



WHITE PAPER

Security and the Auburn Electric AMI System

As Auburn Electric plans for the new AMI (Automated Metering Infrastructure) system and the installation of new meters to replace the ones currently being used, we wanted to address any concerns that residents or businesses may have about the security of the new meter system and the data that is collected.

Your security and that of our network has been a primary consideration since the earliest planning stages. The SmartGRID system we chose (called Tantalus) was selected chosen for two primary reasons:

- **Compatibility:** Tantalus is able to integrate well with the existing Auburn communication infrastructure, making it is easier to understand, monitor and control.
- **Stringent Security Standards:** Tantalus has a set of security standards for the communication and storage of data in their system. These standards – which include both leading industry and federal government practices – include (but are not limited to) the following:
 - NERC CIP-005-1 Cyber Security — Electronic Security Perimeter(s)
 - NERC CIP-007-1 Cyber Security — Systems Security Management
 - ANSI C12.18, 19, 21, Metering protocol standards
 - SHA-2 Secure Hash Standard
 - AES symmetrical encryption standard
 - RSA asymmetrical encryption standard
 - Secure Shell SSH-2
 - NIST IR 7628 Volumes 1,2, and 3
 - AMI-SEC System Security Requirements v1.01 with AMI-SEC Security Profile v2.0
 - NIST 800-14 Principles and Practices for Securing Information Technology Systems
 - The Information Security Forum’s “Standards for Good Practice”
 - NIST IR 7628 Volumes 1,2, and 3
 - AMI-SEC System Security Requirements v1.01 with AMI-SEC Security Profile v2.0
 - NIST 800-82 Guide to SCADA and Industrial Control Systems Security
 - NIST 800-53 Security Controls for Federal Information Systems and Organizations
 - NIST 800-14 Principles and Practices for Securing Information Technology Systems

Firewalls

Auburn Electric then took additional measures to ensure the system met with the City’s strict security measures. To begin with, we designed the network with multiple firewalls to separate the different components of the system. This design approach ensures that only necessary traffic is allowed to pass through the various firewalls. Additionally, the data that does pass through the firewalls is either encrypted or is part of a secured shell connection that only allows data between known devices.

Monitoring

While extremely confident of the firewall infrastructure, we’ve also made it part of our standard practice to monitor the system at all times and at multiple touchpoints.

Below are a handful of examples of how Auburn Electric is alerted to any actions outside of the normal metering activities:

- An alarm is immediately activated to alert Auburn Electric if a meter is tampered with, an ONT is opened or a device is disconnected from an ONT.
- All servers are located in the city's data centers and require both card access and biometric identification to enter.
- Video monitoring verifies only approved personnel enter the data centers.
- Port monitoring of all switches ensures any unplugged device automatically activates an alarm and electronically reports and records the incident.

Access

Access to the SmartGRID is restricted to users that need various types of information. There are two types of users:

- Individuals who need access to the Auburn AMI Network (meters, collectors, servers, etc.)
- Users who need access to the consumption information

As a additional level of security precaution, individuals who require access may only access the information that is relevant for their job or role. For example, an electric department lineman may need access to know if your meter is energized, however he or she can only view that information and not other information, such as the amount of electricity you've used over the last six months, that is inconsequential to the task at hand.

Security Testing

In addition to ensure the network meets the security standards established by Auburn Electric, Auburn Essential Services and the City of Auburn's IT Division, we've contracted an independent security consultant to test the system and provide any additional recommendations to preserve the integrity of the system for both the city, our municipality and our customers.