EXECUTIVE SUMMARY

Market Aware High Performance Buildings Participating in Fast Load Response Utility Programs with a Single Open Standard Methodology

ESTCP Project EW-201401

AUGUST 2018

Page Intentionally Left Blank

Page Intentionally Left Blank

EXECUTIVE SUMMARY

Project: EW-201401

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page Intentionally Left Blank

ACRONYMS AND ABBREVIATIONS

AutoDR	Automated Demand Response
BIP	Base Interruptible Program
BMS	Building Management System
CONUS	Continental United States
COTS	Commercial off the Shelf
DAA	Designated Accreditation Authority
DoD	U.S. Department of Defense
DR	Demand Response
EISS®	Energy Interop Server & System
EISSBox	OpenADR 2.0b-compliant end point/ESI
IOU	Investor Owned Utility
IP	Internet Protocol
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OpenADR	Open Automated Demand Response
PJM	PJM Interconnection, LLC – large RTO with operations in the Mid-Atlantic and Midwest states
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
SDG&E	San Diego Gas and Electric
SSL	Secure Socket Layer
TLS	Transport Layer Security
VEN	Virtual End Node
VTN	Virtual Top Node
XML	Extensible Markup Language

Page Intentionally Left Blank

1.0 INTRODUCTION

Building performance improvement is not just about consuming less energy it is also about managing when this energy is consumed. Historically, federal mandates have been about reducing the energy consumption per square foot and integrating renewable generation. Significant improvements in efficiency have been accomplished. However, the current budgetary climate will require further reductions in operational energy spending and this will be difficult to accomplish purely with further attempts at efficiency gains.

The next area of gains will not be in efficiency but in participation in demand management programs that reward changes in the timing of energy use and participation in rapid response energy markets, such as regulation and spinning reserves. This discussion about the timing of energy consumption is made more relevant by the increased use of renewable energy. Renewables like wind and solar are by their very nature intermittent whereas the consumption of energy does not follow this same pattern. What to do with this excess generation when not needed and how to fill the gaps when it is not present is a significant challenge. Electrical storage technologies are one potential area to mitigate this issue but currently are cost prohibitive and will require more time and research in order to make them cost effective.

To deal with this issue, the federal government and the Department of Energy have undertaken many studies to see if end use consumption can be quickly changed to match the intermittency provided by these renewables. Programs like real time retail pricing, migration to wholesale markets; peak demand charges, solar cutoff programs, etc. have shown that it is possible to balance the grid by signaling load. Participation in these programs typically results in financial incentives and lower utility bills. Grid stability and economic incentives will be the driver for the new "market aware" high performance building.

Unlike legacy demand response programs, which would only be called a few times a year, these new demand management programs may require daily and/or hourly changes to consumption. Manual curtailment will not be able to meet utility program response requirements and provide the reliability needed to maintain grid stability. What is needed is a machine-based direct connection between energy providers and consumers.

Legacy methods to accomplish these machine-to-machine interactions are both proprietary, expensive and lack cyber security controls. In the absence of federal standards for energy communications, each company developed their own proprietary solutions. Recent Smart Grid standards sponsored by the National Institute of Standards and Technology (NIST) and managed by the Organization for the Advancement of Structured Information Standards (OASIS) have created a single open standard solution for energy communications called Open Automated Demand Response version 2.0 (OpenADR 2.0.) These standards use the latest Secure Service Orientated Architecture based web services to allow non-propriety, secure communications of energy market information. For example, the OpenADR 2.0 standard includes the following:

a. Secure Socket Layer (SSL)/Transport Layer Security (TLS)-supported encryption – using either Rivest-Shamir-Adleman (RSA) or Elliptical Curved Cypher sets
b. TLS 1.2 – the latest version of Transport Layer Security for secure end-to-end transmission of data between server and end points

c. X.509 Public Key Infrastructure (PKI) certificates for mutual authentication on both the server and end points. The standard requires that an end point may connect to one, and only one server for its OpenADR 2.0b signals. Mutual authentication insures that an end point may connect only to a server that has its PKI certificate on file.

This new standard has been adopted for use by the Investor Owned Utilities (IOU) in California and Hawaii and is being used in pilots in Texas and the U.S. east coast. This standard provides a single secure bi-directional method for energy providers to signal energy consumers' equipment directly while still providing user choice.

2.0 OBJECTIVES

Demonstrate the feasibility of using OpenADR 2.0 – an open standard web services-based system to allow machine-to-machine communication between U.S. Department of Defense (DoD) facilities and energy providers – to enable secure participation in the new grid balancing/demand management programs.

A baseline comparison of the OpenADR 2.0 compared to legacy Demand Response (DR) systems and to no DR.

Energy Interop Server & System (EISS®) and OpenADR 2.0 help DoD drive greater grid stability by participation in a number of new demand response and energy market programs – some of which require automation as a condition of participation. The technology also has the potential of helping DoD to monetize its microgrid investments by signaling when energy prices make it more cost efficient to sell power to the grid and when it is better to use a microgrid to supplement the needs of the DoD installation. Key measurements associated with the demonstration include:reduced vulnerability to power grid disruptions, signal optimal times to increase use of renewable energy generation, and reducing energy intensity (kWh/ft^2).

Page Intentionally Left Blank

3.0 TECHNOLOGY DESCRIPTION

Description: Our solution consists of two parts: a cloud-based server to distribute market signals from an energy provider according to a standard format and client-side end points to convey market signals to facility energy management systems and/or DR assets. Optionally, a stateful firewall of type and capability required by the Designated Accreditation Authority may be included as well, although this component was not used in the project. The server and end points are connected via web services over an Internet Protocol (IP) network connection. The end points allow existing energy management systems to interface with these open standard web services rather than requiring expensive building upgrades. All system components are commercial-off-the-shelf (COTS).

- Visual Depiction: See Figure 1, below, depicting the building blocks of a typical IPKeys Energy Interop Server & System (EISS®) deployment.

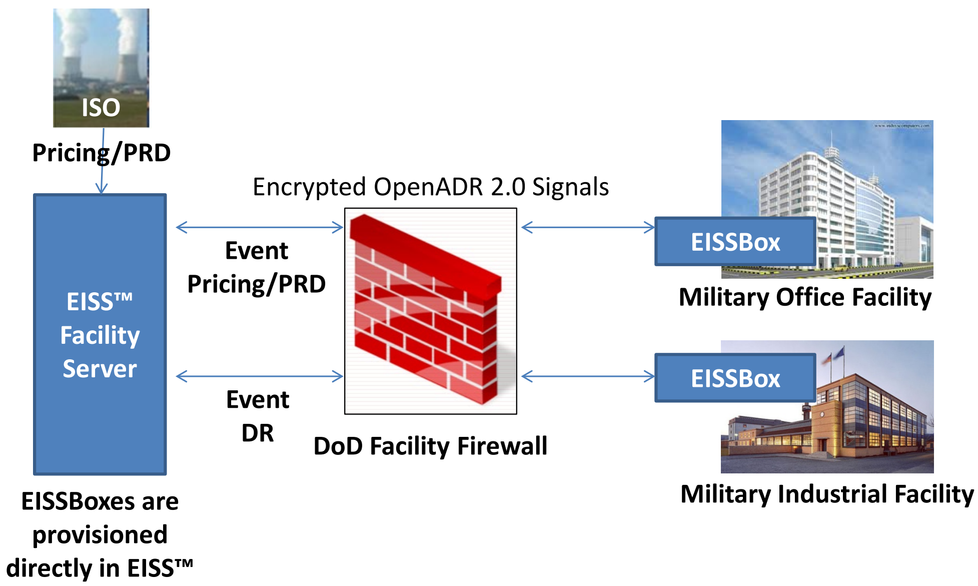

Figure 1. EISS® Server Facility Edition – Typical Deployment

- Components of the System:

  – EISS® 2.0 Server or OpenADR 2.0b Virtual Top Node (VTN) – the EISS® server is a cloud hosted VTN that is the heart of any OpenADR 2.0 deployment. The EISS® server is deployed in two components: the OpenADR 2.0b-certified EISS® 2.0 VTN and EISSPoint – an end point element manager. EISSPoint is used to configure and maintain all EISSBox devices logically attached to it via the Internet. The EISS® server is also a temporary repository for event and meter data collected from fielded EISSBoxes via OpenADR 2.0b's EiEvent and EiReport web services. (The EiEvent and EiReport web services are used to collect responses to calls to perform issued by the VTN server and load shed (kW and kWh) from any attached electric meter or sub-meter.) The EISS® server may be configured to send collected event and meter data to a backup location of the government's choice.

– EISSBox 2.0 or OpenADR 2.0b Virtual End Node (VEN) – the EISSBox is an energy services interface that receives OpenADR 2.0 messages from a VTN and converts those messages into signals actionable by the DR assets under review. IPKeys' EISSBoxes present OpenADR 2.0 signals as either "dry contact" values or Modbus registers.

– Stateful Firewall – if required by the Designated Accreditation Authority (DAA), IPKeys can supply "firewall" technology to perform inspection of all signals sent to endpoints on a DoD installation to ensure the security and integrity of the communication. This safeguard, usually implemented with additional hardware, provides an additional layer of security in that it inspects the XML payload of each packet sent to the end point for conformance to the OpenADR 2.0b XML specification.

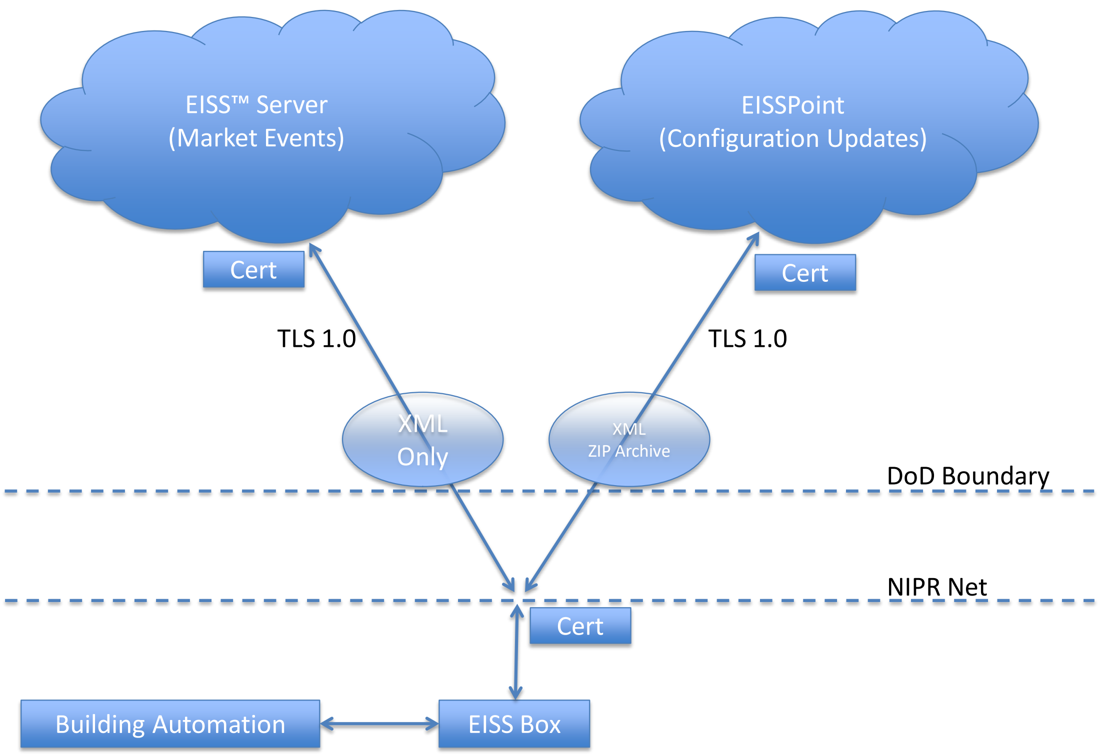

Figure 2. EISS® Component Interaction Diagram

Figure 3 depicts the various components and web services available on IPKeys' EISS® VTN or server. Also shown is the flow of data between components.

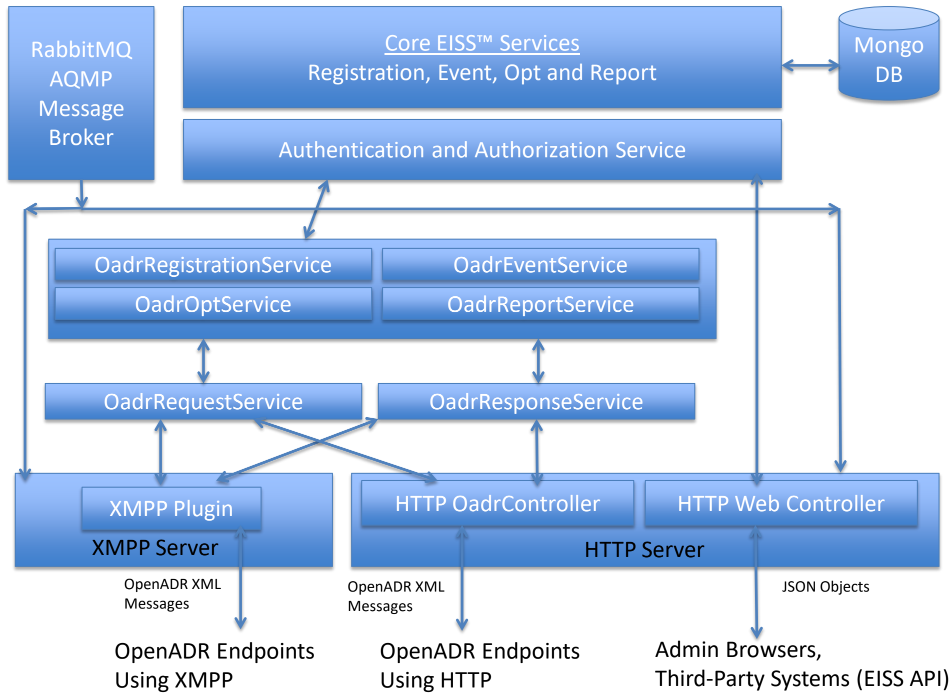

Figure 3. EISS® Server Services

Figure 4 depicts the various components and web services available on IPKeys' EISSBox 3.0 VEN or similar end point hardware. Also shown is the flow of data between components.

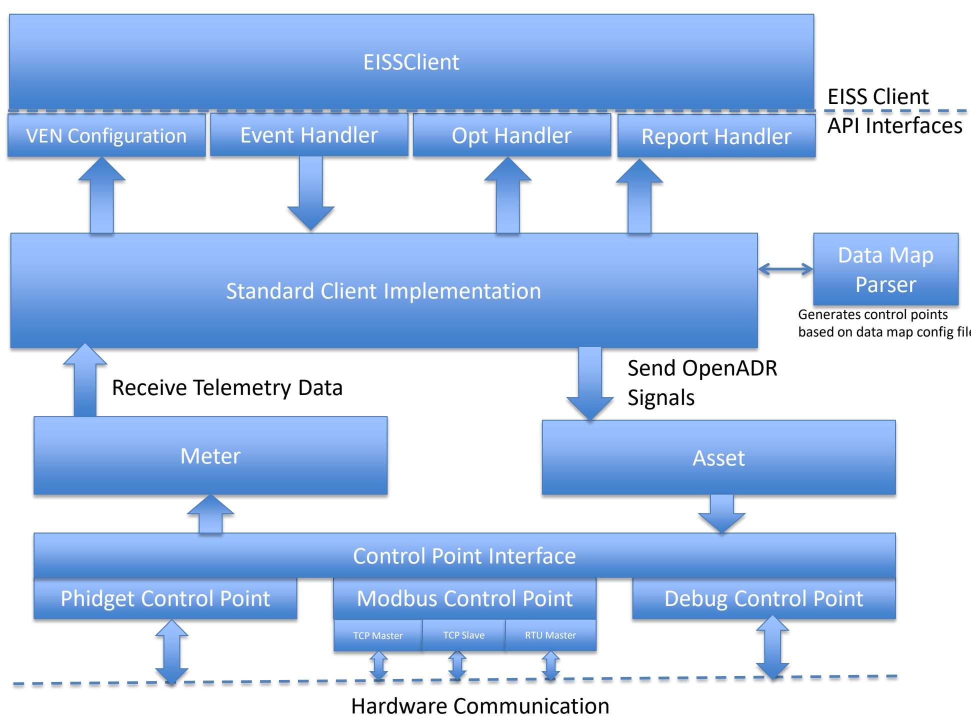

Figure 4. EISSBox Client Services

Page Intentionally Left Blank

4.0 PERFORMANCE ASSESSMENT

The meter data was reviewed and fed into the model, no other performance assessment was performed. A conservative rule of thumb is 10% of the peak load. We have seen facilities who can even go to 40% but that is unusual. Typically, sites can shed at least 10% with a stretch goal of 20%.

To estimate earnings, take 10% of the peak load and multiply it by $6.54/kW to get annual earnings. The $6.54 factor is a blended number based on the Continental United States (CONUS) capacity programs at PJM and SDG&E's Base Interruptible Program (BIP) program that are on the lower end of the spectrum. This number, with the conservative 10% assumption, gives a safe assumption of what can be earned. A useful report prepared in 2012 by staff at Lawrence Berkeley National Laboratory provides a CONUS-level, view.

We can apply this approach to data from the utility meter used to capture the interval data used to invoice Camp Pendleton, shown in Figure 5.

Monthly Usage	Max	Min	Average
Jan-16	2890.5	1551.0	2150.3
Feb-16	3105.0	1494.0	2162.3
Mar-16	2710.5	447.0	2057.3
Apr-16	2767.5	1492.5	1977.1
May-16	2479.5	1447.5	1956.1
Jun-16	3400.5	1540.5	2177.1
Jul-16	3402.0	1720.5	2356.9
Aug-16	3315.0	1834.5	2432.8
Sep-16	3633.0	1755.0	2314.7
Oct-16	3064.5	1630.5	2137.1
Nov-16	3523.5	1584.0	2046.5
Dec-16	2629.5	1434.0	2019.0

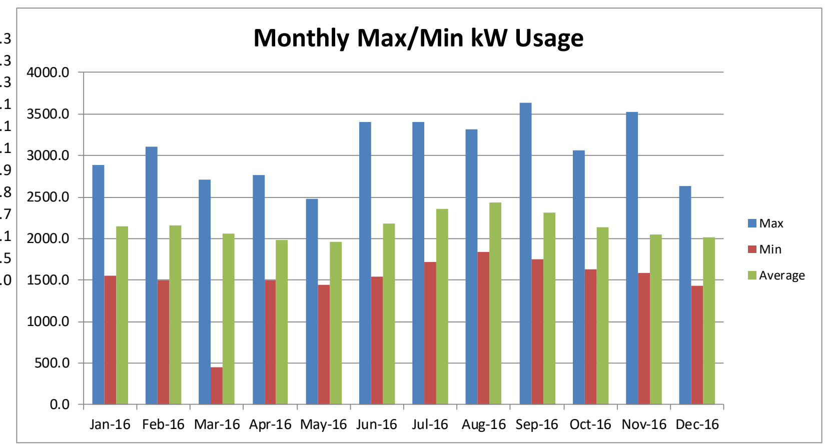

Figure 5. Camp Pendleton Max/Min/Average Usage for 2016

Page Intentionally Left Blank

5.0 COST ASSESSMENT

Table 1. Cost Model for OpenADR 2.0-enabled DR Program Participation

Cost Element	Data Tracked During the Demonstration	Estimated Costs	Comments
Hardware capital costs	OpenADR 2.0b-certified VEN or endpoint (EISSBox)	$2500	
Installation costs	Install gateway	$1200	Gateway installation is $1200 Building Management Program (BMS) programming can range from $5,000 to $20,000 based on our experience in other deployments. The price dependence is based on the presence of predefined scenarios that are present in some BMS systems which make the process of programming of demand response event actions easier.
Consumables	No consumables anticipated		
Facility operational costs	No operational costs anticipated		
Maintenance (Annual)	Cost of maintenance for endpoint. Security logs checked monthly. (This was to be provided as part of the aggregator package during FOC.)	$2430	Endpoint maintenance estimated at 18% of retail cost per year. Included in aggregation package, assume use of a security engineer for one hour per month to review security logs at an estimated rate of $165 per hour.
Hardware lifetime	10 Years +		
Operator training	None		

Automated Demand Response (AutoDR) costs are all up front. Ongoing costs are only incurred if the building management system is changed or updated. These costs are typically nominal.

Page Intentionally Left Blank

6.0 IMPLEMENTATION ISSUES

We have learned during this demonstration that the most critical step is the cyber accreditation. The emergence of energy IoT devices that can save the DoD labor and potentially earn revenue is an emerging topic.

New instructions from the OSD CIO to cover these types of devices were introduced during this demonstration. Since most of these IoT devices require network access, they present a potential vulnerability and the assessment of risk can vary. We saw that a simple change in personnel at Picatinny Arsenal resulted in a decision to withdraw due to the potential risk / reward analysis that every facility ISSM must perform.

To successfully navigate this evolving landscape, we believe these three items are required:

1) Endorsement from command that has the capability to accept risk for the facility. Facility maintenance personnel are typically the first point of adoption but are not able to make these facility-level command decisions

2) Buy in from the facility ISSM before starting.
   Without the continual support of this team this process starts and stops constantly. A POAM and specific personnel must be assigned at the start of the project

3) A complete understanding of the difference between the DoD and the commercial world. We must always keep in mind that the mission of the DoD is to protect this country, not save energy. Anything that could impact their Title 10 responsibilities will be resisted. Our requirements for North American hardware and a Windows operating system show that the closer you can be to a known good deployed system, the easier it is for DoD managers to accept. Anything that can be a gateway for bad actors will be carefully analyzed.