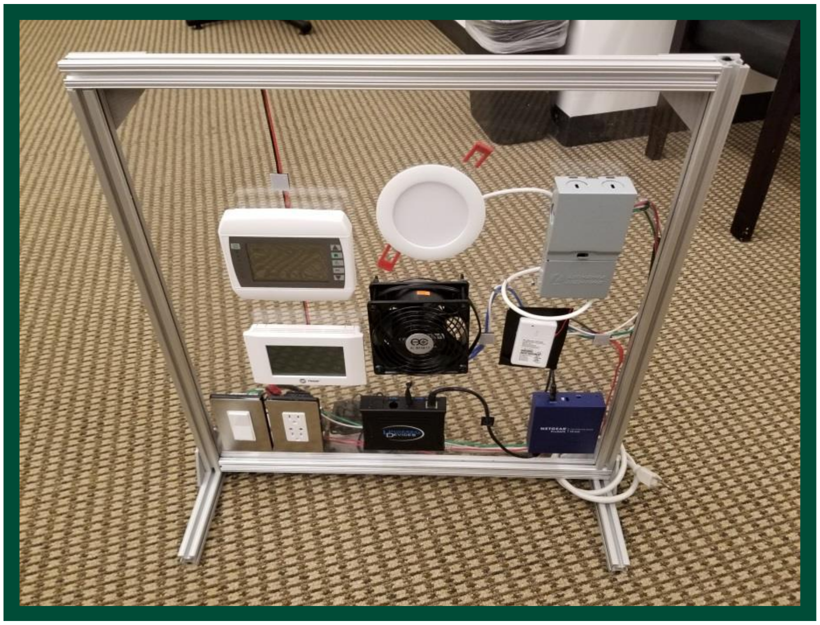
Emerging Products & Technologies

SCE OpenADR Test Lab Development: Phase 1

DR17.01



Prepared by:

Emerging Products & Technologies
Customer Service
Southern California Edison

[August 2019]

SOUTHERN CALIFORNIA
EDISON®
An EDISON INTERNATIONAL® Company

Acknowledgements

Southern California Edison's (SCE) Emerging Products & Technologies group is responsible for this project. It was developed as part of SCE's Emerging Markets & Technologies Program under internal project number DR17.01. ASWB Engineering conducted this technology evaluation with overall guidance and management from Sean Gouw and David Rivers. For more information on this project, contact sean.gouw@sce.com.

This report was prepared by SCE and funded by California utility customers under the auspices of the California Public Utilities Commission. Reproduction or distribution of the whole or any part of the contents of this document without the express written permission of SCE is prohibited. This work was performed with reasonable care and in accordance with professional standards. However, neither SCE nor any entity performing the work pursuant to SCE's authority make any warranty or representation, expressed or implied, with regard to this report, the merchantability or fitness for a particular purpose of the results of the work, or any analyses or conclusions contained in this report. The results reflected in the work are generally representative of operating conditions; however, the results in any other situation may vary depending upon particular operating conditions.

ABBREVIATIONS AND ACRONYMS

ADR	Automated Demand Response
AES	Advanced Encryption Standard
API	Application program interface
ARCNET	Attached Resource Computer NETwork
ASHRAE	The American Society of Heating, Refrigerating and Air-Conditioning Engineers
BACnet	Building Automation and Control Networking Protocol
DDC	Direct Digital Control
DR	Demand Response
DRAS	Demand Response Automation Server
HVAC	Heating, Ventilation, and Air Conditioning
IC	Integrated Circuit
IEEE	The Institute of Electrical and Electronics Engineers
IFTTT	If This Then That
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output
MS/TP	Master – Slave / Token Passing (BACnet)
OSGP	Open Smart Grid Protocol
PC	Personal Computer
SCE	Southern California Edison
SEP	Smart Energy Profile
TCP	Transmission Control Protocol
UDI	Universal Devices, Inc.
VEN	Virtual End Node
VTN	Virtual Top Node

CONTENTS

FIGURES

TABLES

OVERVIEW

Demand Response (DR) controls requirements have been a part of California energy code since the 2008 Building Energy Efficiency Standards, Title 24, Part 6 became effective in January 1, 2010. However, there remains a gap in knowledge and participation, which SCE wants to address. SCE seeks to better engage with its customers, building industry technicians and contractors, end-use equipment manufacturers, and DR technology developers by establishing a DR technology test environment.

A multi-use technology test lab for emerging Auto-DR (ADR) products is sought at the SCE Technology Test Centers in Irwindale, California. A suite of test rigs is needed to facilitate the hands-on development of ADR products that enable to customers and facilities to participate in DR programs. The ADR Test Lab would be designed for maximum flexibility, allowing continuous rotation of products that enable varying configurations of different ADR strategies and devices. It would have multiple Virtual End Nodes (VENs) with capability to accommodate multiple test scenarios. The lab would be a space where technologies could come together to explore their interactive potential, and would be a proving ground for new technologies, where untested products could demonstrate their capability and market readiness.

The inherent challenges of designing a flexible, modular test space drove an approach that leverages multiple phases to incrementally work toward the overall ADR Test Lab vision. This report documents the findings of Phase I of the approach, which consists of preliminary research and a proof-of-concept test rig build. The findings will be leveraged to inform the additional necessary steps.

Phase I Objective: To conduct research on Z-Wave, Wi-Fi, and BACnet communication protocols and load management capabilities to explore the viability of creating a universal lab to test DR load reduction strategies.

Phase I yielded these considerations for Z-Wave-enabled, Wi-Fi-enabled, and BACnet DR-controlled devices:

- The Z-Wave protocol has historically been a proven cost-effective solution for implementing OpenADR2.0a/b DR signals. Due to the proven record of Z-Wave load control devices, it was chosen to establish the test lab baseline, and as the first proof-of-concept build.

- The Wi-Fi protocol replaces only the physical Ethernet cable, which still leaves device-to-device communications unique and specific to their programming. Due to the end-use application being dependent on proprietary programming, a Wi-Fi test lab was determined not to be a current viable universal solution for testing load reduction controls.

- The BACnet protocol shares the application layer and network layer, and is connected by a common Local Area Network (LAN). BACnet devices communicate with each other if they share the same open network protocols; however, if proprietary, they require manufacturer approval to communicate. It was determined to be viable to create a test lab for the BACnet devices using the open network protocol.

The following sections provide the details behind the Phase I research.

Z-Wave Controlled Load Management Devices OpenADR Test Lab

I. Introduction to Z-Wave Protocol

a. Definition

Z-Wave protocol is a wireless self-healing mesh network that connects the Z-Wave gateway to Z-Wave-compatible devices. With any Z-Wave application program, users have full remote control of these technologies. Table 1 provides a general overview of Z-Wave protocol characteristics.

Table 1. Z-Wave Overview

Frequency	868.42 MHz (Europe), 908.42 MHz (America)
Range	30 to 100 meters if unobstructed between two nodes with 4 hops max
Max # of Connected Nodes	232 devices
Communication Limitations	Slower data transfer speeds because of operating at a lower frequency, but Z-Wave devices usually do not send large amounts of data.

b. Types of Z-Wave Network

Z-Wave protocols can be divided into two types, as identified in Table 2.

Table 2. Types of Z-Wave Protocols

Z-Wave	The original open source protocol that shares the same commands and properties of libraries to allow interoperability between different controllers.
Z-Wave Plus	Based off the original protocol but with improved features such as extended battery life, extended range, increased bandwidth, etc.

Application, Advantages, and Disadvantages

Z-Wave has a few applications for load reduction in equipment. Z-Wave, as of now, is not typically integrated with larger commercial equipment like chillers, pumps, or machine processes. In general, Z-Wave is commonly found in smaller consumer products such as thermostats, lights, and plug loads. These end-use devices are scalable, and the thermostats are a workaround for controlling the Heating, Ventilation, and Air Conditioning (HVAC) equipment.

The Z-Wave protocol is proven to work with DR. For the proof of concept, Universal Devices, Inc. (UDI) will increase the current setpoint of thermostats by a predefined amount. Lights will receive a command to dim their levels by any preset percentage. For plug loads, they are only programmed to cut power to the load, so caution must be taken when choosing the device to curtail. Simple plug loads that operate like an on/off switch are more practical than complex plug loads with microcontrollers that can be damaged from power being cut abruptly. Other load control devices that have not been personally tested yet, but are potential candidates, would be refrigerators, water heaters, and battery chargers.

The advantage of Z-Wave is that the protocol is designed to be simple and easy to integrate. There is usually one primary controller, which communicates with multiple secondary controllers through a mesh network. It is a very simple process to add and remove devices from the network with a one-click button. The protocol is also designed to consume much less power and to operate at a lower frequency compared to Wi-Fi.

The disadvantage of Z-Wave is that it requires knowledge of how to use the system. A new user could have difficulties picking up a Z-Wave device and adding it to the network if they did not have prior experience. Replacing a Z-Wave unit would be costlier, because of the technology included in the devices. Due to the radio frequency operating range, the data transfer rate is limited to the frequency's physical abilities. The opportunities and barriers of Z-Wave are further explained in Table 3.

TABLE 3. OPPORTUNITIES AND BARRIERS OF Z-WAVE

Opportunities	Barriers
Simplicity - setting up the network is very simple and easy.	Requires knowledge of the system.
Centrality - there is one primary controller, but multiple secondary controllers.	Replacement costs are higher for Z-Wave appliances.
Scalability - easy to scale and add/remove network devices.	Z-Wave operates on radio frequency and could potentially be attacked by unauthorized users.
Z-Wave protocol inherently consumes less power than other wireless protocols.	Range is limited, so to cover more area, repeaters are needed, eventually driving up the cost.
Z-Wave has interoperability with other wireless devices.	Limited to 232 connected nodes.
Uses the Advanced Encryption Standard, AES-128 for protection.	Slower data communication speed than Zigbee.

C. FEASIBILITY

Z-Wave was originally designed with the intention of creating an open-source protocol by standardizing the libraries and commands that program devices. For example, Z-Wave thermostats created by different manufacturers can use the same commands, such as reporting setpoint temperatures or changing from cooling to heating mode. A dedicated website (openzwave.com) distributes and shares their library on the internet, so anyone can integrate Z-Wave into their devices or products. Z-Wave devices are basically plug-and-play, so the user just needs to press one button to add the device to the Z-Wave network.

Z-Wave devices are proven to work with DR load reduction commands. There should be no issue creating a Z-Wave test lab, so we decided to create a "proof of concept," since the equipment is readily available.

II. Network Infrastructure for Auto-DR

Z-Wave is a wireless communication protocol used primarily in smart networks, allowing smart devices to connect and exchange commands and data. A typical Z-Wave network is similar to Internet of Things (IoT) devices in that it requires a primary controller, also known as a smart hub. The utility's Demand Response Automation Server (DRAS) will send a DR signal from the Virtual Top Node (VTN) to the customer's Virtual End Node (VEN). This signal then routes the command to its destination device to initiate DR[1]. It is a simple process to connect and disconnect Z-Wave devices, because the protocol is designed for the controller to broadcast a signal to the target device when a new device is added.

A typical Z-Wave-enabled ADR infrastructure consists of the DRAS located at the utility servers, a VTN to broadcast the signal, a VEN located at the participating customer site, and smart end-use devices (thermostats, lights, plug loads) that perform the load shed operation. The complete setup and communication hierarchy is displayed in Figure 1. The utility's network DRAS broadcasts a DR signal to a customer VEN, or a group of customer VENs. For some controllers, DR is programmed to apply the same load reduction measures to all connected devices. Depending on how complex the chosen Z-Wave software is, Z-Wave devices may be individually programmable. Currently, the most common DR measures are temperature setpoint adjustment, light dimming, and load curtailment.

Figure 1 provides an illustration of a typical Z-Wave network topology, as well as devices for the proof-of-concept demonstration. UDI is the virtual end node that connects with different end-use devices like HVAC controllers, lights, and plug loads.

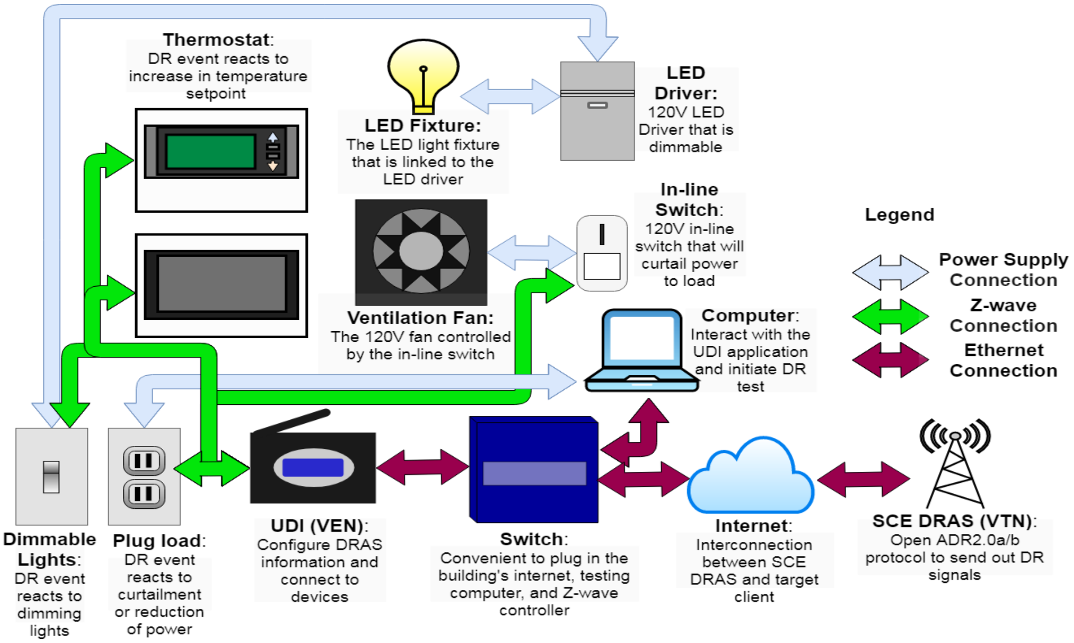

Thermostat: DR event reacts to increase in temperature setpoint
LED Fixture: The LED light fixture that is linked to the LED driver
LED Driver: 120V LED Driver that is dimmable
In-line Switch: 120V in-line switch that will curtail power to load
Legend
Power Supply Connection
Z-wave Connection
Ethernet Connection
Ventilation Fan: The 120V fan controlled by the in-line switch
Computer: Interact with the UDI application and initiate DR test
Dimmable Lights: DR event reacts to dimming lights
Plug load: DR event reacts to curtailment or reduction of power
UDI (VEN): Configure DRAS information and connect to devices
Switch: Convenient to plug in the building's internet, testing computer, and Z-wave controller
Internet: Interconnection between SCE DRAS and target client
SCE DRAS (VTN): Open ADR2.0a/b protocol to send out DR signals

Figure 1. Auto-DR Z-Wave Network Infrastructure.

[1] Definition of Z-Wave - https://internetofthingsagenda.techtarget.com/definition/Z-Wave

III. Procedure to connect Z-Wave devices

Z-Wave devices, like many IoT devices, require a central hub for interface. It is simple to connect and disconnect Z-Wave devices to sync them, because the protocol is designed for a one-click step. In Figure 2, the user only needs to click once to initiate the Z-Wave controller pairing process. During the time it is searching, the user can follow manufacturer instructions to start a similar Z-Wave test device initiating process. For details, please refer to the technical guide in the appendix. UDI was chosen as the Z-Wave controller test lab candidate, as it already has a VEN built in, and has a proven track record of being implemented in commercial ADR applications. Other compatible Z-Wave controllers should have similar (if not the same) device syncing setup procedures.

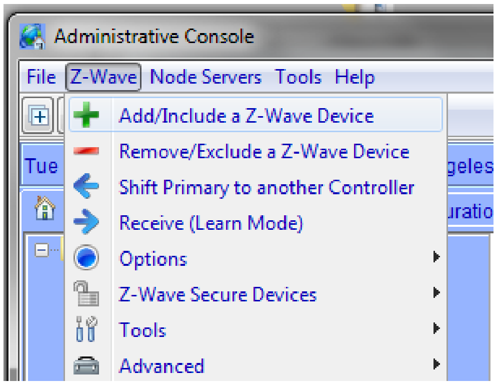


Figure 2. UDI User Interface when Pairing Z-Wave Devices to the Controller

IV. Base Build Cost for the Test Lab

Table 4 provides a breakdown of the cost required to build a Z-Wave board. The estimates are obtained from ASWB’s experience of creating test labs for Z-Wave technology.

Table 4. Cost Breakdown to Build a Test Lab*

UDI Z-Wave with OpenADR certification and Z-Wave module	$381
Router to create virtual Internet Protocol (IP) subnetwork	$37
Ethernet cables x3	$5
Total cost for the Z-Wave test lab equipment	$423

*This does not include the cost of the mounting material, which will depend on the final test lab decision.

V. General User Experience Troubleshooting

a. When setting up OpenADR to interact with UDI-controlled plug loads, the settings must identify an arbitrary end-use device. Without specifying an end-use device, UDI does not know to send the plug load a curtailment command.

b. The UDI user interface has an issue with changing the setpoint and lighting levels on the dashboard. The developer is aware of this issue, but currently has no estimate for resolution. As a workaround, the user may access the settings for the target device and adjust the slider bars.

c. To diagnose Z-Wave device connectivity, in the UDI program, send any command to the device and if it does not respond correctly, the issue may be a glitch. First, try to remove the device from the network by using the "Remove from Z-Wave network" command from the Z-Wave device and the UDI interface. The Z-Wave device may also have a hard-reset button that can be used.

d. To diagnose DRAS-related issues, in the UDI settings, find "Event Viewer" and set the viewing option to "4. All event communications" which will provide a raw output of every action the UDI is processing. Based on the context of information, it will confirm the UDI connection to the utility DRAS, the load reduction request, and the ongoing DR status. The UDI VEN is a separate function from the Z-Wave-connected devices. The VEN will independently contact the DRAS and request DR, so if functionality is confirmed, the problem may be the Z-Wave connected device.

Wi-Fi Controlled Load Management Devices OpenADR Test Lab

I. Introduction to Wi-Fi Protocol

a. Definition

A Wi-Fi network connects to the internet router and wireless-enabled devices using a wireless radio signal. Table 5 highlights the key points of this communication technology[2].

Table 5. Brief Overview of Wi-Fi

Institute of Electrical and Electronics Engineers (IEEE) Standard	IEEE 802.11
Frequency	2.4 GHz, 5 GHz, 60 GHz, varies as Wi-Fi was upgraded with time.
Range	20-70 meters indoor and 100-1000 meters outdoor (based on versions of Wi-Fi, not interference).
Max # of Connected Nodes	50-250 theoretically can go to 250, but realistically 50 for practical usage.
Communication Limitations	Too many wireless devices on the same router will experience high traffic and degraded performance.

b. Types of Wi-Fi Network

Wi-Fi protocols can be divided into multiple types, as identified in Table 6.

Table 6. Types of Wi-Fi Network

a	5 GHz	High frequency reduces effective range. Outdated protocol.
b	2.4 GHz	Many Information Technology (IT) departments are turning off "b" access points. Outdated protocol as well.
g	2.4 GHz	Current universal module for 2.4 GHz only speed. Access points auto-adjust rate to minimize the packet error rate.
n	2.4 GHz & 5 GHz	Must implement Multiple-Input Multiple-Output (MIMO)[3] and 40 MHz bandwidth to get maximum data rates (600 Mb/s).
ac	2.4 GHz & 5 GHz	Implemented MIMO-like protocol n with twice the number of antennae.

[2] https://www.actiontec.com/wifihelp/complete-guide-to-wifi-networking/

[3] MIMO – Multiple Input Multiple Output technique that allows simultaneous data transfer with the 5 GHz and 2.4 GHz antennae.

C. Applications, Advantages and Disadvantages

Wi-Fi networks can be used in many different smart applications to control and monitor end-use operations and, in some cases, implement DR strategies. In a smart building application, there are numerous Wi-Fi-enabled devices, like appliances, home energy managers, home security and controls, building energy managers, hot water heaters, refrigerators, and thermostats. While all have wireless control capabilities, not all are currently designed to initiate DR. Thermostats are the most common Wi-Fi applications to exhibit ADR capabilities.

The advantage of Wi-Fi is the simplicity of connecting devices to the network. It is basically found in every residential or commercial location, making it the most popular wireless network protocol. Wi-Fi upgrades are now exceeding transfer rates faster than ever. Many home appliances and products have integrated Wi-Fi for remote control. Table 7 highlights the opportunities and barriers of Wi-Fi in more detail.

The disadvantage of Wi-Fi is that most manufacturers keep their source code proprietary. With more and more emerging companies creating Wi-Fi load reduction devices, each company has their own applications that must be used to control them. Some manufacturers have permission from different companies to integrate their devices into the same software. In the end, the software is still proprietary. For DR to be integrated into these devices, manufactures must create VENs themselves, and place them into their systems. The other possibility would be to connect external hubs to initiate load reduction commands; however, with most proprietary Wi-Fi devices, it would not be feasible for external hubs to communicate with devices.

Table 7. Opportunities and Barriers of Wi-Fi

Opportunities	Barriers
Convenient – Useful for smartphones, tablet devices, and other portable devices to connect at any convenient location within the premises.	Performance/Speed – Although Gigabit Wi-Fi is available on the market, we cannot get the gigabit speed at all locations; cable networks now have 10 Gbps speed.
Simplicity – To connect a new device with a network, simply turn on the Wi-Fi and apply the basic configuration settings.	Connectivity/Reliability – Wi-Fi signals depend on interference (concrete walls reduce signal strength); also, there is a limited distance to connect Wi-Fi signals.
Mobility – Internet can be accessed from anywhere (bus, train, coffee shop, supermarket, etc.).	Security – Wi-Fi routers have various encryption methods to secure the network password; must be properly configured before using the Wi-Fi network.
Expandability – It is convenient to add more wireless devices with current hardware settings, without cost or time.	Limited Interoperability – Requires additional work to combine different devices to work together.
Efficiency – Wi-Fi-enabled devices are used at offices for convenient file access from any location, resulting in greater productivity.	Proprietary Application Source Code – Most Wi-Fi devices have proprietary application source code and restrict public distribution, making it harder for devices to interact because someone has to bridge the gap.

II. POTENTIAL NETWORK INFRASTRUCTURE FOR AUTO-DR

A typical Wi-Fi-enabled ADR infrastructure consists of the DRAS, located at the utility site, a VEN, located at the participating customer site, and smart end-use devices (thermostats, lights, plug loads) that perform the load shed operation. The complete setup and communication hierarchy is displayed in Figure 3.

The utility network’s DRAS broadcasts a DR signal to a customer VEN (or group of customers VENs). The VEN could be a hub or router that can decipher the DRAS signal and wirelessly communicate with the end-use devices. These devices are equipped with Wi-Fi capabilities and respond to VEN commands based on a built-in, pre-programmable logic sequence. Depending on the DRAS signal, the DR event could be global temperature setpoint adjustment, light dimming, or any other load-shed strategy.

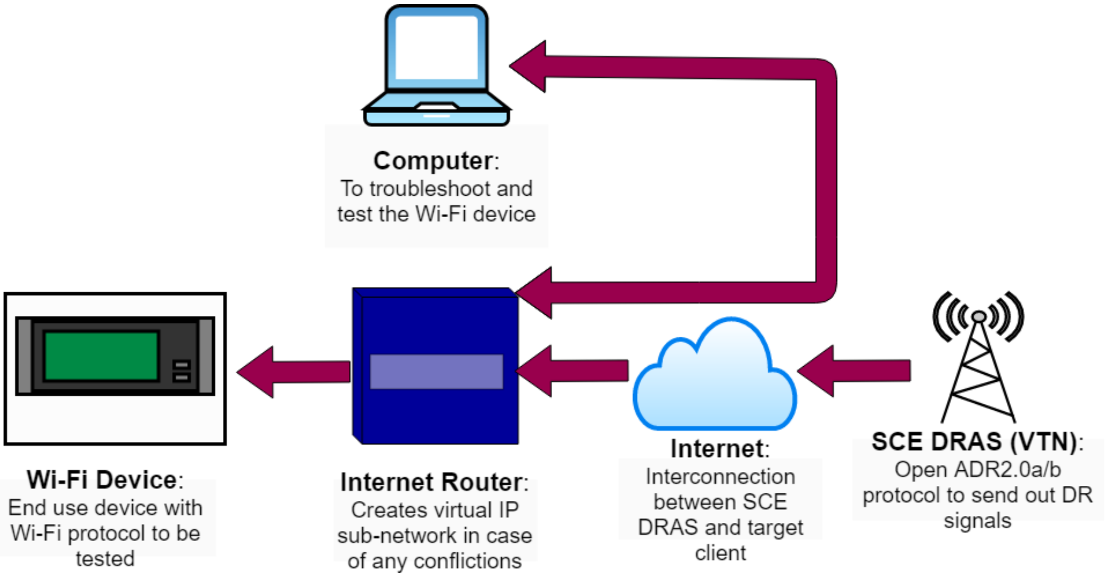

Computer: To troubleshoot and test the Wi-Fi device
Wi-Fi Device: End use device with Wi-Fi protocol to be tested
Internet Router: Creates virtual IP sub-network in case of any conflictions
Internet: Interconnection between SCE DRAS and target client
SCE DRAS (VTN): Open ADR2.0a/b protocol to send out DR signals

FIGURE 3. POTENTIAL AUTO-DR WI-FI NETWORK INFRASTRUCTURE

Any router can be used to connect to Wi-Fi devices and participate in DR; the only missing part is the device’s code that reacts to the utility DRAS. This is the program that either needs to be developed by the manufacturer, or have permission granted to other developers to create.

III. Potential Automated Demand Response Integration Methods

Wi-Fi networks come in both private and open API sources. Networks with private API sources require the developers to code them into their software. Those with public API sources can potentially be controlled. Below are some possible integration methods devised from the research process.

a) SmartThings, Amazon Alexa, Wink, HomeKit, Logitech Harmony, Haiku – Big Ass Fans, Vera Controller, Control4, IRIS by Lowe's[4], Google Home, Securifi Almond, Swann One.

   i) Smart Hubs could potentially be programmed by the manufacturer or developers to incorporate the OpenADR protocol into their products, which would receive DR signals from the utility and initiate load reduction controls.

b) If-This-Then-That (IFTTT) online API by Microsoft.

   i) This is essentially a virtual smart hub that has pre-designed actions enabling proprietary devices to activate based on other device actions. IFTTT bridges the gap in application device layers by getting the permissions from those proprietary companies and linking the actions together. It may be possible to have Microsoft write an API for IFTTT.

c) Smart Energy Profile 2.0 was a research topic that stood out and showed potential for the Wi-Fi protocol to initiate DR. It was a joint partnership between the Wi-Fi Alliance and Zigbee Alliance to develop a device load reduction profile. The Smart Energy Profile (SEP) protocol was designed to be implemented in devices that could potentially run at reduced loads. Since 2010, Wi-Fi Alliance and Zigbee Alliance collaborated to create SEP 2.0, supporting Wi-Fi and Zigbee. SEP 2.0 runs on top of IPv6, servicing Wi-Fi, Home Plug, and other wireless standards. The Open Smart Grid Protocol (OSGP) is an alternative wireless network integration scheme promoted in Europe. Our online research for the Wi-Fi-related SEP work has returned little information, so we've determined progress is still in the early stages.

d) The utility could create an API for Open ADR. It will essentially be a cloud-service VEN when there is no physical VEN on site. The API should be able to send a DR event trigger without the need for a VEN. This approach is ideal for customers with Wi-Fi devices where there is no VTN/VEN support, but where it is open to API interaction.

IV. Research Findings

a. Barriers to Auto-DR Integration

There is no plug-and-play solution, due to most Wi-Fi devices having proprietary software. There is no shared, common set of commands that are universal where an external third-party device can send commands to operate the device. The only way to enable DR on Wi-Fi devices is to program it in the software.

Due to the DR-enabling solution requiring manufacturer support for software integration, there does not seem to be a viable solution for creating a Wi-Fi test lab at this time.

[4] The Iris app and services are permanently discontinued as of March 31, 2019

BACnet Controlled Load Management Devices OpenADR Test Lab

I. Introduction to BACnet Protocol

a. Definition

A BACnet network is a compilation of building control systems integrated into one software application. In concept, typical facilities would upgrade or replace control systems at different times, and would end up using solutions from different companies that had their own proprietary protocols. Eventually, the facilities had multiple applications and software solutions for their building controls systems, which was inconvenient. BACnet was developed to circumvent this problem by establishing standard commands and signals to process raw trending data information. Table 8 highlights BACnet's key points.

Table 8. Brief Overview of BACnet

The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) Standard	ASHRAE Standard 135
Range	Ethernet connections are limited to 100 meters; a twisted pair of wires, 1,200 meters; coaxial cables, 500 meters.
Max # of Connected Nodes	For Ethernet, there is theoretically no limit to the maximum number of nodes on the entire network, with the use of switches and routers. For BACnet Master-Slave Token Passing (MS/TP) the practical limit is 60 for a single network line.
Communication Limitations	Requires engineering to properly commission the BACnet system.

b. Types of BACnet Network

The BACnet protocol can be divided into multiple types, as identified in Table 9.

Table 9. Types of BACnet Network

IP	Uses IP addresses to target devices; similar to Ethernet, but can communicate across different subnetworks using a BACnet Broadcast Management Device. Able to use the building's existing Ethernet network.
Ethernet	Uses a Media Access Control (MAC) address, and is limited to the same subnetwork; most costly, due to router, repeaters, and unused wire in cables; able to use the building's existing Ethernet network.
Attached Resource Computer NETwork (ARCNET)	Requires dedicated IC chips for a separate transmitter and receiver per device; a little less costly than Ethernet, but costs the most compared to the other options; able to use a twisted pair of wires, fiber optics, or coaxial.
MS/TP	Master Slave Transfer Protocol, based on RS-485; three-wire twisted-pair system, daisy-chained together; cheapest solution.
LonTalk	Proprietary protocol from the Echelon Corporation, later released to the public; requires special end-device chips to communicate. Uses a twisted pair of wires like RS-485.

c. Applications, Advantages and Disadvantages

BACnet can tie in crucial building control systems such as HVAC, lighting, security, access controls, and many others. There are BACnet controllers with analog and digital input and output terminals, which can directly manage air conditioning, water heaters, and lights. Other applications include field water pump control devices for irrigation, municipal water services, and waste treatment. BACnet can also be connected to industrial controls systems such as heavy machinery, automated processes, and equipment charging management. Many other applications are available – mostly load control devices that can be configured for Auto-DR. SCE currently has industrial Auto-DR customers who use BACnet systems.

The advantage of BACnet is its ability to merge various building control systems into one software application. It can be configured to provide large amounts of trending data, and with the right engineering, building energy usage can be optimized. BACnet-embedded devices are standardized, allowing manufacturers to share commands and references.

The disadvantage of BACnet is that it requires intensive engineering to correctly configure the entire system. By default, BACnet has vulnerability in that anyone who plugs into the building's Ethernet will be allowed to control the system. Manufacturers have overcome this issue by requiring a login page, but this leads to making the software almost proprietary. Table 10 highlights BACnet's opportunities and barriers in more detail.

TABLE 10. OPPORTUNITIES AND BARRIERS OF BACNET

Opportunities	Barriers
Convenient – Different building controls systems can be integrated into one main application for convenience and increased productivity.	Performance/Speed – BACnet's physical transfer rate is limited for certain data types.
Customized Solution – To properly implement BACnet, engineering is necessary, creating an opportunity to customize and tailor the application for customers.	Security – The BACnet network could potentially be hacked; for the industrial protocol ethernet, an individual with a connection could access the BACnet network.
Open Protocol – BACnet is an open protocol which shares the source code with the public, so BACnet devices should be able to communicate with each other.	Engineering for Interoperability – Requires engineering-level work to combine different devices to communicate with the BACnet network.
Expandability – As an open-source protocol, manufacturers have the ability to incorporate BACnet communications on all their devices, if desired.	Proprietary Source Code – Although BACnet is an open protocol, manufacturers have the ability to create their own proprietary BACnet code, which would typically require a license or fee.
Robust – The BACnet network is designed to be reliable for data transmission and building communication.	

d. FEASIBILITY

Building Automation Systems have grown into many different communication protocols, and some of them are written as proprietary software. Due to the nature of the proprietary software, when a facility wants to regulate two different control systems together, they need an engineer to basically translate between the two protocols. BACnet was initially created as a proprietary protocol, but was released to the public later and became a primary/secondary protocol to be installed in control systems to allow a variety of equipment on the LAN to be remotely interconnected.

BACnet's open-source protocol allows manufacturers of BACnet-embedded products to combine their various control systems into one terminal. However, BACnet allows manufacturers to create their own proprietary code to add to the normal BACnet protocol. To allow access to the proprietary code, manufacturers often charge licensing fees.

The open-source protocol enables computer terminals with the proper software to control any BACnet device. With the right BACnet setup, an Auto-DR test lab can be created to send load reduction commands to BACnet devices. Manufacturers seeking SCE's advice regarding the test lab will be assumed to be cooperative and provide any licenses necessary to test load reduction commands. Therefore, there should be no issue with creating an SCE Auto-DR test lab for BACnet, as it is an open protocol, and manufacturers seeking SCE's advice will be expected to provide access to their proprietary code.

II. NETWORK INFRASTRUCTURE FOR AUTO-DR

A typical BACnet-enabled ADR infrastructure (see Figure 4) consists of the building's existing Ethernet internet, an operator workstation, and the building controller. For BACnet devices connected via Ethernet, there is no need for the BACnet router, because the workstation can communicate with it. For testing the protocols BACnet MS/TP, ARCNET, LonTalk, or Direct Digital Control, a BACnet controller would be ideal to use because of the input/output ports. A BACnet router would suffice if Direct Digital Control equipment testing was not necessary; however, for this lab, the BACnet controller would be recommended.

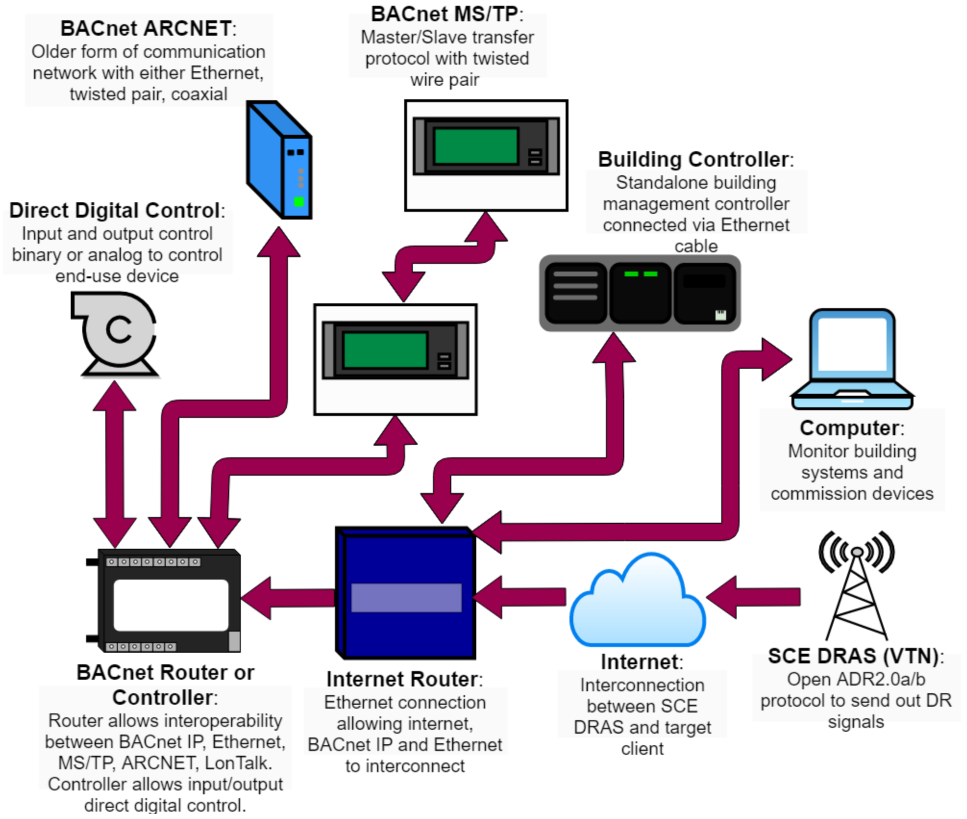

BACnet ARCNET: Older form of communication network with either Ethernet, twisted pair, coaxial
BACnet MS/TP: Master/Slave transfer protocol with twisted wire pair
Building Controller: Standalone building management controller connected via Ethernet cable
Direct Digital Control: Input and output control binary or analog to control end-use device
Computer: Monitor building systems and commission devices
BACnet Router or Controller: Router allows interoperability between BACnet IP, Ethernet, MS/TP, ARCNET, LonTalk. Controller allows input/output direct digital control.
Internet Router: Ethernet connection allowing internet, BACnet IP and Ethernet to interconnect
Internet: Interconnection between SCE DRAS and target client
SCE DRAS (VTN): Open ADR2.0a/b protocol to send out DR signals

FIGURE 4. AUTOMATED DEMAND RESPONSE BACNET NETWORK INFRASTRUCTURE

III. PROCEDURE TO CONNECT BACNET DEVICES

Devices that support BACnet/IP or BACnet/Ethernet can be controlled via a computer terminal connected on the same Ethernet network, making integration easier with existing internet Ethernet networks in the building. BACnet device factory settings either come with a MAC address or a default IP address, which the user can directly access through the computer terminal and change the settings to properly commission the device into the building's BACnet network.

To connect BACnet MS/TP to the building's Ethernet network for continuous monitoring from a computer terminal), a BACnet router will be required to convert the messages from the Ethernet network to the RS-485 network. When maintaining a connection to the building's Ethernet network is not necessary, the BACnet MS/TP device can be commissioned with a portable BACnet router. The naming convention of the MS/TP devices will vary, depending on the network configuration. To commission the MS/TP network, the control network designer will daisy-chain the device wires together and assign the devices a logical naming convention via a computer terminal. There is a limit to the number of devices that can be connected to one MS/TP network, but additional MS/TP networks may be created and added.

ARCNET was initially developed in the 1980s, to automate office tasks. This communication protocol requires special ARCNET network extender nodes, ARCNET computer slots for the operator workstation, and a main ARCNET controller hub. The physical connection can range from twisted pair, fiber optic, and coaxial cable. To sync the devices to the building's network, the ARCNET physical connection is wired from network extenders to the end-use devices all the way to the main hub. From an operator workstation, the ARCNET system can be programmed to building requirements. LonTalk was designed as a proprietary protocol by the Echelon Corporation, and eventually released as an open protocol. The design included Neuron chips embedded into their devices, allowing any type of physical wire routing schemes between devices. The protocol comes with a software application to sync the devices and control the network.

IV. BASE BUILD COST FOR THE TEST LAB

BACnet-controlled applications range from Direct Digital Controls (DDCs), such as variable air volume boxes, to complete devices, such as thermostats. For this lab, it would be ideal to get a test controller that could interface with DDC, Ethernet, and MS/TP. ARCnet and LonTalk are old protocols with a limited number of users. It would be best to target the larger part of the sector. The base model build only requires a BACnet controller, with connection leads for the possible physical connections, and a Personal Computer (PC). A router may be necessary to create a virtual IP subnetwork, depending on how the facility network using this test board reacts to directly connecting the BACnet controller. As an open source, there is free software available on the internet that can be installed on a PC to control BACnet. With the hardware and software mentioned, a BACnet test lab could be created to test DDC, Ethernet, and MS/TP.

The most popular physical wiring connection types (Ethernet and shielded twisted pair) are recommended. Table 11 provides a cost breakdown of the simplest setup that will be able to test the most popular types, like Ethernet, RS-485 twisted wire, and Direct Digital Control.

Table 11. Cost Breakdown to Build a Test Lab*

BACnet controller, BACnet client/server 22-point 6 relay	$325
Router to create virtual IP subnetwork	$37
Ethernet cables x3	$5
Shielded twisted pair of wire 1’ - $6 (estimate taken from 100’ roll)	$6
Total cost of BACnet test lab equipment - $373	$373

*This does not include the cost of the mounting material, which will depend on the final test lab decision.

V. Research Findings

a. Barriers to Auto-DR Integration

Some manufacturers have proprietary controls for their devices (for example, Mitsubishi Variable Refrigerant Flow systems) and offer BACnet connectivity as an additional license to purchase. Small businesses hoping to use the secondary BACnet protocol to initiate DR may be faced with the burden of purchasing the BACnet license.

When commissioning BACnet devices, depending on how the device connects to the network, an engineer may be needed to understand the schematics and how to set up the application. Due to the open-source protocol and other factors, a BACnet test lab is potentially viable for creating an ADR test lab.