White Paper **WP910002EN** Effective February 2017

COOPER POWER SERIES

Yukon hosted demand response deployment

Eaton, EAS—application and deployment outline

Version: 5.6
June 2016

J. Childs,
J. Benoit,
and D.Sutton
Eaton

Document audience

The document is written for IT and security personnel to understand the computing and security architecture of the Eaton Cooper Power™ series Yukon Advanced Energy Services software platform for the deployment of demand response (DR) solutions.

Document purpose

This document provides information on the deployment characteristics for a demand response system. It provides information on the architecture, system integration, and external interfaces. The purpose of each section in the document is provided below.

- **Yukon™ demand response solution**—provides an overview of DR. It includes a description of the logical elements of the Yukon system and the primary DR field equipment
- **IT deployment**—provides details on the logical architecture of the Yukon server
- **System security plan**—provides information on securing the computing environment with user class controls using role-based security and the assignment of application properties to the roles
- **Personnel**—summarizes the personnel policies within Eaton with respect to technical services personnel and system administrators
- **Software development lifecycle**—describes the software development practices and how security is designed into Yukon
- **Application and data server network architecture**—describes the multi-tier architecture of Yukon and the secure deployment configuration. Describes Eaton hosting environment configuration for systems
- **Communication with field devices**—provides information on the communication between Yukon and DR devices
- **Change history**—summary of the change history of the document

Yukon demand response solution

Yukon demand management is a suite of applications that interoperate together to provide a utility company's customers with the ability to manage demand, and in the process, provide emergency, energy, and capacity management to the utility. There are retail users (switches and smart thermostats in residential housing), small commercial users (switches and smart thermostats), and large commercial and industrial users (gateways, direct EMS/BCS links, and direct control devices).

The Yukon software provides the tools to effectively manage a demand response program. More specifically, it provides both automated DR and messaging options. In automated DR situations, Yukon initiates a signal to adjust the load profile of air conditioners, pool pumps, water heaters, motors, and other industrial loads. It can also signal building control systems or perform load management function or turn on customer-owned generation. Messaging refers to the software initiating messages to provide the customer with information and notification messages detailing curtailment and real-time pricing information. Both automated DR and messaging can be initiated by an operator or automatically using a dynamic trigger.

Yukon design emphasis has been placed on integration to other systems because of the diverse needs of today's utility operation center. The master station is built to work as a stand-alone system or in concert with SCADA, EMS, CIS, Work Order Management, Inventory Control and Outage Management. Supported interfaces are documented in Eaton EMS/SCADA interface technical note.

Yukon provides a Web-based front-end client for administrative, help desk, and end user services; a Web service channel that takes requests from the Web front end; and back office services that communicate with remote field equipment and utilities' systems as shown in **Figure 1**.

Powering Business Worldwide

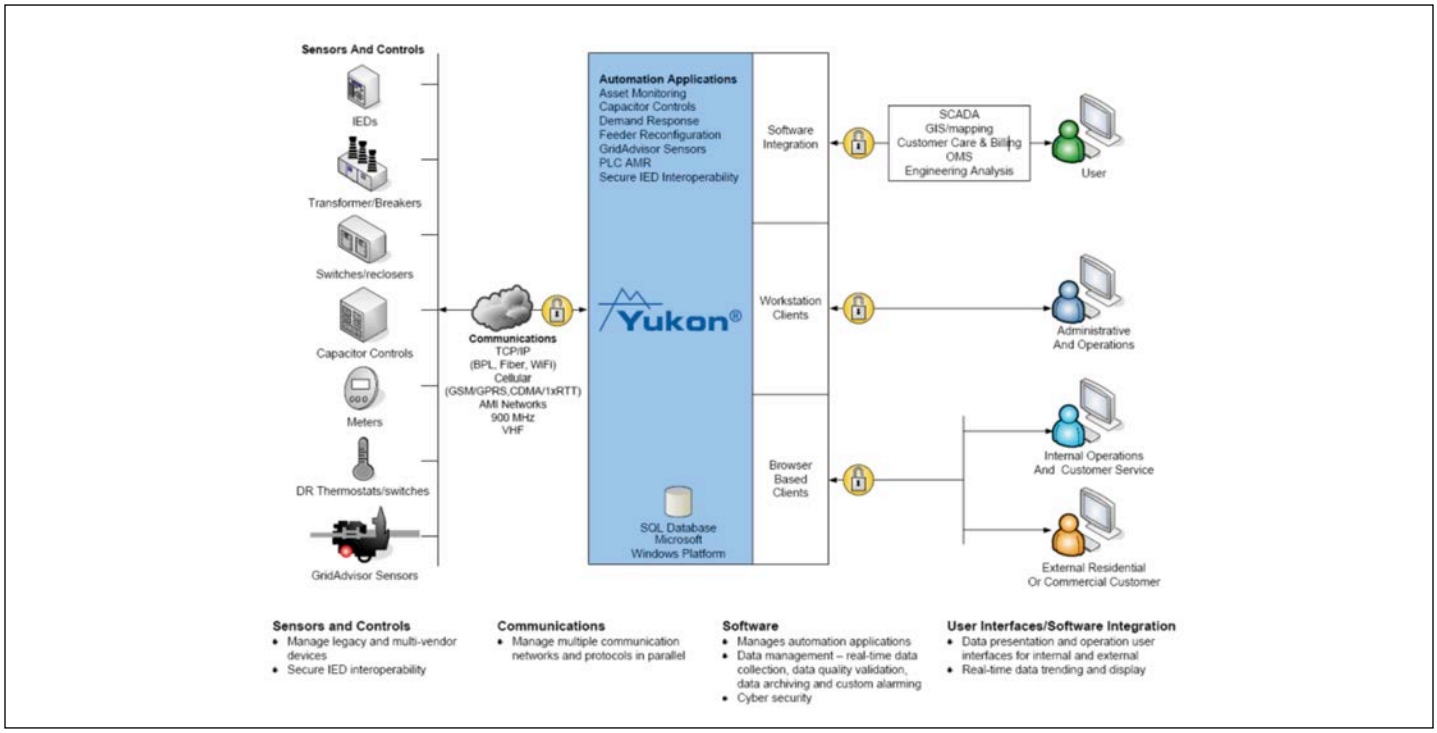

Figure 1. Yukon systems

There are three key areas of the Yukon suite that should be discussed for DR purposes:

- Web-based front end
  - Demand response operator displays
  - Customer service portal
  - Consumer portal
- Yukon background services
- System administration clients
  - Java system administration
  - Java load management setup

Web-based front end

The primary means of interacting with Yukon is through a Web browser. Yukon Web displays offer a rich and flexible solution appropriate for the many types of users that may interact with a DR deployment. Access is managed through a role-based security profile. During system commissioning, user roles are identified and mapped to role properties that define the access controls for the user classes. For example, the utility can establish separate roles and provide different functionality to DR program administrators, call center representatives, control room operators, IT system administrators, commercial load supervisors, or end-consumers.

Yukon background services

The backbone of Yukon is a set of services that contain the business logic for various processes to carry out specialized tasks and maintain interoperability of Yukon components. These crucial pieces of the Yukon master station run on a Windows® server as standard services, making Yukon deployment into an existing IT framework simple and straightforward. The servers can run together on a machine with clients in a simple "stand-alone mode" or can be distributed on dedicated servers or clusters.

The following Yukon services are typical of a DR deployment:

- **Message dispatcher**—This service is responsible for receiving and passing on messages between the server and client applications. The application's functions include real-time point management, data archiving, and alarm and event handling. Its real-time coordination improves the speed of the overall system and allows it to be set up in a distributed configuration.
- **Port control**—This service is responsible for channel management and field hardware communications. This port control sub-system can utilize communications ports for a variety of communication media.
- **Load management**—This business logic engine schedules and executes DR control strategies that have been defined by the user. It is also capable of automatic control based on real-time inputs from other systems. Additionally, it enforces any constraints or rules that may have been placed around control by a program administrator.
- **Notification**—This service is responsible for coordinating and sending messages that notify utility personnel, end-customers, and other program shareholders of control event activity. The use of such notification messages is extremely flexible and a variety of methods are supported, such as email and SMS.
- **Yukon Web server**—This service is the heart and brain of direct user interaction with Yukon. Its primary purpose is to host all browser-based interactions with Yukon, including a Web-based front-end client for administrative, help desk, and end user services. Additionally, it provides login authentication for all client applications.
- **Enterprise Integration Module (EIM)**—The EIM is an optional Web server that includes a toolkit of Web Services (WS) that provide specific Yukon DR functionality to other software applications (e.g., SCADA/EMS or other function system). The EIM service is documented in the Yukon system administrator's manual.

- **Foreign data router**—This optional service supports a large number of data point integrations with outside systems. A common DR use of general point exchanges available through this service is triggering a load management event with data from EMS or SCADA systems. The supported interfaces are documented in the EMA/SCADA integration technical note.

Yukon system administration (Java) clients

The following are the administrative Yukon client modules; each Java application is used by administrative personnel to set up and manage the system within the corporate data network. These can be used in tandem with Yukon's primary Web portals to support and maintain the system or can be isolated to specific workstations. In all cases, access to the system administration tools is controlled by the user class role properties.

- **Yukon Database Editor**—The Yukon Database Editor is used to add, modify, or remove components from the Yukon database. Components are split across several categories: core components define all shared communication that is common throughout the system, while the Load Management, Capacitor Control, and System components are specific to Load Management, Capacitor Control, or System operations and equipment respectively.
- **Yukon Scheduler**—The Yukon Scheduler allows users to create, edit, execute, and view the status of Metering and Control schedules. It is also used to change the state of a schedule, including start, stop, enable and disable, and to modify schedule information.
- **Yukon Trending**—The Yukon Trending editor allows an administrator to setup and define graphs of interval data. The module displays real-time and historical data. Multiple data points with different intervals can be displayed on a trend. The trends are displayed through the Web browser. A trend can be global or have a role property.

Demand response hardware

Direct load control switches

Eaton offers a variety of application-oriented switches, with wide configurability, choice of relay configuration, and a choice of communications.

Eaton switches have several unique strengths:

- **ExpressCom™ protocol**—The ExpressCom protocol provides advanced addressing and feature options while minimizing communication bandwidth requirements and cost. ExpressCom is supported in all Eaton devices. The value to the utility is to provide flexible control and addressing features without having to re-program installed equipment.
- **ZigBee® Smart Energy Profile 1.1**—Some Eaton switches come with a ZigBee radio and the Smart Energy Profile security and control stack for operating in an AMI network or through a home gateway.
- **Complete over-the-air programmability**—All devices are over-the-air programmable, meaning the utility can change frequencies and CAP codes to ensure best performance. The utility benefits by having a flexible communication system that can evolve as business requirements change.
- **Choices of cost-effective packaging**—Eaton offers switch technology in a multiple load enclosure, supporting the installation of up to three relays in the device chassis. The relays can be a mixture of 5 A and 30 A. This feature allows your utility to deliver cost-effective controls to customers for loads in addition to air conditioning for residential, small commercial, and industrial applications. Eaton also offers a single load, small footprint package for the quickest and most effective installation in single load, air conditioner control applications.

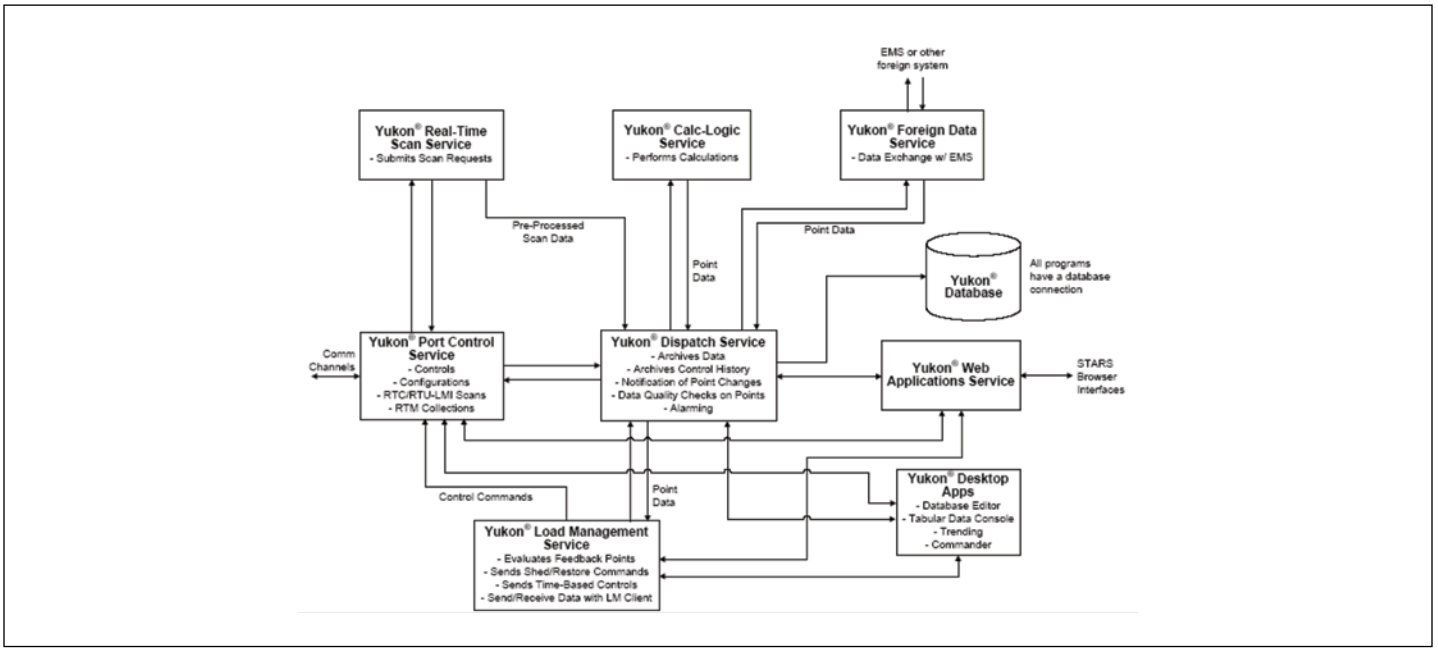

Figure 2. Yukon services

Smart thermostats

Eaton provides an interface to smart thermostats that are manufactured by third parties. Yukon is integrated to the thermostat manufacturer cloud services through APIs provided by the smart thermostat manufacturer. The smart thermostat vendor performs communication from their cloud services to the end device.

Industrial and utility gateways

Eaton offers a complete line of direct control gateway devices with flexible configurations to meet the requirements of controlling large commercial and industrial clients. The gateways support a wide range of utility and industrial protocols. All gateways include the ability to communicate to Yukon in one protocol and communicate to the end device in a separate protocol (e.g., EMS/BCS, IEDs, etc.). The gateways also include the ability to add I/O boards to collect analog and digital data and support latching and pulse relays.

IT deployment

A standard installation of Yukon consists of multiple Windows services including 1–2 Apache Tomcat Java Servlet containers, 4–5 C++ services, and potentially several Java services. The Yukon architecture is designed to be deployed in an existing IT environment. This allows Yukon to take advantage of existing disaster recovery, high availability, backup policies, and security policies used with similar enterprise platforms at the utility or hosting site.

Security

For details about security in Yukon, please see the system security plan section.

An important note for deployments that may not have a security or IT policy for Tomcat: Apache can be used as a front door to different Tomcats for different URL namespaces (/app1/, /app2/, /app3/, or virtual hosts). The Tomcats can then be each in a protected area and from a security point of view; you only need to worry about the Apache server. Essentially, Apache becomes a smart proxy server.

Database

The Java applications use a JDBC driver for database connectivity. The server side applications use a third-party database access library. Yukon supports the following database software:

- SQL server
- Oracle

Note: Eaton publishes a Platform Validation Matrix documenting version support of OS, database, and browser covering current and future release plans.

Communication between the Yukon services and the database can be configured with encryption so that all requests and responses are not visible on the sub-network between the application server and the database server. The encryption can be disabled to support system troubleshooting.

As indicated by the above list, the Yukon database requires an Oracle or Microsoft® SQL server environment. In many instances, the system is integrated into the utility's existing RDBMS environment. The server platform for Oracle can be UNIX or Microsoft Windows based. Disk storage requirements are driven mostly by the count, duration, and frequency of interval data stored in the system. A typical configuration includes:

- Windows server 2012 R2
- SQL server 2014 Standard 5 CAL license
- CPU: 32 Logical cores from at least 4 physical cores
- RAM: 64 G
- C: OS—300G Raid 1
- D: Data Drives—1TB Raid 10 (per 25,000 nodes for 13 months online data)
- E: DB Logs drive—300G Raid 1
- F: Page File: 300G Raid 1
- G: Backup Drive—2 TB Raid 1 (this drive size may change based on the size of the backups once a final archive days to keep has been determined)

Notes: D: and E: Drives should be solid-state drives for higher performance. Detailed minimum database server hardware requirements are published at least annually based on internal testing with currently supported RBMS versions. The database server requirements are sensitive to application functionality, interval data, and the number of simultaneous users.

Web server and application interfaces

Yukon supports the following Internet browsers:

- Internet® Explorer®
- Mozilla Firefox™

Note: Eaton publishes a Platform Validation Matrix documenting version support of OS, database, and browser covering current and future release plans.

Yukon's Web-based front end is specifically designed to avoid using browser plug-ins due to potential deployment problems in some utility environments. However, some portions of Yukon require the use of cookies to function correctly. Session information such as the user's main entry page and also the re-direct on logoff is saved in a cookie pushed to the user's machine.

The browser clients have been designed for the daily use of the system. Functionality for customer service, system operators, and end user access if provided by the utility are all available through the browser-based clients. The browser client applications are all JSP/Servlet-based, much of it based on the Spring model. Set up and administration of the system is mainly performed through a suite of Java-based applications. These applications are available from the browser through the use of Java WebStart. Additionally, they are part of the standard platform installation and may be placed locally on multiple machines. Typical installations deploy these programs locally on the application server and again on the system administrator's machine.

Apache Tomcat is the primary Web server used by the Yukon Web application service. There are several ways that this Web server can be used. It can be installed in the utility's DMZ directly and given a TCP/IP connection to the Yukon application server. A second installation option is to leave the Web server on the Yukon application server and deploy a Web server in the DMZ (such as IIS) to pass through the data requests to the Yukon application server.

Additionally, the Enterprise Integration Module (EIM) portion of Yukon is designed to be deployed within Tomcat. The installation options of this auxiliary Web server are exactly the same as those described above for Yukon's primary Web server. The Yukon EIM offers a set of SOAP-based Web Service calls that provide information and data interaction when an outside client application makes a request to them.

Web server hardware requirements are dependent on the expected number of users. For most installations, the Web servers are installed on the application server. If the specific solution includes access to the system by 50 or more simultaneous users, a separate hardware server for Web functionality should be provided. This hardware server can be configured in a similar fashion to the application server described in the next sub-section.

Application server

The Yukon platform requires an application server. As mentioned above, the application server typically houses the Web server, as well. It will also house the communication and business logic applications. The Yukon application server runs on the Microsoft Windows platform and operates on server hardware supplied by the major equipment providers. Equipment can be acquired by the utility. The minimum system requirements include:

- Application Server (all Yukon and Network Management Services)
- OS: Windows server 2012R2
- CPU: 16 Logical cores from at least 2 physical processors
- RAM: 32G
- C: OS: 300G Raid 1
- D: Application: 300G Raid 10
- E: Page File: 300G Raid 1

Dual network adapters are recommended with the backbone between the application server and the DB server being a minimum of 1 Gb with 10 Gb recommended.

Note: Detailed minimum application server hardware requirements are published at least annually based on internal testing with currently supported OS, Tomcat, and Yukon services. The application server requirements are sensitive to application functionality and the number of simultaneous users.

Network

Communication between the application portions of Yukon is performed using TCP/IP connections. As stated above, the connection between the Yukon services and the database supports data encryption.

The network bandwidth requirements are minor traffic in a typical deployment. In Eaton's central hosted environment, a T1 supplies all connectivity for 15–20 separate Yukon systems. The bandwidth is monitored and has never approached a level that would cause alarm.

Yukon does not produce additional network traffic during the execution of specific processes in measurable amounts. The number of simultaneous users affects the network traffic more than a specific process.

High availability

Numerous Yukon installations have been performed on fault tolerant hardware platforms that include RAID disk storage, redundant power supplies and other components to reduce increase system reliability.

The Yukon platform has also been deployed in both Microsoft and Veritas clustering environments. While the Yukon applications do not report their health directly to the cluster, the clustering software is given control over starting and stopping the applications. This allows the cluster to control which node is active on the system.

Yukon has also been deployed on the NEC fault tolerant server platform.

Yukon platform validation matrix

A minimum system requirements chart is provided with each release of the software. This chart details operating systems, databases, and browsers used for the validation of that particular release. A longer term testing matrix is updated annually to contain the expected support for these system items in upcoming releases. Eaton makes these documents available through our customer service website to allow for better planning of upgrades and maintenance schedules.

Hosting services

Eaton hosting services are designed for customers that are running mission-critical, real-time applications. Examples of these applications include: Price Response Systems, Demand Response Systems, Distribution Automation, Distributed Generation Management, and any application where dispatch or communications with field devices is required. The following describes the basic hosting environment. Additional functionality can be provided, but requires statement of work and change order.

- **Connectivity.** The facility is connected to the Internet over multiple Ethernet connections with self-healing automatic redundant paths. This network is connected to multiple peering points on the Internet, allowing for a high degree of redundancy and routing flexibility. The facility uses managed bandwidth and Border Gateway Protocol (BGP) routing across redundant Internet backbone connections with multiple Tier 1 carriers. The facility has redundant fiber entrances and is carrier neutral.
- **Firewall/router and internal network protection.** The facility uses a combination of technical platforms to counterattack known methods of compromising the core network. Technologies include firewalls and load balancers. Firewalls are used to restrict access to the network and filters have been added to the routers and switches. IP restrictions and username/password authentication are used where appropriate. The facility is actively monitored using intrusion detection, to detect and respond to intrusion attempts. These methods individually and in conjunction with each other provide the highest level of security. The internal network is protected by state-of-the-art firewall and layer 4 switching technology for maximum availability and uptime. All core services are complete and n+1 redundant, providing maximum fault tolerance.
- **Facility power.** The facility is powered by two separate power grids and equipped with multiple redundant full-time inline uninterruptible power supply (UPS) systems. In addition, backup generators are located on-site in the event of a sustained electrical outage.
- **Server monitoring.** CPU, file systems space, swap space, and memory utilization will be monitored and alarmed. The system will undergo constant pinging. The hosting facility will troubleshoot and attempt to resolve any operating system related problems identified by server monitoring.
  - Alarms are based on critical thresholds identified for the CPU, file systems, swap space, and memory
  - Server monitoring verifies that data is being posted and the server is alive. It does not guarantee data validity and does not monitor log files
  - Network pinging provides confirmation that the customer's equipment is responding at the network level
- **Virus protection and software update.** Virus protection software looks for updates, and installs the same, approximately every four hours. We release all security updates of platform software monthly after testing and certification.
- **Backup-to-disk.** Backup-to-disk services provide scheduled, off-site backups of critical system data. The backup schedule includes weekly full backups and daily incremental backups of both critical application and database data. The backups are retained off-site for 14 days. The backup data is encrypted in-transit.
- **Hosting facility hours of operation.** The hosting facility is manned 24 hours a day, 7 days a week.

System hardware. The solution is an enterprise-class cloud computing Infrastructure-as-a-Service (IaaS) platform designed to support heavy compute, high memory, and high storage IO application workloads. The platform utilizes only best-in-class hardware and software from Cisco, EMC, and VMware. It was specifically designed for high availability with enterprise-class functionality and security.

System and database software. Licensor provides all software required to operate the system. This includes the operating system, Web services, and database server. The Yukon software operates on the current Microsoft Windows Server operating system. The business logic, accessing data, authenticating logins, etc. is done through several servlets. We use jsp for the presentation layer to generate dynamic html. The database engine is built upon the Microsoft SQL server technology.

System security. Eaton provides a security framework for the system for the utility's personnel, consumers, and system administration access to the system. Every system is installed with a Third Party Secure Certificate Authority SSL Certificate. All Licensee's Personnel access to the system is done through HTTPS via a Web portal. All Web portal access to the system is managed by role-based security and all changes to the system are logged with the Login ID. Licensee is given individual logon access that restricts them to access only their enrolled applications. Licensee has write capabilities to adjust only specific information about their access or enrollment. Licensee's personnel are given individual logon access that provides them with Web access to only applications and capabilities that meet their job function. Licensor's System Administrators access the system through an IPsec VPN. Licensee's personnel do not have access to the hosted virtual server, the only access provided is to the Yukon software.

A typical Eaton managed (hosted ASP) system set up is shown in **Figure 3**.

System security plan

The Yukon software platform is designed to support many of the key technologies that drive the development of the Smart Grid:

- Integrated communications
- Sensing and measurement technologies
- Advanced control methods
- Operations interfaces and decision support

Because it bridges the gap between the consumer and the utility, the Yukon software meets the availability and integrity requirements of control systems, while ensuring the confidentiality of consumer data as is expected of a business system.

To meet these requirements, Eaton has addressed the technology, policies, and procedures that provide the operational resilience required from a Smart Grid system. The security program addresses the following:

- Personnel—employee risk assessment, access to critical assets and information, security, and awareness training
- Development lifecycle—implementation of a Security Development Lifecycle, design and code reviews, configuration management, product security and robustness testing, third-party security testing
- Secure network architecture
- Role-based access control
- Maintenance—including software and security updates

Personnel

Eaton recognizes that its employees constitute a critical element of any security plan. Because many of its customers operate systems that fall under the requirements of the NERC CIP, Eaton has established an internal program called "Helping Utilities Meet NERC CIP". Key components of this program are policies that help utilities meet the CIP-003 information security and CIP-004 personnel requirements.

All Eaton employees are subject to a security assessment at the time of hiring and must comply with the Eaton substance abuse policy. Through its "EAS Security Qualified Engineering Team Policy", Eaton further ensures that all employees who perform engineering and integration work for its customers meet the CIP-004 requirements including seven-year criminal background checks, cybersecurity training, and awareness.

Through its "EAS Information Security Policy", Eaton also ensures that all employees who are exposed to confidential customer information apply the appropriate security controls.

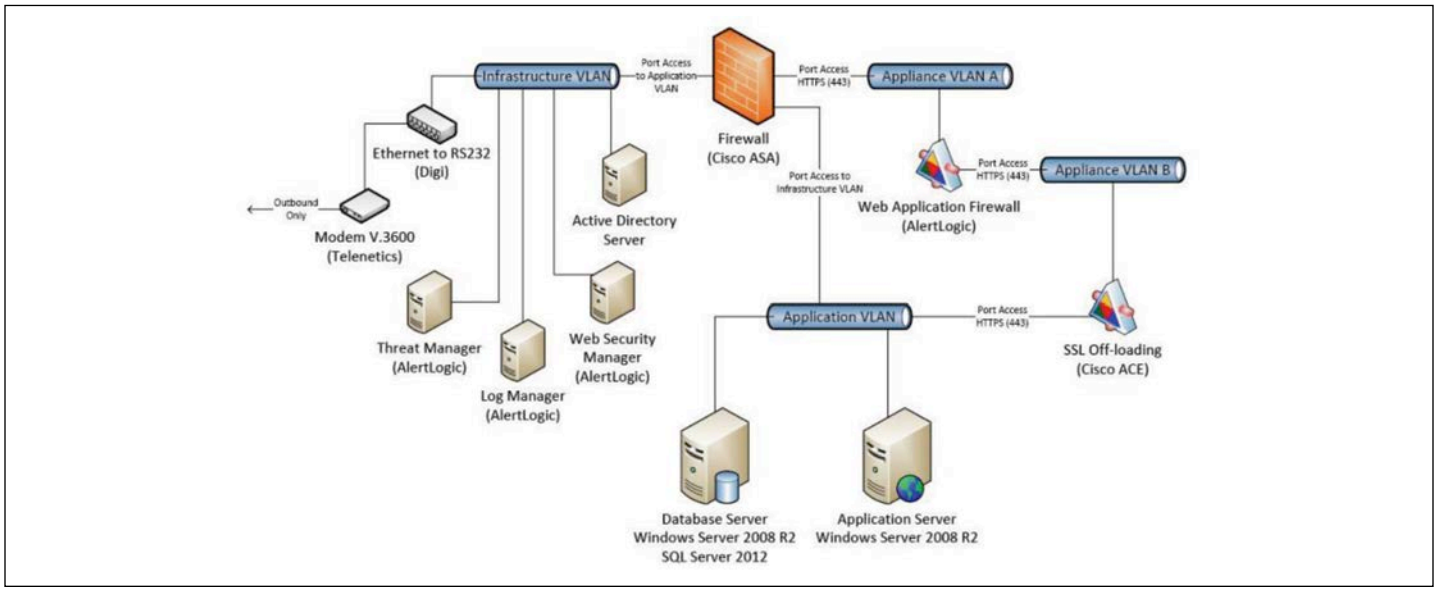

Figure 3. Typical Eaton managed (hosted ASP) system

Software development lifecycle

Security cannot be added on; it must be built in. Eaton product development teams already apply industry best practices, including security, to the development process. The Eaton quality assurance process includes security testing and secure design training for engineering staff, source code and configuration management, along with an independent security validation of Eaton enterprise applications.

Eaton has already implemented a security update validation process for its substation products. Additionally, we are integrating security and robustness testing of our network-enabled products using the Wurldtech Achilles device with the goal of achieving the Achilles certification for all applicable devices.

Eaton has implemented a constant improvement process for its Security Development Lifecycle to continue to meet its customers' security requirements with a comprehensive patch and update process, system hardening guidelines, and network architecture guidelines expanding on the policies identified in this plan.

Yukon third-party security audit

Eaton has worked with Aspect Security (www.aspectsecurity.com), both as part of a specific customer's DR deployment and within Eaton's own development cycle process, to ensure Yukon is a more secure Web-based application. Using a combination of on-site sessions and investigation in the field, Aspect:

- Performed penetration testing of Yukon's external Web portions
- Scanned access points of Yukon for common weaknesses
- Reviewed Yukon source code and policies for approaches to:
  - Session management
  - Access control
  - Input validation and encoding
  - Database security
  - Sensitive data encryption
  - Error handling
  - Logging
  - Denial of service attacks
  - Cross site scripting
- Trained Yukon developers in best practices from a security standpoint
- Trained Yukon developers and QA personnel to test using the above criteria

One of the primary goals of working with Aspect was making sure that no unauthorized user could start or stop control of devices from any Yukon access point. After a thorough investigation, Aspect's team was unable to invoke unauthorized Event Activation capabilities within Yukon. The Aspect investigators verified that all of Yukon's security controls were in place to prevent unauthorized users from any load management control interfaces through the Web application. Additionally, they made sure that no matter the access point, Yukon still required the user a) authenticate and b) be in the appropriate role before allowing access.

The Yukon software is continually updated and enhanced to support our utility customers. There are two major releases of Yukon per year and maintenance releases as necessary. Maintenance releases contain minor improvements and defect fixes. Each major release of the software is independently checked for intrusion detection and secure computing practices by the Eaton COE security group. Eaton recommends the software be updated annually to stay current with the newest features available as well as the continuous security improvements.

Application and data server network architecture

Computing environment security is critical to utility operations. Implementing a secure computing environment requires a utility-wide focus that starts with the Utility IT infrastructure, includes network access, server access, user access, communication methods, protocols, and field equipment. Any utility that deploys solutions for internal infrastructure and with external customers must be concerned about the secure operation of the system and the protection of the system from malicious attacks. Eaton has engineered Yukon to meet these requirements by making it multi-tiered, compliant with industry security standards, and by using secure and encrypted communication protocols.

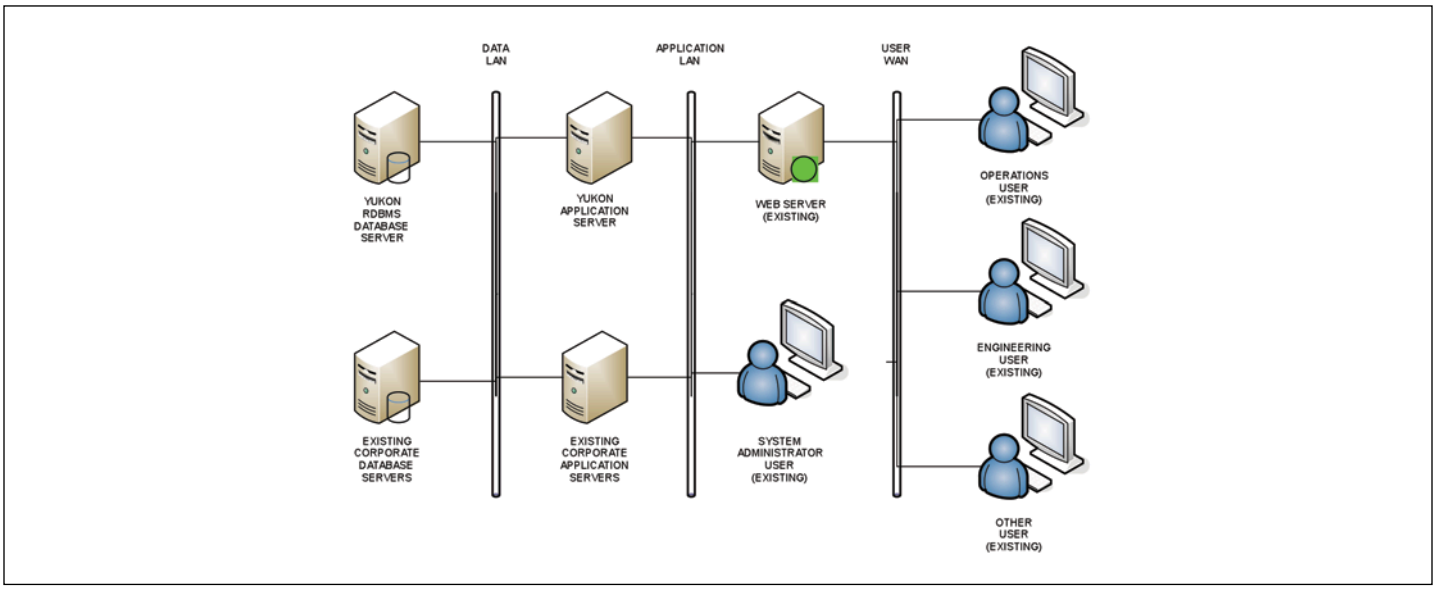

Figure 4. Application and data server network architecture

The Eaton enterprise applications protect data via authentication, authorization, and encryption. Multi-level permissions are used to authorize user actions and restrict data access. Sensitive customer data is maintained and updated via secure integration standards. User and data actions are logged for historical auditing. Data is protected during use of any Eaton application. These security features are consistent across all Eaton applications and are covered in this plan.

Yukon is built upon a three-tier computing architecture as recommended by NIST SP800-82. This architecture separates the database, application, and presentation services to independent servers and trusted security levels within the utility.

When Yukon is integrated into the utility infrastructure and becomes part of the utility-wide computing environment, it can be deployed as shown in **Figure 4**. This architecture takes full advantage of the three-tier security infrastructure by physically and logically separating the computing functions. The data layer applications are completely isolated from application processing. Database administration and system backups are accomplished as an integrated function. Only trusted and secure clients and application servers have access to the data LAN. At the Application Server level, servers are configured with two (or more) Ethernet ports. One port is dedicated to communicate over the data layer for access to the corporate computing and database resources and the other port(s) connect to trusted physically isolated clients. The final component, the presentation layer, connects users with applications. This configuration when combined with routers and firewall devices (not shown) provides a secure computing environment where levels of system access and capability can be provided to utility users that require access to applications and databases.

External Web access security

In order to provide secure communications to all Web-based users, and more specifically to the utility's customers, Yukon fully supports the use of Transport Layer Security (TLS, successor to Secure Sockets Layer, or SSL). This standard protocol, supported by all Web browsers, ensure the authenticity of the server and provides encryption for all data exchanges.

In order to implement secure communications, the utility will need to purchase a Web certificate from a Certification Authority such as VeriSign. Eaton can assist utilities in setting up their secure Web servers.

Yukon can be configured to work with additional security devices including direct VPN and SSL VPN products. The VPN products provide an additional level of security by allowing only authorized computers with access to the network. Hardware and software VPN solutions are available from multiple suppliers, and Eaton has performed integration to several packages.

Hosting security

Eaton can also deploy Yukon at a customer preferred hosting provider. Eaton requires hosting providers to provide a formal security plan that addresses the following requirements as stated by the American Recovery and Reinvestment Act of 2009 (ARRA):

- Personnel security—including security screening, behavioral observation, hiring, and penalties for security violations
- Physical and environmental protection—including the protection of physical locations, access control and monitoring, tracking of people and assets, and environmental protection (i.e., safeguarding the operating and environmental infrastructure)
- Contingency planning—including the restoration of operations in the event of a cybersecurity incident or emergency
- Configuration management—covering modifications to hardware, firmware, software, and documentation
- Maintenance—including routine and preventative maintenance, repairs, use of tools, and management of maintenance personnel
- System and information integrity—including design testing and approval, verification testing, intrusion detection and prevention, anti-virus and anti-malware screening, and security alerting
- Media protection for limiting access to physical and electronic media—including labeling, storage, transport, sanitization, and disposal
- Incident response to detect, respond to, and limit consequences—including training, testing, monitoring, and reporting
- Security awareness and training—including position-specific training, communication, and an awareness of social engineering threats

Our standard security policies meet the requirements of most utility programs. If additional security policies and or services are required, we work with our hosted service provider and the utility partner to define and agree to revisions, implementation and document within the contract.

User permissions and application access

Yukon controls user access through a series of robust permissions. Before any user request is acted upon, strict validation is applied to verify the user's authority and access rights within the application. These roles and permissions are organized by login group membership and per individual user. Each user has their own password.

The Yukon platform can currently perform password authentication, based on user lookup, against an existing Active Directory, LDAP or Radius server. This allows an IT department or hosting provider the ability to apply their preexisting password rules to their Yukon deployment. Yukon is also capable of directly controlling login security through use of login names and passwords kept in its own database. Password rules are supported that meet the current NIST recommendations and are encrypted.

Yukon's diverse user permissions allow numerous types of business and technical users to be represented. However, the majority of deployments involve the following three basic user roles:

- Administrator roles
- Customer service representative (CSR) roles
- End consumer roles

Table 1 shows an access control matrix and key functions and user level mapping examples typical at many customer sites. As mentioned before, the number of possible login group and role property combinations means many combinations of user levels and system permissions are possible, but this matrix and matching descriptions represent standard Yukon DR use.

Table 1. Access control matrix

Key functions/user levels	IT administrator	Load control operator	CSR manager/ business manager	CSR	Advanced consumer (commercial)	Typical residential consumer
Perform/monitor load control	■	■				
View application logs	■		■			
Access Yukon "heavy" clients	■					
Generate reports	■		■			
Send configuration commands	■		■			
Deactivate a switch or thermostat device	■		■	■		
Add or remove a switch or thermostat device	■		■			
Edit customer account data	■		■	■		
Add or remove a customer account	■		■			
Change account username and password	■		■	■	■ ①	■ ①
Manually adjust thermostat	■		■	■	■ ②	■ ②
Change program enrollment	■		■	■	■ ③	■ ③
Send opt out to a switch or thermostat	■		■	■	■ ④	■ ④
View control history	■		■	■	■ ⑤	■ ⑤

① An operator or administrator can change the username and password of any customer account. A consumer end-user can be given the ability to change their own username and password only.

② A consumer can only adjust the thermostat(s) on a specific assigned account; an operator or administrator can adjust the thermostat(s) of any account.

③ An operator or administrator can change enrollment on any customer account, as well as adjust the more specific addressing group attached to that program and physical relay number of the switch. A consumer end-user can only change enrollment on a single assigned customer account, and cannot alter addressing group information or relay number. A customer can change enrollment options, for example, the preferred control category or level that have been designed by the DR administrator, but cannot create new categories. A customer can enroll in a new program that will trigger notifications to the appropriate utility users to process the request that may include the requirement to install additional hardware.

④ An authorized utility user or administrator can override any device on any customer account; a consumer end-user can override the devices on a single assigned account only. All end-users can be limited to a maximum number of overrides allowed in a month or year period.

⑤ An authorized utility user or administrator can view the control history of an customer account; a consumer end-user can view the history of their assigned account only.

Key function descriptions

Perform/monitor load control

The application allows the administrator the ability to start, stop, and monitor load management programs. When a DR program is activated, the application sends out commands to devices in the field, including both thermostats and switches. The devices in the field will respond to these commands by either adjusting temperature settings, ramping set point temperature, or performing advanced cycling.

View application logs

The application allows an administrator to view the Yukon services logs through the Web browser. These logs include satellite heavy client logs, the Web service logs, and other Yukon application logs.

Access Yukon "heavy" clients

The application allows access to its "heavier" Java Swing administrative and control client applications through the Web. This access would normally only be granted to an IT or DR administrator. This functionality utilizes Java Web Start to download and run the Java Swing client application onto a local machine (although this functionality can be disabled).

Generate reports

The application allows an IT or DR administrator to generate various reports that return data from different components of the application. Depending on the report, contents may consist of raw values directly from the database, calculated values, or both.

Send configuration commands

Individual switches and thermostats have internal levels of addressing that affect communication. The application allows an administrator or high-level operator to change this addressing and reconfigure a device or devices with the updated addressing information.

Deactivate a switch or thermostat

The application allows devices, either switches or thermostats, at customer accounts to be removed from service. This can be done by a system interface with a separate application (e.g., direct interface, file import, or EIM call) or per account through the user interface.

Add or remove a switch or thermostat

The application allows devices, either switches or thermostats, to be assigned to customer accounts. Only an operator or administrator can add or remove devices. This can be done by a system interface with a separate application (e.g., direct interface, file import, or EIM call) or per account through the user interface.

Edit customer account data

The application tracks basic customer account information, such as street address. Only an operator or an administrator can both view and edit this information for any account.

Add or remove a customer account

The application allows an administrator or high-level operator to add or remove individual customer accounts. This can be done by a manual file import or per account through the user interface and is normally in tandem with the ability to Edit Customer Account Data.

Change account username and password

Every customer account in the application can be assigned a username and password that grants a consumer end-user access to that account.

Manually adjust thermostat

The application allows a consumer (end-user) or operator to manually adjust a thermostat in the consumer's home. The temperature can be raised or lowered and fan speeds adjusted through the application; these changes are then sent out to the thermostat. This also includes changing the thermostat schedule.

Change program enrollment

A consumer's thermostats and switches can be enrolled in load programs. These program enrollments determine how load control will affect those devices. The application allows an operator/administrator, or in some cases, a consumer end-user, to change the program(s) in which a switch or thermostat is enrolled.

Send opt out to a switch or thermostat

An opt out, or override, sends a temporary out-of-service command to a device, telling it to not respond to load control for a given number of days. An override example might be the request by a customer who has visitors with a medical condition or scheduled social gathering. The application allows the DR administrator to define the opt out rules.

View control history

The application allows load control history to be viewed per account. Load control history gives the duration of control for varying periods of time, organized by load program. This ability can be given to any user in the energy company but is read-only; the control history data cannot be changed.

Application logging

An effective application security policy should include a strong audit trail. Through its extensive logging capabilities, Yukon is able to record a great deal of information to various database tables and to its full application logs on the server file system. This logged information can be used for auditing purposes by program administrators and managers, as well as for technical troubleshooting.

In general, Yukon records the following attributes (where applicable to the logged transaction or application action):

- Date/timestamp of logged item
- Username performing transaction (if relevant to type of logged item)
- Type of transaction
- Account number (if relevant)
- Device identifier (if relevant)

Information logged to the database can be maintained for the life of the application. Information that is also replicated in log files can be found on the server until the end of the standard 30-day rotation of all Yukon log files.

Such logged information is extremely sensitive. Yukon will only allow viewing of logging information through its Web interfaces to users with the appropriate rights. Users with direct logon access to the Yukon Application server (generally only the IT administrator) can access the text log files on the system for archiving and management.

Communications with field devices

The Yukon platform supports a wide range of communication protocols, medium, and methods to support the needs of our utility clients. For DR solutions, the following communication technologies are currently being deployed:

- **Direct TCP/IP devices.** These devices have the IP stack within their firmware. An example of radio technology is Wi-Fi.
- **ZigBee® SEP home area network devices.** Eaton supports SEP devices on the Eaton RF Network, iDigi home network gateway, and third-party AMI networks.
- **Cellular network.** These devices connect to commercial cellular networks.
- **Eaton RF mesh network.** Eaton provides a 900 MHz RF mesh network with native ratio DR devices and ZigBee SEP HAN devices.
- **AMI networks.** Eaton supports native AMI vendor radio integration.
- **Commercial paging.** Flex 900 MHz paging and digital VHF paging.
- **Private paging.** VHF digital paging for utilities with internally owned and operated networks.
- **Power Line Carrier (PLC).** Communication over Eaton PLC network.

Figure 5 provides an overview of the communications options for residential and small commercial DR systems.

Yukon (either upon a trigger or an action by a user) creates a message to one or more field devices. Prior to transmitting the message, it is encrypted using one of the methods supported by Eaton. The field device upon receipt of the message, de-crypts the message and processes it. In all cases, the communication system between the Yukon master station and the field device comprises multiple components as follows:

- **Backhaul.** The backhaul system is the infrastructure required to get the message from Yukon to the network system. This component varies depending on the network communication type and for most network communications have several options. For example, the backhaul communication to an Eaton RF network is in many cases the Utilities fiber to a field office or distribution substation. In many cases, the backhaul communication system is protected by an additional layer of security using COTS equipment and software.
- **Network.** The network communication system can be a public communication infrastructure, for example, the Internet or a cellular network, or a privately owned utility network as in the case of a private VHF network or RF mesh network.

The sections that follow provide details on the communication system and security for each of the DR network communication types shown in **Figure 5**.

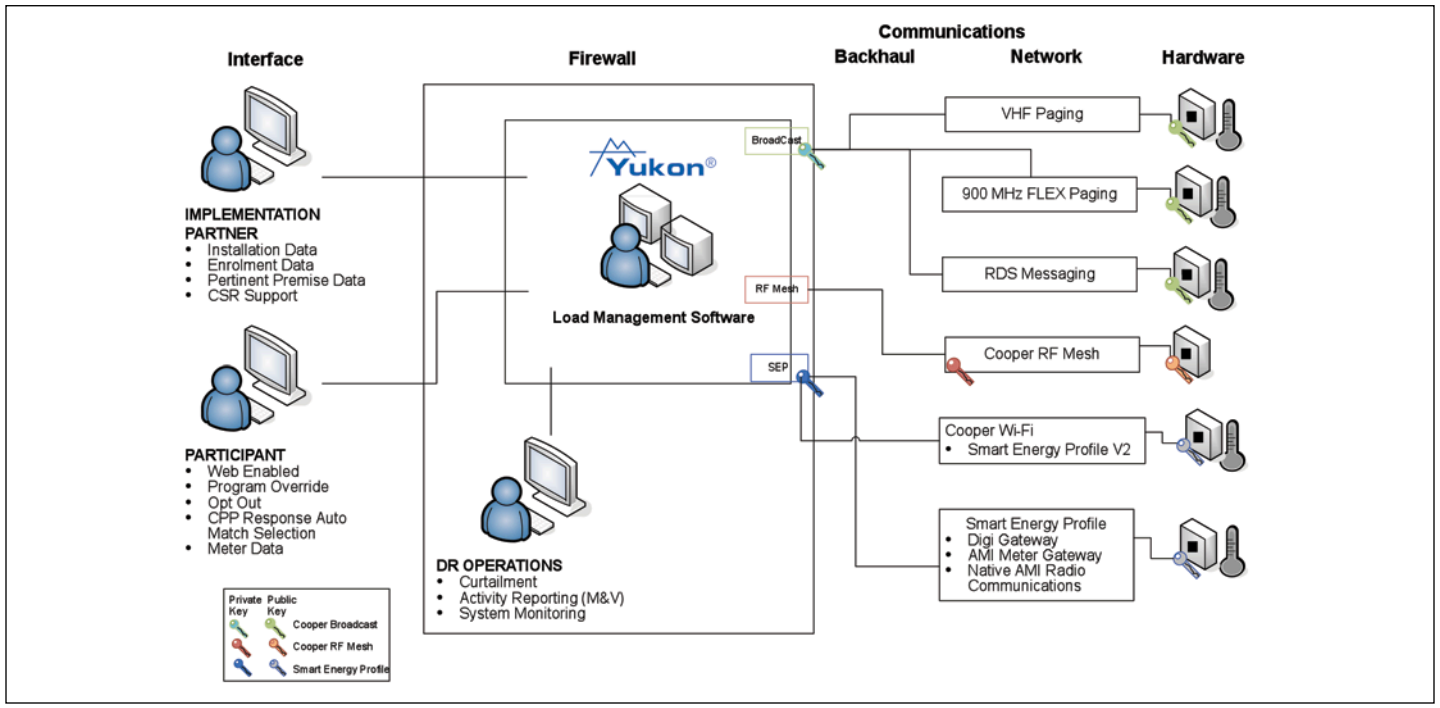

Figure 5. DR device communication overview

Broadcast DR

The majority of all mass market (residential and small commercial) DR systems use a one-way broadcast communications system to transmit DR signals from the master station to the end device. Eaton supports three broadcast communication systems:

- **VHF digital paging.** VHF paging occupies the frequency range of 135–175 MHz. VHF paging networks are commercially available from a communication company or can be owned and operated by a utility. Eaton uses the VHF network to deliver DR messages across the network to the receiver using the ExpressCom protocol.
- **900 MHz flex paging.** 900 MHz flex paging occupies the frequency range of 929–932 MHz. 900 MHz flex paging networks are commercially available from multiple nationwide carriers and local carriers. The 900 MHz flex system is an internationally accepted standard and is prevalent across the U.S. Eaton uses the 900 MHz flex network to deliver DR messages across the network to the receiver using the ExpressCom protocol.
- **RDS messaging.** Radio Data Services (RDS) occupies the frequency range of 87.5–108 MHz. RDS networks are commercially available through FM radio broadcast companies and can be locally owned. RDS is an international standard for encoding and sending digital messages on a sideband of the analog FM radio signal.

Eaton has implemented a secure protocol for the one-way communication environment. The Eaton one-way message encryption algorithms use industry standard security methods that are applied in a unique way to address the inherent limitations of a one-way and lossy communication system. The system is deployed with a utility-unique private key and two daughter keys. The private key is used to encrypt all messages. The daughter keys are used to authenticate and decrypt the messages. The daughter keys are loaded into the hardware during manufacturing. The security features include:

- **Encryption.** The content of messages is kept secret through the use of symmetric AES-128 in Cypher Block Chaining (CBC)—Residual Block Termination (RBT) mode.
- **Authentication.** Authentication of the sender is verified using AES CBC-CMAC.
- **Initialization Vector (IV).** The initialization vector for CBC is generated with an MD5 hash of the sequence number.
- **Sequence number.** Each receiving device keeps a record of the highest sequence number message it has ever seen. It will never respond to an incoming message that has a sequence number at or lower than this highest recorded value.

There is a common DR architecture for all of the broadcast communication solutions provided by Eaton as shown in **Figure 6**.

A DR message can be created at a user request (utility or end-consumer) or by a trigger mechanism (e.g., execute load event upon price signal). The processing of a DR message is described below.

- **IT environment.** The DR message is packaged into an ExpressCom message. The ExpressCom message includes the addressing (group or individual) and the command to the device. The ExpressCom message is then encrypted using a 128-bit AES encryption algorithm. It is formatted into a TAP protocol message for transmitting to the network communications system.
- **Backhaul communications.** The DR message is transmitted to the network communications provider using one of several methods. In all methods, a session is started that includes a logon process with password authentication. The session can include the transmittal of multiple messages.
  - **Internet TAP portal.** The message can be sent using the Internet to the network provider that establishes a session with Yukon
  - **Modem communication.** The message can be sent using a dial-up modem connection to the network communication provider
  - **TCP/IP link.** If the network provider is the utility, a session can be started between Yukon and the utility's communication server within the utilities firewalled IT environment

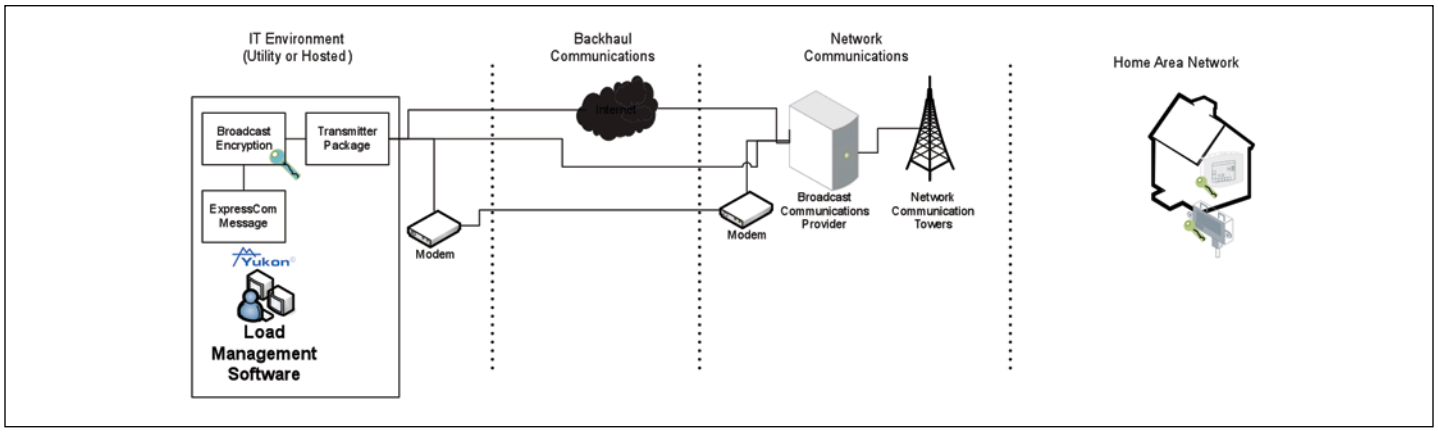

Figure 6. Broadcast DR overview

- **Network communications.** The network communications provider transmits the message to its communication towers. The messages are sent in the TAP encoding over the network communications provider network. This network comprises various communication technologies and is secured using standard network devices. At the communication towers, the message is broadcast using RF technology within the specific bands subscribed by the network communications carrier.
- **Home area network.** The broadcast message is received by all Eaton DR devices within the broadcast range that are programmed to receive messages on the RF frequency. The message is decoded using the daughter keys installed in the device during manufacturing. The ExpressCom processing includes the verification that the message is a valid message. In addition, the device verifies that the message is specific to it by matching several fields in the message against its internal configuration (serial number, group address, utility code, etc.).

Eaton RF mesh DR

Eaton offers a two-way RF mesh communication system for DR applications. The DR end devices can be native RF mesh, ZigBee SEP HAN ①, or a combination of both. The Eaton RF mesh communication system uses a superior performing mesh technology as a basis for the intelligent DR network capable of fast control event broadcasting as well as provides post-event confirmation of individual device event participation. The network is also capable of supporting real-time event reporting. Mesh communications provide high network communications reliability by supporting multiple diverse paths through which bi-directional communications can occur. In the case of DR event activation broadcasting, the Eaton RF mesh employs unique transmission diversity schemes that increase both the reliability as well as the speed with which event activation is signaled across the network. The RF mesh network delivers this highly reliable two-way communications across the unlicensed 900 MHz (902–928 MHz) band where the high available spectrum allows support for high data rate communications. The system employs frequency hopping spread spectrum communications across the available 25 MHz of bandwidth.

① The ZigBee HAN solution requires an AMI meter with the ZigBee HAN gateway.

The Eaton RF mesh network is 100% self-organizing, self-forming, self-healing, and self-optimizing. No configuration of the nodes at the utility or in the field is required. The nodes automatically identify neighbors, form communication relationships, and they independently determine the most efficient path to the gateway. If these primary communication relationships are interrupted, the nodes automatically migrate to alternative routes to the gateway without any single point of failure. DR end devices are able to take advantage of the two-way network connectivity to support autonomous registration as well as provide updated status upon request.

Eaton system security has been designed, developed, and implemented on the basis of maintaining Confidentiality, Integrity and Availability (CIA) of data from devices to the head-end system across the different system exchanges, where:

- Confidentiality involves protecting information against unintended and/or unauthorized access
- Integrity entails protecting system elements and information from unauthorized and improper modification
- Availability entails ensuring that information and system elements are available when required for system functioning

Additional details of the security architecture are provided in the Eaton AMI Network Security Brief document:

- Eaton Smart Grid AMI Network Security Brief Version 4.0, February 24, 2015
- Eaton RF Mesh DR with Native Radios

Figure 7 shows the communication system for a DR system with native RF mesh radios.

A DR message can be created at a user request (utility or end-consumer) or by a trigger mechanism (e.g., execute load event upon price signal). The processing of a DR message is described below.

- **IT environment.** The DR message is packaged into an ExpressCom message. The ExpressCom message includes the addressing (group or individual) and the command to the device. The ExpressCom message is passed to the RF Mesh Network Manager. This process can be located on the same physical machine as the Load Management Software or on a separate machine in a separate environment. All communications between the Load Management Software and the Network Manager occur over an IP-based Transport Layer Security (TLS)/Secure Socket Layer (SSL) channel. The confidentiality and integrity of the data exchanges that is supported by the TLS/SSL tunnels between the Load Management Software and the Network Manager can be further augmented by software WAN VPN to enhance security.

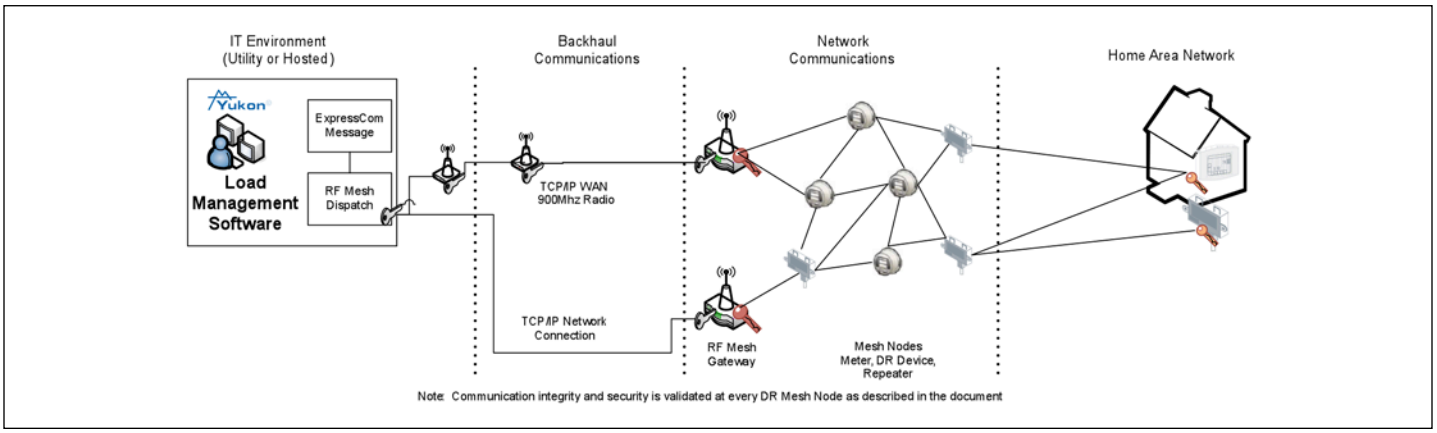

Figure 7. RF mesh with native DR node communication

- **Backhaul communications.** Eaton supports a wide variety of media between the IT environment and the Eaton RF network gateway, and most systems use a combination of communication media as communication paths. In most cases, utilities have physical assets (office buildings, distribution substations, maintenance facilities, etc.) that are connected to the Utility WAN and available as connection points. Eaton also provides a TCP/IP WAN 900 MHz radio system that can be used as the WAN backhaul communication. The network manager path to the RF Network Gateway uses 256-bit AES cryptographic algorithms for traffic encryption along with 1024/2048-bit RSA public key-based authentication and key exchange, and with Secure Hash Algorithm (SHA) for integrity. This security is applied through industry standard X.509 certificates configured at the gateways and the Eaton Yukon network manager. The confidentiality and integrity of the data exchanges that is supported by the TLS/SSL tunnels between the gateways and the Eaton Yukon network manager can be further augmented by software WAN VPN to enhance network availability security.
- **Network communications.** All wireless communications in the Eaton RF Network mesh network are protected by mutual device authentication and a derived, per-session encryption key to ensure hardened encryption. The mechanism used is a server-less peer-to-peer key derivation scheme using a challenge-response exchange between nodes that guarantees freshness without reliance on timestamps. Every pair of nodes mutually authenticates each other during the link establishment challenge response exchange and each node contributes unique key material to derive the session key. This unique session key is then used for encrypting all data traffic (including routing or other system management data) communicated during the particular link session. The derived session key is used to perform AES-128 based data encryption. Careful attention has been paid to the generation of nonces (using NIST-Recommended Random Number Generator Based on ANSI X9.31) used in the challenges and for the random numbers used for key derivation to ensure robust cryptographic implementation. All Eaton RF system AES security implementations meet the NIST (National Institute of Standards and Technology) recommendations governing key length for ensuring algorithm security in the post 2014 timeframe (see NIST SP800-131, February 2011). The secure node-to-node communications exchange is repeated on every link as data passes from the meter Node to the serving network gateway. This pattern ensures that the mesh network and its connectivity across all hops to the gateway are fully secured. The security procedures applied at each wireless hop thus ensures authentication, confidentiality, and data checking integrity protection for all network devices—Eaton RF Network DR Devices, Meter Nodes, Relays, Wireless Network Field Tool, and Wireless Gateways. Additionally, for all Node firmware upgrades including firmware for upgrade of connected DR end devices, the application of digital signatures using public key-based 2048-bit RSA security algorithm with Secure Hash Algorithm (SHA-256) guarantees the integrity and authenticity of accepted firmware code.
- **Broadcast communications.** In addition to the above security mechanisms at the head-end system and across the WAN, where RF system broadcast is applied for Demand Response (DR) event notifications or other group-based communications, message security, including AES-based confidentiality and data integrity is always applied. In conjunction with data confidentiality and integrity protections, delay and replay protection are also supported to ensure that repeated messages received after a defined validity are directly discarded. The AES-based encryption protection is implemented using broadcast-specific security keys. Furthermore, to limit the potential for denial of service (DOS) attacks through the unauthorized initiation of network broadcasts within the RF network, no unsecured broadcast messages are ever supported within the system. An RF node is therefore always able to immediately discard without the need for further processing and never re-broadcasts any message that fails integrity verification.
- **Home area network.** A DR broadcast message is received by all Eaton DR devices on the network. A targeted message is sent to a single device. In either case, the ExpressCom processing on the device includes the verification that the message is a valid message. In addition, the device verifies that the message is specific to it by matching several fields in the message against its internal configuration.

DR with Digi® IP to ZigBee SEP gateway

Eaton has partnered with Digi International, Inc. to provide an end-to-end broadband ZigBee SEP solution. The solution uses the Internet and the end-consumers broadband communications as the backhaul and network communication system. At the end-consumer location, the Digi gateway connects to the end-consumer's broadband communication and provides the wireless ZigBee SEP HAN Trust Center that allows the connection of any ZigBee SEP 1.0 or 1.1 device. Additional details on the ZigBee SEP are provided in the "DR with ZigBee Smart Energy Profile (SEP)" section on **page 15**. **Figure 8** shows the end-to-end system configuration for DR solution using the Digi Gateway and iDigi software.

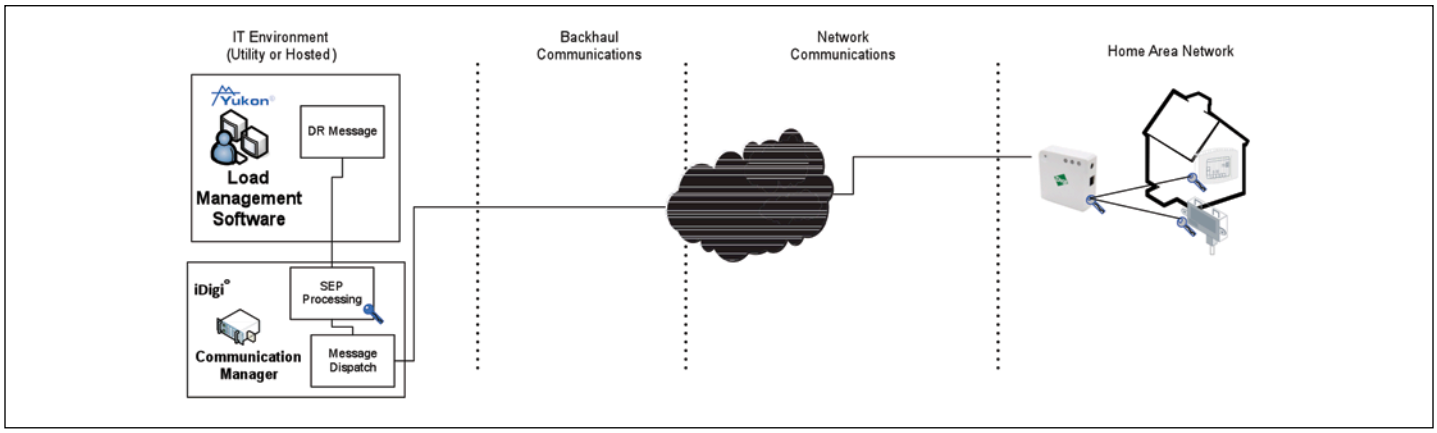

Figure 8. iDigi ZigBee SEP DR communication

A DR message can be created at a user request (utility or end-consumer) or by a trigger mechanism (e.g., execute load event upon price signal). The processing of a DR message is described below.

- **IT environment.** The DR messages are created in the Yukon environment and passed to the iDigi environment.
  - **Yukon environment.** The DR message is processed within the Yukon environment and passed to the iDigi environment via a REST-style API over HTTP or HTTPS. The iDigi cloud service manages the devices for the DR system and is responsible for message delivery between the devices and the Yukon environment.
  - **iDigi environment.** iDigi is a hosted Machine to Machine (M2M) management cloud service software platform that ties together enterprise applications and remote device assets regardless of location or network. iDigi allows easy and secure connectivity and management of remote devices and offers web services protocol for application integration including: end to end, device to application integration; connectivity and management of remote devices; and Digi hosted, no infrastructure required security infrastructure.
    - **IDigi hosting environment.** Digi has forged a partnership with a SAS70 certified network and hosting service provider to host the iDigi platform. SAS70 certifies that a service organization has had an in-depth audit of its controls (including control objectives and control activities), which in the case of our partnership, relates to operational performance and security to safeguard customer data. Host systems reside behind firewalls with additional preventative measures against distributed denial of service (DDoS) and Man-in-the-Middle (MITM) attacks. Further intrusion prevention includes IP-spoofing and packet-sniffing disablement. Monitored host access is limited to authorized Digi personnel who must successfully complete background checks during the hiring process. Host management practices align with ITIL such as a change management process for system and application changes.
    - **Authentication.** Authentication is the process of ascertaining users' and devices' identity, and relies on credentials ranging from username and password to the use of digital certificates and signatures. The iDigi management platform and Web service APIs are available via endpoints protected with SSL using AES 256-bit encryption and require a valid username and password pair for authentication. The management console provides an inactivity timeout for additional security. User passwords are stored using a one-way Message Digest Algorithm (MD5) encryption
- **Backhaul communications.** The iDigi hosting environments provides the connection to the Internet for the transport to the end-user home area network.
- **Network communications.** The solution uses the Internet and the end-consumer broadband connect for the network communications layer.
- **HAN.** The ConnectPort X2e gateway utilizes a proprietary protocol over Secure Socket Layer (SSL) transport to establish an encrypted connect to the iDigi Platform. The device is a compact ZigBee to Ethernet/Wi-Fi gateway that provides a low-cost secure IP network. ConnectPort X2e enables custom applications to run locally while interfacing across existing Ethernet/Wi-Fi networks for WAN connectivity to a centralized server. The ConnectPort X2e uses secure http (https) Web interfaces for all communication to the back office software and to Yukon and provides the backhaul functionality required to successfully manage a two-way DR program. Over the air programmability for firmware upgrades in the ConnectPort X2e and DR devices is also supported. To maintain system integrity, the gateway performs a firmware integrity check and will disable the boot process if this check fails. This process is maintained through each firmware update. iDigi Energy gateways enable secure administration through Secure Shell (SSH) and Secure Socket Layer (SSL) transports. Authentication is provided by a SSH public key authentication or by username and password pair. Configuration options on the gateway allow Access Control Lists, or IP source filtering and disabling of various protocols to provide an additional layer of security.

The Eaton and Digi international solution has been field tested with all Eaton DR SEP hardware at multiple locations. The solution also includes a SEP range extender for applications where the consumer loads are not within range of the gateway. The XBee® PRO ZB is a Smart Energy Profile (SEP) certified wall plug RF range extender that increases distance and signal strength within the ZigBee mesh Home Area Network (HAN).

Figure 9 shows the complete DR solution including an end consumer's access to their home devices using a smart phone application. The solution allows the end consumer remote management of their energy user, programmability of their thermostat, and monitoring of their thermostat settings. The solution can be used to manage AC energy use, pool pumps, water heaters, and other residential and small commercial loads.

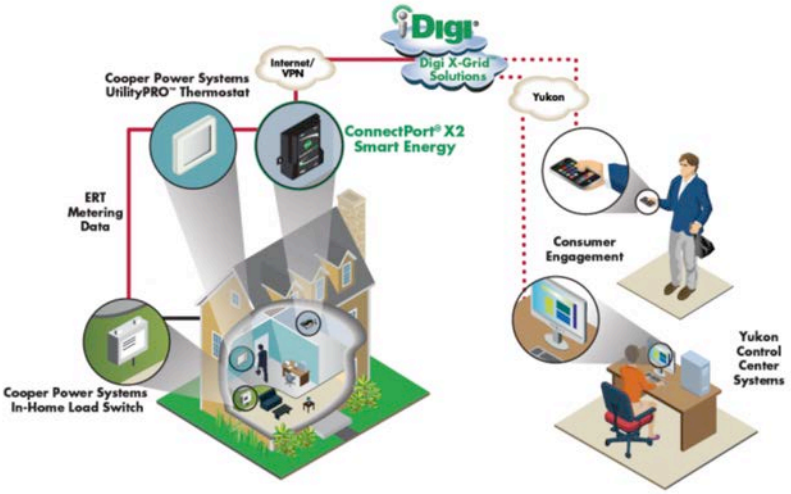

Figure 9. Complete DR solution including an end consumer's access to their home devices using a smart phone application

DR with ZigBee Smart Energy Profile (SEP)

Eaton is an active participant in the ZigBee SEP 1.x and SEP 2.0 working groups. Our devices are SEP 1.0 and 1.1 certified. Eaton is developing SEP 2.0 devices in conjunction with the completion of the technical and testing requirements process. This section summarizes the secure computing environment of the SEP. Additional details on ZigBee radios and SEP are published in open forums. The SEP 1.0 and 1.1 are part of the NIST accepted standards.

The SEP specification covers the original encoding/decoding of messages in the IT environment and the decoding/encoding of the messages at the field equipment locations. The backhaul and network communication environment to transport the messages from the IT environment to the field equipment locations are provided by a communication manager (see **Figure 10**).

A DR message can be created at a user request (utility or end-consumer) or by a trigger mechanism (e.g., execute load event upon price signal). The processing of a DR message is described below.

- **IT environment.** The DR message is processed within the Yukon environment and passed to the communication provider. Message dispatch is done using an Enterprise Integration Manager (EIM) API that uses Web Services Description Language (WSDL) files to define the Web Services that are used by the applications to exchange Simple Object Access Protocol (SOAP) messages with each other. All communications between the Yukon load management software and the communication provider occur over an IP-based Transport Layer Security (TLS)/Secure Socket Layer (SSL) channel. The confidentiality and integrity of the data exchanges that is supported by the TLS/SSL tunnels between the Load Management Software and Network Manager can be further augmented by software WAN VPN to enhance security.
- **Backhaul and network communications.** Eaton works with a number of providers that provide the backhaul and network communication system including the Eaton RF mesh network, Digi International, and other AMI vendors. End-to-end communication examples are documented in the "Eaton RF mesh DR" and the "DR with Digi IP to ZigBee SEP Gateway" sections.
- **Transmission security.** SEP utilizes Elliptic Curve Cryptography (ECC) to perform authentication. SEP adheres to the IEEE® 802.15.4 standard and uses the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key. The AES provides encryption to prevent against eavesdropping and ensures data integrity by using a Message Authentication Code (MAC). This code ensures integrity of the MAC header and payload data attached and all messages with an invalid code are discarded. This is accomplished by loading a certificate on each device that is unique to that device. Each certificate binds the EUI of the radio to an ECC key pair, providing the means for the device to uniquely identify itself on the smart energy network.
- **HAN security.** A series of keys are used to permit devices to join a secure and trusted SEP home area network (HAN). All devices share a common network key, and link keys permit two devices to establish communications. One device on the network is called the Trust Center and is responsible for key management for the network. As shown in the figure, this device can be an AMI meter or a gateway. Once an SEP device receives the network key, it will ask to join the network. The Trust Center compares the link key of the device asking to join with a list of trusted link keys. If a trusted key is found, the device is admitted to the network, otherwise the request is denied.
- **Trust Center security.** To maintain system integrity, the Trust Center performs a firmware integrity check and will disable the boot process if this check fails. This process is maintained through each firmware update.

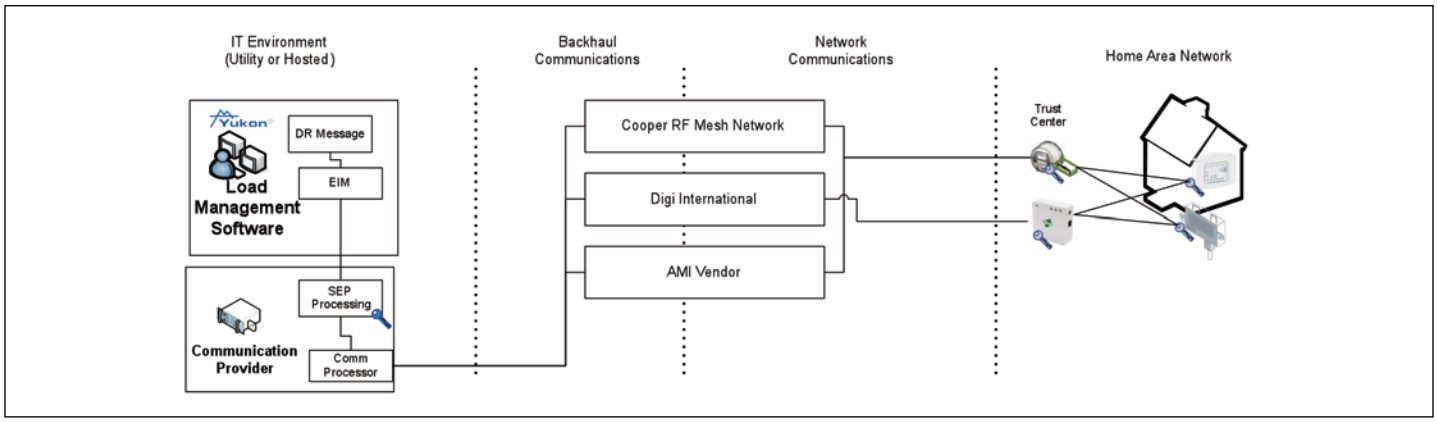

Figure 10. ZigBee SEP DR communication

Change history

Version	Date	Change summary	Person
3	August 2007	Initial release. Originally entitled Technical Bulletin Utility IT integration.	J. Childs
3.6	July 2009	Updated document to address changes in server requirements, and supported browser and database.	D. Sutton
3.7	September 2009	Review of materials update for OS functions.	D. Sutton
3.9	October 2009	Removed external system interface details and created separate technical bulletin for server-to-server interface details.	J. Childs
4.1	April 2010	Rewrote document to incorporate NIST recommended outline and content.	J. Benoit
4.2	May 2010	Update of materials for submission with security plan for ARRA project grant.	J. Childs
4.6	April 2011	Update of materials to include password rules and encryption native to Yukon instead of a password services platform.	D. Sutton
4.7	February 2012	Review and update of document to update supported browser and database.	D. Sutton
4.9	January 2013	Update of materials to remove information that is not specific to the secure computing environment. Added audience and change history.	J. Childs
5.1	February 2013	Review and update of all language. Added new sections on ZigBee and RF communications.	J. Childs
5.2	February 2013	Review of changes with technical review team for accuracy.	J. Childs
5.3	February 2013	Updated the RF mesh section to put ZigBee in standalone section.	J. Childs
5.4	June 2013	Updated ZigBee section. Updated the hosting services section.	J. Childs
5.5	November 2016	Updated hosting services section. Updated system specifications. Updated Yukon security testing.	J. Childs
5.6	June 2016	Revised document to include licensed and hosted deployment. Changed the organization name to Eaton. Formatted the document to the current template.	J. Childs

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Eaton's Power Systems Division
2300 Badger Drive
Waukesha, WI 53188
United States
Eaton.com/cooperpowerseries

Printed in USA
Publication No. WP910002EN / Z19148
February 2017

Powering Business Worldwide