The protocols and standards that comprise the initial design for the AMI and smart grid initiatives are consistent with the standards outlined in version 1.0 released by NIST.

5.2. Cyber Security

We have traditionally taken a conservative approach as it relates to cyber security of its systems, applications, and networks, particularly with real-time systems such as SCADA. In the AMI and smart grid implementation, we will continue its conservative stance. As part of this implementation, GPA will continue to promote separate network domains for SCADA and other real-time and/or reliability-sensitive applications, with specific firewalls and interfaces for data sharing and communication. GPA will continue to leverage DNP3 and IEC-61850 for SA and DA communications and control. Additionally, with respect to the various smart grid devices and smart meters, the security architecture is based on a platform of 'mutual distrust.' This ensures promotion of the highest levels of security without limiting the functionality and benefits of the devices themselves.

GPA's approach for smart grid devices is based upon a primary focus on security. The plan is to have encrypted point-to-point communication paths to each device from its primary application. GPA believes this is a solid approach and mitigates key security risks compared to an approach of devices that are permitted to communicate with each other as well as their primary applications. VLAN segmentation is going to be used when a Layer 2 approach is deemed necessary.

5.3. Using NERC-CIP Standards in Smart Grid solutions

The following are the key NERC CIP Standards that we have incorporated as appropriate for both critical and non-critical smart grid cyber assets. We have leveraged the NERC CIP standards in the creation of its smart grid cyber security policies and design. These cyber security standards are embedded in the GPA Cyber Security Handbook that is described later in this section:

- Critical (Cyber) Asset Identification (CIP-002-1)
- Security Management Controls (CIP-003-1)
- Personnel and Training (CIP-004-1)
- Electronic Security Perimeters (ESPs)(CIP-005-1)
- Physical Security Perimeters (PSPs)(CIP-006-1a)
- Systems Security Management (CIP-007-1)
- Incident Reporting and Response Planning (CIP-008-1)
- Recovery plans for Critical Cyber Assets (CIP-009-1)

5.4. Guam Smart Grid Lab

As part of its smart grid and AMI roll-out, GPA will establish a smart grid lab which will be used for initial testing and configuration of devices. The lab will also serve as a test bed for replicating problems, replacement, and upgrade of devices as well as testing of functional features. The lab will supplement GPA's already stringent IT testing and upgrade processes, providing a non-operational environment in which to validate performance and functionality without affecting real-time reliability or other operational systems. This approach provides the best overall means of mitigating potential problems without directly impacting customer or distribution operation systems.

5.5. Guam Cyber Security Handbook

GPA will create a Security Handbook for its AMI and smart grid solutions to ensure that clear life-cycle management processes are outlined for all of the equipment and applications. This handbook will be based on several best in class security sources including the NERC-CIP security requirements for the Department of Energy - Basic Energy Sciences (DOE BES) as well as the network security strategies implemented for financial institutions. The following chapters of this security handbook will cover how

we will maintain compliance to the NERC-CIP requirements to all parts of the smart grid network, even though the majority of these assets are not classified as critical cyber assets. This handbook will be a living document updated on a regular basis based on findings from internal audits, organizations like NIST, GridWise, EPRI, and the utility industry.

5.6. Summary of cyber security standards and best practices

5.6.1. AMI

While security practices and implementations vary between vendors, a number of general features or concepts will be implemented in any AMI collector or access point. The goal of the AMI system is to be resilient to downtime in the upstream communication system; in the case of an AMI collector, it might be temporarily storing or caching meter data until the AMI head-end returns to service. The stored meter data should be encrypted with strong encryption algorithms, such as the Advanced Encryption Standard (AES), in case the collector is compromised by attackers. Otherwise, data related to power quality and voltage of lines and power usage data from the AMI meters could be manipulated to provide false readings.

Many of the same concepts found in the AMI collector will be implemented within the AMI smart meter, too. Features such as encrypted data transmission and the ability to cache encrypted data if the collector is unavailable are built into the system. Encryption schemes should utilize strong cryptographic standards, again using AES, to ensure data confidentiality. A mutual distrust architecture is necessary to ensure integrity of messages being received by the meter. If an attacker were able to send unauthenticated messages to the meter, they may be able to forge a remote disconnect command, disconnecting the customer's power until the utility becomes aware of the forgery.

The AMI collectors run an embedded Linux platform, and, thus, can utilize security features such as firewall rules and secure tunnels, in order to increase network security to these devices. The AMI collectors themselves are locked down such that only necessary ports are opened, such as SSH/SFTP for management and firmware updates, NTP for time synchronization, and the necessary AMI communication ports. The system features 256-bit AES encryption end-to-end; that is, from meter, through AMI collector, into the AMI head-end. A streaming cipher is utilized in order to prevent replay attacks. Separating device types into different VLANs allows GPA to configure Access Control Lists (ACLs) between VLANs to prevent network traffic from traversing unsecured ports and network segments. For example, the AMI collectors will have an ACL applied to allow access only to the AMI head-end servers.

Security for AMI should utilize a PKI infrastructure for authenticating meters and a 256-bit AES encryption end-to-end (meter to RNI) for communication. Additionally, a secure tunnel will be created to encrypt all traffic between AMI elements while utilizing a streaming cipher to prevent packet replay attacks. ACLs on AMI collectors to prevent unauthorized devices from establishing communication with the collectors will also be implemented. In terms of management, HTTP over SSL for web management pages will be used to ensure data integrity, as well as centralized authentication for AMI head-ends and collectors using RADIUS, TACACS+, and LDAP/Active Directory for centralized logging of access attempts, both authorized and unauthorized. AMI collectors and AMI head-ends will use SNMPv3 for secure trap generation and management.

In terms of system resiliency/disaster recovery, the meters will be able to store data for 60 days following an outage, AMI collectors for 30 days, and the AMI head-end for 30 days as well. The stored meter data (meter, AMI collector, AMI head-end) will be encrypted.

5.6.2. Distribution Automation

The DNP3 protocol that the communication gateways and relays utilize is a Layer 2, non-routable protocol. While network traffic will pass through devices that have IP addresses assigned to them, it will be in a separate network segment with no IP connectivity; a Layer 2 connection from substation directly to the Siemens SCADA Master System. SCADA traffic will be encapsulated on a Layer 2 VLAN connection. For routed traffic, each substation will be provisioned on its own Layer 3 network segment so that it may communicate with the primary datacenter and the disaster recovery site. This ensures that all potential communication between substations is separated and secure.

DA equipment and devices should support IPSec VPN tunnels (supporting both a primary and backup peer) with AES 128-bit encryption, SHA-1 hashing algorithm, and Perfect Forward Secrecy (PFS) for secure tunneling over the network back to the utility. The devices will also support a stateful firewall capable of being managed from SSH or HTTP over SSL for management. For logging, the device will use SNMPv3 and syslog for secure log transport.

In terms of connectivity, the DA devices will utilize one of the following communication methods: RS-232 (dual for resiliency), a cellular network radio, and Ethernet (dual for resiliency that would support NIC teaming). The devices will also be environmentally hardened for physical resiliency.

5.6.3. Substation Automation

Substations will be secured in a manner that is consistent with the guidelines in CIP-006-1a for physical security. Two-factor locks such as card-swipe and keypad access code will be implemented as a first defense, with the ability to log access attempts and correlate entry with incidents, if necessary. SCADA traffic coming into the substation will be segmented from IP traffic that is brought into the substation.

IP-based devices in the substation will be locked down, authenticating from a centralized user database, if possible, with detailed logging/accounting of entry or access. Each substation will be terminated into a separate firewall sub-interface within the GPA datacenter. Each "substation" firewall sub-interface will deny all traffic by default and only allow specific traffic. By segmenting each substation into a sub-interface ensures that if anyone attempts and succeeds in breaking into a single substation and gains access to the substation IP network, they will not have the ability to compromise the remaining substations without physically breaking into all of them. This architecture effectively compartmentalizes any break-ins, reducing overall risk from an incident.

Substation switching infrastructure includes Layer 3 switches. At remote substations, hardened switches will be installed for the environmental conditions. The switches will be configured with the following features: 802.1x authentication, MAC-address locking on a port-by-port basis, intrusion detection, and speed/packet thresholds per port.

Switch ports in substations will be locked down, using access control lists and private VLAN tagging to ensure that each port may only communicate with its respective head-end system. For example, any ports assigned to the AMI VLAN will only have communication with the AMI head-end system. This helps to thwart attackers that wish to break into a substation and attempt to take down the entire network and/or all substations from a single physical point.

For security, the switches will be configured with SSH to a centralized authentication database via RADIUS. The logging subsystem will utilize SNMPv3 and syslog for secure log transport.

(VRRP) along with physical redundancy. The router will also be configured with QoS to ensure timely delivery of critical packets. For security, the router will be configured with SSH to a centralized authentication database via RADIUS. The logging subsystem will utilize SNMPv3 and syslog for secure log transport.

6. Project Costs and Benefits

This section captures the costs for the Project as well as the expected benefits by quantity and category. GPA has done extensive work on the design of the smart grid solutions proposed in this project plan including quantifying the related costs and benefits and defining how they can be tracked during the deployment and post-deployment period. This project plan will describe how the metrics in section 6.4 will be measured, as well as how the benefits in section 6.2 and 6.3 will be quantified so that they can be included in the DOE quarterly and annual reporting. In addition, the data collection and reporting solution will be used as an operational dashboard to continually monitor and manage the progress and benefits of the Project compared to the milestones and expectations.

This Project, if awarded, will be the beginning of a rollout of distribution and substation automation (DA/SA) and AMI to the entire GPA service territory and customer base. The deployment of AMI, DA, and SA equipment will occur within the first three years for all existing customers and new customers will be supplied AMI equipment in each year after that.

The waterfall chart below captures the cost benefit analysis of this Project over a 15-year period. (Note: The values from the chart are expressed in the form of their respective Net Present Values. The values listed in the verbiage in this section are expressed in their actual projected costs/benefits). The waterfall chart shows a Net Present Value of $213.8M in overall benefits over the 15-year period. (Note: all $'s expressed in "000's"). This chart also assumes that a grant for 50% of the qualified capital and expenses is awarded.

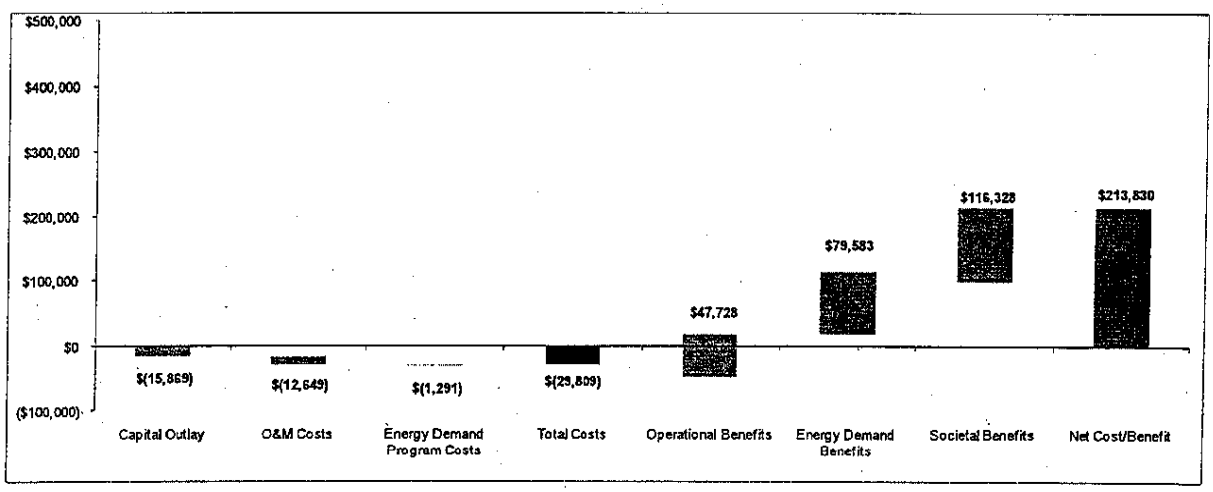

Figure 6-1 GPA 15-Year NPV Waterfall Chart (All $'s in 000's)

During the first three years of the project there is a total requirement of $33.0M in capital expenses. GPA will cover $16.5M of these costs and requests an SGIG award of $16.5M during this three-year period for the remainder. It is noteworthy from an economic stimulus perspective that 100% of the funds from ARRA will be spent in the first three years.