exploited or compromised by a malicious attacker.

Summary

Security solutions must provide the protection utilities need today, while continuing to adapt and grow to meet the needs of tomorrow. Industry standards and protocols should set a high standard for consistent and interoperable performance.

By developing a best-in-class security solution that focuses on industry-driven standards, open non-proprietary standards and NSA Suite B recommended cryptography, Landis+Gyr is able to offer a robust feature set and proven appliances provided by world-class partners. This provides the necessary confidence that data security and critical infrastructure are secure, electric service is protected and the utility's reputation will remain intact.

Have security concerns you'd like to discuss?
Want to know more about our smart grid solutions?

Contact us today to start a conversation: Security.NA@landisgyr.com