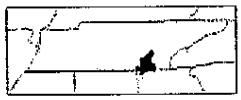


failure the MDMS will identify meters that are not reporting properly either by showing usage outside "normal" meter parameters or by theft, or failure. Battery backup at the meter and ONT location insure meter reporting in the event of a power failure. The MDMS software also has important applications that can be applied to failures of customer systems. For example there is an approximate 70 percent penetration of the EPB residential customer market by heat pump heating systems. When these fail, resistance heating occurs which is very inefficient and energy consumptive resulting in much higher customer bills. Typically this failure is undetected by the customer until weeks later when billing occurs. The AMI will develop customer use profiles which will can detect and issue an alert for unusual usage patterns as well as a meter failure, power failure or meter theft. EPB has tested this AMI system on a small scale (50 meters) in a lab and is now preparing to actively test the system with a 1,000 meter deployment in the EPB area.

Upgrade scenarios traditionally involve greater demand for bandwidth. In an effort to future-proof the system, EPB has designed the fiber system to have a very high availability of bandwidth.

4) How will the project support compatibility with NIST

In 2006, EPB asked the Electric Power Research Institute (EPRI) to conduct an independent review and evaluation of the proposed Chattanooga fiber to the home project. The final report issued on February 20, 2007 was a basis for planning and designing the EPB system roadmap to meet and support national emerging protocols and interoperability standards. The National Institute of Standards and Technology (NIST) has now asked EPRI to work with leaders in the industry to build a national roadmap for interoperability. EPB anticipates working and coordinating with EPRI and NIST as this framework is developed.

EPB has worked to select software and hardware that has tight adherence to accepted industry standards and is working in partnership with Alcatel-Lucent and Tantalus, both leaders in interoperability standards development in the industry. EPB considers these steps to be practical and necessary actions to support the NIST responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart grid devices and systems

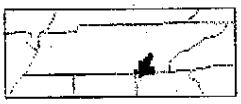
B. Cyber Security –comprehensive & capable of upgrade

1) Summary of risks and how they will be mitigated at each stage (vulnerabilities and impacts)

EPB's Advanced Metering Infrastructure systems offer tremendous potential, yet they introduce the requirements for industry proven, strong, robust, scalable, and open standards-based security solutions. The goal of EPB is to define an exhaustive list of the potential security threats, threat agents and vulnerabilities to the systems, perform detailed analysis to determine the risks they present, prioritize these risks and address these risks using a risk management framework.

System Design Stage

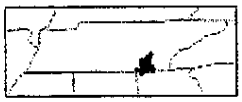
- Identify high level assets associated with each business function.
- Evaluate dependence of each business function upon high level assets.
- Evaluate applicable threats and vulnerabilities for each high level asset.
- Determine threat likelihood based on means, motive, and opportunity.
- Select security functional objectives for assets.
- Map security functional objectives through assets to security domains.
- Aggregate threats for each asset to security domains.



- Evaluate impact and consequence for applicable threats against all assets within a security domain.
- Determine risk based on threat likelihood and associated consequences.
- Analysis of the expected flow of information through the system under development (including: data inputs and connections to the system; transmission of data between system components; storage of information; access to databases and other types of storage; connections to other systems and applications; connections to application data from other systems; and security of information outputs).
- Consideration of the full range of security controls to protect live data (policies, methods, procedures, devices or programmed mechanisms intended to protect the confidentiality, integrity or availability of information).
- Identification of specific security controls required by particular business processes supported by the system under development (encryption of sensitive information).
- Evaluation of how and where security controls are to be applied (by developing security architecture for the system under development).
- Review of designs to ensure security controls are specified, and are compliant with organizational security requirements.
- Documentation of security controls that do not fully meet EPB's requirements.
- Development of a security architecture that can support the technical system requirements, such as flexibility or scalability.
- Consideration of how individual security controls (manual and automated) work together to produce an integrated set of controls.
- Provide in dept multiple layers of protection to avoid reliance on one type or method of security control.
- Consider input from external systems as insecure and addressed as such.
- Ensure repeat of client validation at the server, to defend against 'man in the middle' attacks.
- Ensure key components 'fail securely' (in the event of a system failure, information is not accessible to unauthorized individuals, and cannot be tampered with or modified).
- Minimize privileges granted to a user or a process when accessing the system.
- Ensure all data is to be encrypted across any public or none secured data networks.

Procurement (Vendor/device selection) Stage

- Using information and classifications developed in the Design Phase, an RFP was developed to solicit responses for an AMI solution that would utilize our substantial investment in our fiber optic network thus positioning our future investments in AMI and Smart Grid technologies on a platform that will allow substantial logical and physical growth and be less subject to obsolescence into the foreseeable future, unlike platforms based on power line carrier (PLC) or Radio Frequency (RF) wireless.
- The RFP included security requirements based upon AMI-SEC ASAP standards for cyber security. Vendor responses were evaluated in part on their ability to meet these standards in the general categories of confidentiality, integrity and availability of their systems and customer data. Vendor responses were evaluated on their ability to satisfy AMI-SEC ASAP requirements for software development, procurement and installation.
- Our vendor of choice is an auditing member of AMI-SEC and thus well versed on that task force's cyber security standards, as well as a DOE approved guiding entity for the development and management of AMI centric security standards. Standards adhered to throughout the systems and application includes AMI-SEC System Security, NIST 800-14 and the Information Security Forum's "Standards for Good Practice".



- Additionally, the product chosen utilizes specific subcomponents of the following standards with respect to security, authentication and encryption: ANSI C12.18,19,21, Metering protocol standards; NERC CIP-005-1 and 007-1; AES symmetrical encryption standard; RSA asymmetrical encryption standard; Secure Shell SSH-2.
- Each device subcomponent of the product (WAN devices, infrastructure, data; LAN devices, infrastructure, data; HAN devices) implements controls in its architecture to address the three areas of interest of Confidentiality, Integrity and Availability.
- An Escrow agreement to give EPB possession of intellectual property that makes up the products is in place between EPB and the chosen vendor to mitigate the risk of the vendor ceasing to exist

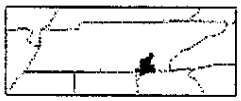
The AMI system is being deployed in a 1000 meter proof-of-concept phase and will proceed to full deployment upon successful completion of a thorough Systems Acceptance Test. A Summary of processes performed during this phase is listed below.

Smart Grid AMI Installation Stage

- Evaluated vendor configuration and altered deployment to meet North American Electric Reliability Corporation (NERC) and AMI-SEC ASAP security guide line requirements. This was done to meet a higher standard of network security beyond the vendor's standard deployment guide.
- Separated all the Smart Grid and AMI server resources into three different segmented network security groups to provide defense in depth by isolating network traffic to prevent an attacker from gaining access by bypassing one network level.
- Isolate network traffic to each domain network to only allow specified protocols through the secured firewalls. This was done to limit the number of open protocols that would be exposed.
- Restrict AMI devices to only assign IP addressing by IEEE OUI company ID assignments. This meets the ANSI/IEEE 802 and ISO/IEC 8802 standards. (By restricting DHCP assignment by requiring Organization Company ID (OUI) limits the chance of an attacker getting assigned an IP address).
- AMI devices can only transmit data to designated servers over encrypted protocols to limit the ability of attack via MAC spoofing. Only authorized protocols are allowed to send data to designated servers.
- The AMI and Smart Grid servers will ignore all traffic that doesn't have embedded software ID. (This was done in case an attacker gains access to one of the assigned IP addresses).
- All internal network traffic is blocked access to the AMI and Smart Grid networks other than the established infrastructure that is required to provide system data. (This security feature was put into place to prevent internal tampering from employees, hackers using worms or spyware to penetrate internal systems).
- All AMI and Smart Grid networks are three layers deep behind multiple firewalls and routers using Access Control Lists (ACL's).providing further layers of protection from both external (internet) and internal networks.
- A test lab was created to test, certify configuration, software design and security penetration of all the systems.

Commissioning Stage

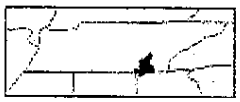
- The Supervisory Control and Data Acquisition (SCADA) system controls the electrical network systems in the field to provide secure control of our substations.
- North American Electric Reliability Corporation (NERC) and National Infrastructure Protection Plan (NIPP) provide the unifying structure for the integration of critical infrastructures and key resources (CI/KR).
- CI/KR guidelines have been followed to provide a secure network platform.



- All data is separated into multiple Virtual LAN (VLANS) IEEE 802.1q standards to provide separation of data.
- Each segment of network has a separate Quality of Service (QOS) IEEE 802.1p and 802.1q standard defined to guarantee that high level data is transmitted at the correct priory order.
- All network segments of the Smart Grid network have multiple fiber paths to reduce the chance of losing network connectivity to any part of the network.
- Both the Smart Grid and AMI networks are isolated into separate domain networks secured by multiple firewalls in a layered environment for maximum protection.
- The AMI segment meets the AMI-SEC System Security V1.01 (DOE approved) and NIST 800-14, NERC CIP-00501 and NERC CIP-007-1 requirements.
- Data encryption between the AMI devices utilizes SSH-2 over TCP/IP to provide a secure tunnel to the servers. The SSH V2 standard meets the Advanced Encryption Standard (AES) using 1024-bit and RSA keys to guarantee data security.
- All aspects of the Smart Grid/AMI network are monitored and set to alert engineering personnel; see the "Monitoring and Notifications" section for more detail.

Maintenance and Support Stage

- Aforementioned various guidelines and best practices are used for maintaining the confidentiality, integrity and availability of systems, application delivery, network infrastructure and devices.
- Contracts with vendors are maintained on all mission critical software, systems, servers, appliances and devices. High level assets are supported by 24/7 vendor contracts.
- In general updates to software, servers, appliances and devices are first rigorously tested for both production issues and possible security flaws in the Change Management Lab. Update processes include but are not limited to:
- Updates on firmware to devices are completed regularly to correct known bugs and security issues. Firmware updates can be rolled back and cannot be performed locally but only through secure access via a network server.
- Updates to the software along with security patches to servers protect systems from known security threats. Software updates can be rolled back and may be performed only by personnel who can provide privileged user credentials including key, certificate and pass phrase.
- Replacement of failed or older equipment, switches, routers, servers, drives, power supplies is performed on an as-needed basis.
- Adding of new devices to the networks.
- Installing new supported routes, ACL's, NAT rules and firewall rules.
- Updating control systems to better automate any high availability process.
- Monitoring of all systems and configuring to distribute alerts to the appropriate engineer.
- Normal system maintenance.
- Periodically conducting penetration tests.
- Access control changes.
- Periodic internal and external audits of system user access and rights.
- Scans of the systems looking for spyware, viruses, worms and malware.
- Updating infrastructure to support new or existing systems.
- Extending the LAN, WAN and HAN network infrastructure.
- Adding new system controls to increase availability and stability.
- Design and testing of new communication devices in the production environment.
- Maintaining the IP infrastructure.
- Updating documentation and network drawings.



Cyber security criteria used for vendor, device selection

(see vendor stage above)

2) Summary of relevant cyber security best practices that will be followed:

- National Infrastructure Protection Plan (NIPP).
- Department of Homeland Security Control Systems Security Program.
- National Institute of Standards and Technology Special Publication (NIST SP) 800-39, and NIST SP 800-53.
- Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) and FIPS 199.
- Advanced Metering Infrastructure (AMI) System Security Requirements.
- North American Electric Reliability Corporation (NERC) Security Guidelines and Critical Infrastructure Protection Standards (CIP-002 through CIP-009) for the Electricity Sector.
- Information systems Audit and Control Association (ISACA).
- Control Objects for Information and Related Technologies (COBIT).
- National Infrastructure Protection Plan Control System Security, Standards and Best Practices, assessment tools (CSVA, CS2SAT, DHS/NIST National Vulnerability Database)and Los Alamos National Labs (LANL) Cyber Security Requirements Guidelines for Contractors.
- SANS Software Security Institute Application Security Procurement Language Standards.
- SANS Institute Consensus Audit Guidelines 20 Critical Security Controls.

3) Summary of how the project will support emerging SG standards

Using NIPP guidelines for Long Term Cyber Security:

- Participation in the various Cross Sector working group programs (CIP CS, Software Assurance, Control System Security, Standards and Best Practices), forums (GFIRST, CSCSCWG, NCRCG) and assessment tools (CSVA, CS2SAT, DHS/NIST National Vulnerability Database)
- Participate in information sharing and awareness via interagency coordination such as FBI Cyber Task Force, Infraguard program.
- Participating in various DHS Cyber Security Awareness and Analysis Center activities including National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Participation in the DHS Cyberspace Emerging Readiness (US-CERT) program.
- Adherence to DHS IT Security Essential Body of Knowledge (EBK) for training purposes and IT workforce security development.
- Participation in energy sector compliance programs including North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards.
- Adhere to the NIPP Risk Management Framework's continuous feedback loop to provide continual improvement to enhance protection of Critical Infrastructure and Key Resources.