live display. The information includes market prices for the hour ahead, day ahead, and emergency status. The system can be programmed to take automatic action to curtail load on a price or emergency status signal.

- Energy Market Clearinghouse Markets. The system can provide live load reduction to the clearinghouse from the substation metering and utility baseline calculations.
- Customer. The system communicates to the customer the status of Demand Response events and provides a mechanism for the utility to send messages in the case of an emergency or high energy price event. In addition, the system provides direct and automatic demand response control.

CYBER SECURITY

Risk Management

Cyber Security Rick Identification

- To identify cyber security risks, PCS employs several methods. First at the outer edge of our network boundaries we have engaged the security company, SecureWorks. We utilize the SecureWorks Managed Intrusion Prevention and Detection Service. This service is delivered via an NSS-approved IPS appliance that is managed by SecureWorks. This system performs deep packed inspection to all traffic that flows into and out of PCS networks. SecureWorks also provides continuous research and update of attack signatures and installs them when new threats are discovered.
- SecureWorks also maintains a security research group that can map the latest vulnerabilities and real-world threats and update our monitoring equipment at the earliest possible time. The service provided gives us actionable information that is tailored to our environment, early warnings to emerging threats, remediation information and ongoing threat and vulnerability analysis.
- Internally a second Intrusion Protection System (IPS) is in place to monitor activity on the inside of the network and report on any suspicious activities or processes.

Cyber Security Rick Mitigation

- Risk mitigation begins at the start of all projects and processes for PCS. Security is part of the initial planning process for hardware staging, application development and all processes in the data center.
- PCS has been ranked as a Payment Card Industry (PCI) service center and must meet the highest level of security standards the PCI organization requires. This level of standard covers all aspects of the processes at PCS and provides for the highest level of logging, monitoring, alarm and notification available today. PCS also meets the Payment Application Data Security Standard (PA-DSS) requirements for application development security standards. PCS also only does business, regarding credit card transactions, with PCI approved payment card processors.
- The PCI standard meets and in some places exceeds the requirements in the NERC CIP standard that governs cyber security aspects of electric system operations.

Security Criteria Utilized

The core of the load control management system (PCI DSS) that PCS uses is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

- Build and Maintain a Secure Network
  - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data

  - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - *Requirement 3:* Protect stored cardholder data
  - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - *Requirement 5:* Use and regularly update anti-virus software
  - *Requirement 6:* Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - *Requirement 7:* Restrict access to cardholder data by business need-to-know
  - *Requirement 8:* Assign a unique ID to each person with computer access
  - *Requirement 9:* Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - *Requirement 10:* Track and monitor all access to network resources and cardholder data
  - *Requirement 11:* Regularly test security systems and processes
- Maintain an Information Security Policy
    - *Requirement 12:* Maintain a policy that addresses information security

Cyber Security Standards

The relevant security standards that PCS uses are as follows:

- The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.
- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
- Because of the PCI requirements, PCS and the data center is audited annually by a PCI certified security assessor. These assessors are qualified by the PCI organization and they are under continual certification process with PCI. Only PCI approved Qualified Security Assessor (QSA) are able to perform the annual audit of PCS and our data center.

Support of Emerging Smart Grid Security Standards

The solution proposed uses open standards extensively and has been certified interoperable with a number of standard utility systems.

- The Yukon® master station makes wide use of IP communications, allowing browser-based interfaces; web calls from foreign systems; distributed, as well as virtual, client/server architecture; and IP-based communications to transmitters such as substation injectors and paging terminals. In addition, Yukon® utilizes SQL databases, accessible via IP, allowing flexible data access for both reporting and/or connectivity. The interoperability of Yukon® is unmatched. Yukon®'s data can obtained by any utility system via a number of open methods including: MultiSpeak 3.0 web service interfaces; Cooper's Real-time Data EXchange (RDEX), which is an open, published API; the ability of the master to be polled via the industry standard DNP 3.0; the acceptance of contact closures for event-based actuation; views within SQL databases; published MDM interfaces; and browser/web calls directly into Yukon's user interfaces. Cooper also uses

open protocols such as DNP and IEC 61850 to perform Distribution Automation applications such as substation or feeder monitoring and control. Yukon® can even utilize IP and ANSI protocols to perform communications directly to commercial meters such as the TransData Mark IV and Itron SENTINEL.

- The Cannon AMI system from Cooper provides open standards access to both the head end software and the metering endpoint. The field equipment supports open standards such as TCP/IP and/or ANSI C12.19 to communicate to connected metering devices. The PLC technology itself is highly optimized for the physics and environment of the power line. Highly specialized equipment is required to couple to the power grid and special algorithms and circuits are utilized to transmit messages in parallel with the delivery of 60 Hz power. The protocols used by Cooper maximize the payload size and transmission capacity of the system, allowing users with large, dispersed service territories to quickly collect vast amounts of advanced operational information with little latency.
- At the endpoints, open protocols such as ANSI are used to access data from high-end polyphase and single-phase meters such as the Landis+Gyr S4e, the Elster A3 ALPHA, the Itron SENTINEL, the Landis+Gyr FOCUS, etc. The MCT-470 microRTU endpoint can make use of the open DNP protocol to communicate with downline devices such as reclosers and regulators. Cooper's UtilityPRO™ thermostat/In-Home-Display is currently undergoing ZigBee and Smart Energy Profile standards certification testing and can facilitate consumer messaging, information presentation, and control.

The capability of the components and systems of the load control management system will be updated to meet future security requirements or technologies. PSC will not run equipment that is not under full manufacturer's warranty. These warranties ensure that the equipment will be kept up to date and current. Any equipment that falls out of warranty is removed from active service in the data center.

Cyber Security Testing and Review

- PCS has the appropriate policies in effect and adequate controls and the necessary monitoring in place to confirm the enforcement and application of the policies.
- The annual audit includes actual penetration testing from external and internal points to confirm that the systems in place are working as designed and are being maintained properly by PCS staff.

Vendor and Device Selection Criteria

Cooper Power Systems has long been a provider of comprehensive reliability and productivity solutions for utility, commercial and industrial customers. The Energy Automation Solutions (EAS) group within Cooper Power Systems is a leading provider of innovative Smart Grid technologies and solutions that enable customers to optimize their distribution grid performance. These solutions include Advanced Metering Infrastructure (AMI), Demand Response (DR), Smart Sensors, Power Systems Engineering Software, Substation Automation and Feeder Automation.

PCS is uniquely qualified to host the Yukon® software and provide the support and security that will make the project a success. PCS has over 27 years of experience in delivering application software and services to the utility industry. It can meet the cyber security standards demanded in the industry. PCS was the first third-party host of Cooper's Yukon® software. The company has hosted application software for utilities for over 8 years and has worked with municipal utilities, RECs, and utility districts from Alaska to Bermuda. Its location in Iowa is an obvious advantage for project management and cost control.

Standards/Best Practices

Employee Practices and Polices

- Cooper is constantly testing the security of its software and communications systems to mitigate security concerns. In addition to internal testing, Cooper's Yukon® platform undergoes outside third party vulnerability testing.
- All developers undergo routine cyber-security training to ensure product designs are robust, including training on the NERC-CIP requirements and how they apply to both the utility and the solutions offered to the utility. Employees are aware of the requirements and will comply with guidelines outlined by our utility customers to ensure compliance.
- Cooper's employee conduct policy includes provisions for the security of remote access to our users' systems and is also subject to additional requests from our utility users.

System Software

- Yukon® uses items such as login/permission protections, role-based security, user authentication via LDAP and Active-Directory, Secure Socket Layers, firewalls, Virtual Private Networks, etc. Use of Antivirus protections and installation of OS security patches are encouraged, and Cooper tests our software in conjunction with these tools. Yukon® is specifically designed to fit into existing utility IT environments. All users must be authenticated and all user activities are logged.

Demand Response System

- The Demand Response system utilizes the FlexNet 900Mhz communication system to communication to the programmable communicating thermostats. The FlexNet protocol requires that all transmitting and receiving devices include the FlexNet authentication and encryption chip as part of the solution. All device Ids and commands are encrypted within this protocol. No consumer privacy information is communicated over this network to the end devices.

System Components

- Power Line Carrier technology is extremely secure and the information transmitted in the message is merely data without any unique identifiers. No personal information is ever sent via any Power Line Carrier message. The security of the meter endpoints is enforced via the integration methods used within the Cannon AMI modules. The endpoints are polled, transmitting only when requested to by the master station. This PLC injection equipment is installed in the utility's secure substations, thus limiting unauthorized access.

Cooper can assist utilities to ensure any backhaul WAN communications subsystem meets appropriate security standards. Servers are housed within the utility's IT environment so any procedures followed to secure the utility's IT environment would apply to the Cooper supplied servers. As described previously, the Yukon® software platform utilizes a number of security methods to ensure security.

Cooper EAS also offer NERC-CIP compliant gateways, which can be used in other areas of Smart Grid deployments, where applicable.

Emerging Standards Support

Cooper and PCS have both have long and substantial histories as product and service providers to the utility industry. The companies will monitor and implement relevant standards that emerge through the National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Act of 2002 or amendments thereto.