Cyber Security

The M2M System interfaces currently consist of secure virtual private networks connecting to each device through cellular communication. Each smart grid device connects to the cellular network through secure digital identification numbers assigned at the time of provisioning. The digital signatures allow the devices onto the cellular network. Each carrier then passes data to their central operations center which is connected to the M2M operations center with a secure virtual private network. Smart grid devices can pass data to and from the M2M operations center through this secured communications path.

The M2M System smart grid devices communicate to the operations center in a proprietary format which is not published or openly available. M2M Communications does provide web services for integration with the operations center. Through these web services smart grid devices can be issued control commands in a very specific and secure manner.

The M2M System has several mechanisms built into it for redundancy and communication failure. Redundancy is addressed in the Information Technology infrastructure at the operations center. Servers are duplicated for failover purposes. Databases which drive the front end services are mirrored so that in a hardware failure event, no data loss or downtime is incurred. Communication is configured to retry in an optimal fashion when devices do not respond to command attempts. Devices that are configured properly respond quickly and reliably.

M2M Communications will meet the required NIST standards by integrating with the AMI-SEC System Security Requirements. Integration with AMI-SEC will allow us to connect to many existing smart grid applications and extend the geographic footprint of the system(s). The system will also comply with NERC CIP 002-009 Cyber security standards for the bulk power system through secure and encrypted access to the system. The M2M System security best practices are modeled after Microsoft recommendations for web applications and software.

M2M System vulnerabilities can be primarily found at the point of public exposure. The web site is the public facing interface. By following Microsoft security best practices we can ensure that risk of intrusion is minimized. Access to the operations center servers are firewalled and monitored. Because access to the system is limited through a single portal, as cyber security standards change the system can be adapted to meet those security standards and maintain required security levels. All login and password information will be stored encrypted.

VeriSign® Security Services

For security implementation related to the NERC standards M2M will work with VeriSign to achieve and maintain compliance with regulatory requirements and standards of good practice. In particular, we follow the requirements with key regulations and requirements such as NERC standards CIP-002 through CIP-009.

Technical Security Assessments

NERC CIP-007 requires an annual cyber vulnerability assessment. By working with VeriSign we will ensure that the following steps are performed:

- Architecture assessment
- Network vulnerability assessments
- Application security assessments

Program Development and Remediation

There is significant ground to cover in the NERC standards, not to mention future regulations and standards. Examples include:

- Program management –Prioritizing and managing key security improvement activities.
- Policy development
- Incident response program development
- Business continuity and disaster recovery

Firewall Management

An electronic secure perimeter is a core requirement our NERC Cyber Security Standards.

Our firewall harnesses industry best practices to ensure a high level of network access and information availability, integrity, and privacy. The M2M firewall also meets or exceeds the monitoring and response requirements as outlined in NERC standard CIP-005 by delivering around-the-clock firewall monitoring and generating immediate alerts and responses for service outages and security alerts associated with critical Internet access points.

Managed Intrusion Detection and Prevention

Monitoring electronic access is discussed in CIP-005 of the NERC Cyber Security Standards, and intrusion detection is also mentioned in the Systems Security Management requirements under CIP-007.

All intrusion attempts, regardless of severity, are logged, and well-defined customer notification and resolution procedures are executed for all security events.

Vulnerability Management Services

The information protection and systems management requirements in CIP-007 of the NERC Cyber Security Standards address the inherent need to proactively identify and manage vulnerabilities across the network. The performance of this portion of work includes an upfront risk assessment, recurring vulnerability scanning, vulnerability testing, and penetration testing.

Unified Authentication

Access control is addressed in NERC Cyber Security Standard CIP-005. This section requires that "the entity…implement strong procedural or technical controls to the access points to ensure authenticity of the accessing party." Strong, two-factor authentication provides a higher level of security than solutions based on static passwords alone.

Section #6 - Project Costs and Benefits

Financial Metrics & Summary

The M2M Lodestar Irrigation Load Control system benefits everyone involved – grower, utility and the general public.

Project Results

1. Significant reduction of agricultural peak demand
2. Reduced likelihood of future electricity shortages
3. Reduced customer energy bills
4. Reduced peak power prices
5. Reduced requirement for additional power generation facilities, transmission, and distribution networks
6. Reduced air pollution
7. Reduced dependency on foreign oil

The most applicable metrics for this project are based on participants and controlled load.

The Lodestar system maintains a detailed record of all sites including the KW of each piece of controlled equipment. The *total* number and percentage of load control participants and the total dispatchable load is easily determined from the system site database.

All Lodestar field units communicate information automatically about on/off status and availability for load control.

The *actual* number of participants for any specific dispatch and the actual KW shed is readily measurable in two different ways:

1. The utility's interval meter reports the demand before, during, and after a load control event.
2. The Lodestar system independently monitors and reports the demand before, during, and after a load control event. The system plots the demand curves for any specific intervals.