Tab: Communications Network

Requirement 9 – Security Overview

The Landis+Gyr Gridstream security suite is built to US government and international standards. The Landis+Gyr cyber security system is built to Federal Information Processing Standard government computer security standard (FIPS 140) and includes National Security Agency suite B compliant cryptography. It is also built on the Common Criteria for Information Technology Security Evaluation which is an international standard (ISO/IEC 15408) for computer security certification.

Working with partners such as EMC/RSA Laboratories and SafeNet, the Gridstream security solution is based on open, non-proprietary mechanisms that provide compliance with industry standards and best practices including the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, NSA Suite B, AMI-SEC, NERC CIP, DOE and others.

Landis+Gyr also address dynamic risk management through ongoing penetration testing of the Gridstream AMI system. Landis+Gyr engaged Lockheed Martin to perform an objective NERC CIP and NIST focused risk assessment of the Gridstream AMI system in an effort to identify risk areas. This is in addition to internal and external risk assessments 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 with future development guided by industry standards.

Compliance with the industry, government and international standards for security, along with periodic penetration testing will assure utilities that the Landis+Gyr security systems are the best available in the industry. Landis+Gyr in cooperation with AEP deployed the first end-to-end secure AMI system utilizing these standards.

NISTIR 7628 Compliance

NISTIR 7628 is a set of guidelines 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 standards based approach toward the development of the Gridstream AMI security solution that leverages much of the relevant information provided by NIST. Landis+Gyr has implemented security controls in all phases of the development cycle, from the design phase through implementation, maintenance, and device/product decommissioning. Landis+Gyr has developed and performed 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. Landis+Gyr has maintained 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.

NERC CIP

The applicability of the NERC CIP standards as they relate to AMI is still being debated. However, it is commonly believed that compliance with these standards may become a future requirement. Landis+Gyr has

taken a proactive approach by retaining Lockheed Martin to perform NERC CIP assessments of the Gridstream AMI system.

The assessment covered all CIP standards, including the following:

- 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.

Systemic Security Controls

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

The Gridstream AMI system provides extensive key management capabilities, including 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 network communications devices and the AMI meters using the BSAFE crypto-library and at the head-end system 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 head-end system and stored in the key manager. Each network communications device or AMI meter generates its own key, eliminating the possibility that the key could be stolen or compromised during manufacturing.

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.