EPIC Final Report

Program	**Electric Program Investment Charge (EPIC)**
Administrator	**San Diego Gas & Electric Company**
Project Number	**EPIC-1, Project 4**
Project Name	**Demonstration of Grid Support Functions of Distributed Energy Resources (DER)**
Module Name	**Module 2, Pre-Commercial Demonstration of Communication Standards for DER**
Date	**December 31, 2017**

Attribution

This comprehensive final report documents the work done in this EPIC project.

The project team for this work included the following individuals:

Internal SDG&E Staff

Frank Goodman

Zoltan Kertay

Prajwal Raval

Amin Salmani

Aung Thant

Kitu Systems, Inc.

Gordon Lum

Executive Summary

The objective of EPIC-1, Project 4, Demonstration of Grid Support Functions of Distributed Energy Resources (DER) was to demonstrate grid support functions of DER, which can improve distribution system operations. The chosen sub-projects and modules quantified the value of specific grid support functions in specific application situations and provided a basis for San Diego Gas & Electric Company (SDG&E) to determine which functions it wants to pursue commercially in the development of its smart grid. This project consists of three modules: value assessment of grid support functions of DER, communication standards for grid support functions of DER, and demonstration and comparison of the Electric Power Research Institute (EPRI) and SDG&E DER hosting capacity analysis tools. This executive summary addresses the module on pre-commercial demonstration of communication standards for grid support functions of DER.

With the proliferation of residential solar and storage systems, the CPUC is in the process of updating California Electric Tariff Rule 21 (CA Rule 21) governing the interconnection of generation and storage resources to utility distribution systems. As part of the update to CA Rule 21, the Smart Inverter Working Group (SIWG) has generated recommendations regarding DER grid support functions, the ability to modify and control these functions, and the needed communication standards. The CA Rule 21 update has been partitioned into 3 phases, with Phase 1 addressing the implementation of autonomous functions that operate without the need for communications, Phase 2 addressing communications to control Phase 1 and Phase 3 functions, and Phase 3 addressing advanced functions.

At this time, Phase 1 functions are well defined, Phase 2 default communications protocol has been chosen, and Phase 3 functions will be designed to align with Institute of Electrical and Electronics Engineers (IEEE) 1547 (the IEEE standard for interconnecting distributed resources with electric power systems, which is also currently being updated).

Although IEEE 2030.5-2013 was chosen as the default communications protocol for CA Rule 21, the current standard (2013) does not fully support all the Phase 1 and Phase 3 functions. A revision to the IEEE 2030.5 specification to support all Phase 1 and Phase 3 functions is currently in process and may be ready for adoption in early 2018. In the long term, it cannot be known at this time what the communication protocol specified in CA Rule 21 will be.

This EPIC pre-commercial demonstration tested the communications performance of the IEEE 2030.5 protocol (also known as SEP 2.0) on testable Phase 1 functions. The objective was to determine the impact of protocol selection on the viability and value of DER grid support functions. The testable Phase 1 control commands includes connect/disconnect, power factor, volt-VAr, and real power output. The demonstration system consisted of an IEEE 2030.5 server on the internet that creates and stores Phase 1 control actions, a cellular gateway and Wi-Fi access point for providing internet connectivity, an IEEE 2030.5 DER protocol translator for converting IEEE 2030.5 controls to Modbus controls, and a DER Device that acts on the translated Phase 1 controls. IEEE 2030.5 security was applied to secure the communications.

All the testable Phase 1 functions were successfully sent from the IEEE 2030.5 server, received by the IEEE 2030.5 DER protocol translator, and executed by the DER device. In addition, metrology data (e.g., real and reactive power output) was successfully read from the DER device over Modbus, translated and sent by the IEEE 3020.5 DER protocol translator, and received by the IEEE 2030.5 server.

Analyzing the IEEE 2030.5 protocol shows that a polling model is used, whereby the DER protocol translator periodically polls the IEEE 2030.5 server for new control actions. This polling mechanism introduces a latency on the order of 10’s of seconds, so the IEEE 2030.5 protocol is well suited for “quasi-real-time” systems on the order of 10’s of seconds to minutes. Thus, it is not suited for system response times of seconds or sub-seconds.

The demonstration successfully showed that the IEEE 2030.5 protocol could successfully communicate Phase 1 functions. Some recommendations for future steps are:

1. Although this pre-commercial demonstration could only test a subset of the CA Rule 21 Phase 1 functions, IEEE 2030.5 appears to be the protocol of choice for providing quasi-real-time DER grid support services in the foreseeable future. Many stakeholders from the SIWG, standards organizations, equipment manufacturers, and utilities are actively working on harmonizing IEEE 2030.5 with CA Rule 21 and IEEE 1547. No other communications protocol is at this advanced stage of development. At this time, both the IEEE 2030.5 protocol and the Phase 3 functions are being revised and updated. As the protocols for the CA Rule 21 standard or for international standards change from time to time, the successful performance of the intended functions for the new protocols should be re-demonstrated for certification by a qualified organization to validate the suitability of the new standard each time. This validation process should verify that the updated IEEE 2030.5 protocol (or any other alternative that may be adopted in CA Rule 21 or international standards) could successfully transport all Phase 1 and Phase 3 functions. SDG&E is not a certification organization.
2. The IEEE 2030.5 security model uses a power cipher suite that cannot be easily broken even for desired functions like packet inspection. IT security departments should be aware of this fact and design/modify their IT infrastructure accordingly.
3. The DER device in this demonstration used a proprietary Modbus control map. For large-scale deployments, a standardized DER Modbus model needs to be used.

Table of Contents

List of Figures

Acronyms and Abbreviations

AES	Advanced Encryption Standard
CA Rule 21	California Electric Tariff Rule 21
CBC	Cipher Block Chaining
CPUC	California Public Utilities Commission
CSIP	Common Smart Inverter Profile
DC	Direct Current
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management System
DMZ	De-militarized Zone
DRLC	Demand Response Load Control
EPIC	Electric Program Investment Charge
EPRI	Electric Power Research Institute

ESS	Energy Storage System
IEEE	Institute of Electrical and Electronics Engineers
IOUs	Investor-Owned Utilities
IT	Information Technology
mRID	Master Resource Identifier
NSA	National Security Agency
PC	Personal Computer
PV	Photovoltaic
SDG&E	San Diego Gas & Electric Company
SIWG	Smart Inverter Working Group
SEP	Smart Energy Profile
SEP 2.0	Smart Energy Profile 2.0 (synonymous with IEEE 2030.5)
SFDI	Short Form Device Identifier
T&D	Transmission & Distribution
TLS	Transport Layer Security
WAF	Web Application Firewall

1.0 Introduction

1.1 Statement of Project Objective

The objective of EPIC-1, Project 4, Demonstration of Grid Support Functions of Distributed Energy Resources (DER) was to demonstrate grid support functions of DER, which can improve distribution system operations. The chosen sub-projects and modules quantified the value of specific grid support functions in specific application situations and provided a basis for SDG&E to determine which functions it wants to pursue commercially in the development of its smart grid. This project consists of three modules: value assessment of grid support functions of DER, communication standards for grid support functions of DER, and demonstration and comparison of the EPRI and SDG&E DER hosting capacity analysis tools. This final report addresses the second module on pre-commercial demonstration of communication standards for grid support functions of DER.

The California Public Utilities Commission (CPUC) initiated a rulemaking proceeding to review and, if necessary, revise the rules and regulations governing interconnecting generation and storage resources to the electric distribution systems. This proceeding is generally referred to as updates to Electric Tariff Rule 21 (CA Rule 21), and the Smart Inverter Working Group (SIWG) has been tasked with generating recommendations for this proceeding.

As a result of the SIWG work, CA Rule 21 has been divided into 3 phases:

- Phase 1 – Addresses autonomous functions that smart inverters must support. Autonomous means these functions must exist and work without the need for communications.
- Phase 2 – Addresses communications to change and/or control Phase 1 and Phase 3 functions. The default protocol for communications is IEEE 2030.5 (also known as SEP 2.0).
- Phase 3 – Addresses advanced smart inverter functions.

The focus of this module of the EPIC project was to perform a pre-commercial demonstration of IEEE 2030.5-2013 as a protocol to communicate CA Rule 21 DER grid support functions. Supported Phase 1 functions were tested. Phase 3 functions were not tested, because the list of advanced functions have not been finalized and current inverters do not yet support many of these advanced functions.

The IEEE 2030.5 protocol was chosen because it provides the most support for communicating with the DER controls required by CA Rule 21. IEEE 2030.5 was initially developed as Smart Energy Profile 2.0 (SEP 2.0). The purpose of SEP 2.0 was to provide an IP based protocol for communication smart energy functions like demand response load control (DRLC), metering, pricing, and DER. Subsequently, SEP 2.0 was formally ratified in 2013. Shortly after ratification, ownership and maintenance of the standard was transferred to IEEE, and the protocol was renamed IEEE 2030.5 and the adopted version was renamed IEEE 2030.5-2013. Therefore, SEP 2.0 and IEEE 2030.5 are the same protocols. The name “SEP 2.0” is now deprecated in favor of the name “IEEE 2030.5”.

1.2 Project Approach

For this pre-commercial demonstration, a test system was set up to perform the tests. The test system architecture is described in the next section. Seven test cases were tested. The description of each use case is described in the “Use Cases” section. For each test case, DER grid support controls were first created on the IEEE 2030.5 Server. The DER Protocol Translator, the DER Device, and the DER System Simulator were then started. All the IEEE 2030.5 communications were recorded for later analysis.

1.3 Test System Architecture

The test system architecture is shown in Figure 1. The system consists of the following components:

- **IEEE 2030.5 Server** – This server is the "front-end" of the utility Distributed Energy Resource Management System (DERMS). It can be thought of as an "IEEE 2030.5 protocol translator" that converts commands from the utility DERMs to IEEE 2030.5 format. For this demonstration, a real DERMS was not used. Instead, a human operator created the controls that DERMS would normally provide. These controls were entered via webpages linked to the IEEE 2030.5 internet server.
- **Cellular Gateway** – This device provides internet connectivity to the local DER test site.
- **Wi-Fi Access Poin**t – This device uses the Cellular Gateway to provide Wi-Fi internet access to devices at the DER test site.
- **DER Protocol Translator** – This device translates the IEEE 2030.5 protocol information to Modbus register controls for the DER. Physically, this device is a computer module running the IEEE 2030.5 DER client code. Logically, this device acts as IEEE 2030.5 client when interfacing to the IEEE 2030.5 server, and acts as Modbus master when interfacing with the DER Modbus slave. In this report, the term DER client will be used to refer to the DER protocol translator.
- **DER Device** – The DER device used in this system is an 88-kW Energy Storage System (ESS) that has been widely utilized in the SDG&E DER sites.
- **DER System Simulator** – The DER System Simulator consists of a real-time power system simulation, grid simulator (as power amplifier), smart inverter, direct current (DC) power supply to provide DC source as battery or photovoltaic (PV).
- **Ethernet Sniffer** – This is a personal computer (PC) monitoring Ethernet traffic between the Cellular Gateway and the Wi-Fi Access Point. At this location, the sniffer can monitor all traffic between the IEEE 2030.5 Server and the DER Protocol Translator.

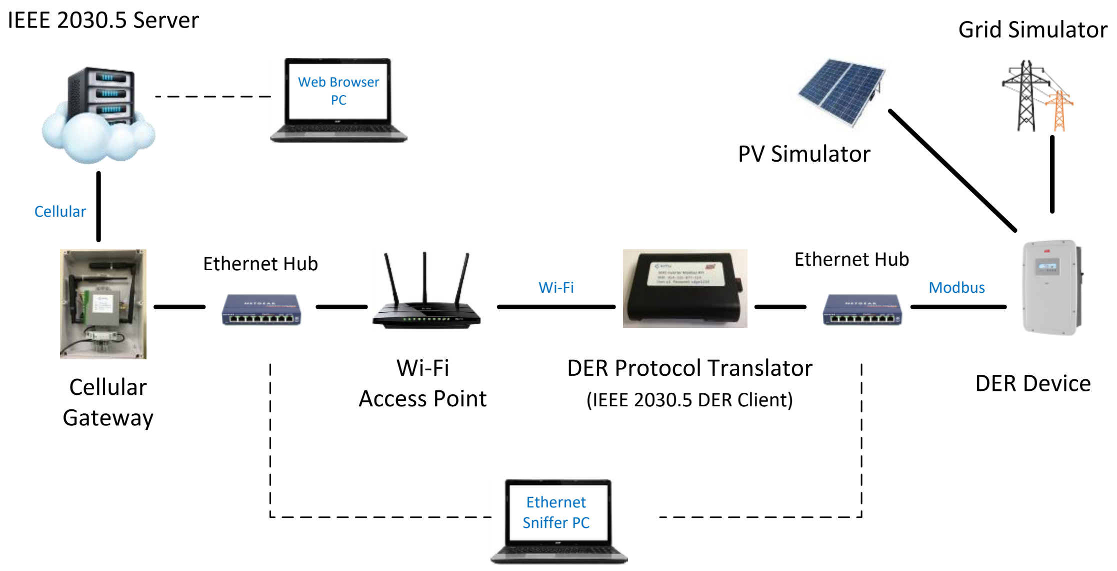


Figure 1 – Test System Architecture

1.4 Test Terminology and Other Information

This report uses information and terminology associated with the IEEE 2030.5 protocol. This section briefly explains some terms and information that will appear in this report.

- **Events** – In IEEE 2030.5, controls (e.g., real and reactive power settings) are events. An event is an IEEE 2030.5 resource that has a start time (in UTC), a duration (in seconds), and some control value.
- **mRID** – In IEEE 2030.5, an mRID is a 128-bit number that servers as a unique identifier of a resource on the server.
- Control values like real and reactive power settings are expresses as a percentage of the device's nameplate maximum settings. The DER Device used in this report has a real power output maximum setting of 50 kW and a reactive power output maximum of 50 kVAr. The units are in 0.01 percent (i.e., a value of 1 represents 0.01 percent, and a value of 10000 represents 100 percent). For example, to set the real power output to 90% of its nameplate maximum setting, a setting of 9000 is used.
- The DER Protocol Translator returns meter readings (e.g., real and reactive power output) read from the DER Device's Modbus registers. In IEEE 2030.5, meter readings have a value and a power of 10 multiplier. For all of the tests discussed in this report, the power of 10 multiplier was set to -1, so the unit of measure for real power is 0.1 watts and the unit of measure for reactive power is 0.1 VArs. For example, a reported power level of 500000 represents 50 kW.

2.0 Use Cases

This pre-commercial demonstration will test seven use cases. Each use case focuses on one or more DER functions that are expected to be important for grid support services.

2.1 Test #1 – Register the DER System

Registration is an important part of any production system as it provides a means of identifying and managing devices on the system. This test case will verify the Registration capabilities of the IEEE 2030.5 protocol.

2.2 Test #2 – Monitor the Output of the DER System

Many grid support services need to monitor the real and reactive power output of DER Devices. This information is important for evaluating the effectiveness of current controls and to forecast future controls. This test will verify the reporting capabilities of the IEEE 2030.5 protocol by measuring the real and reactive power outputs of the DER Device prior to and during an active DER control.

2.3 Test #3 – Issue Control Commands to the DER System

Many grid support services need to issue control commands to change the behavior of the DER Device. This test will verify the transmission of control commands using the IEEE 2030.5 protocol. The DER Device output (e.g., real and reactive power) will be measured prior to and during a control command to verify the command was properly executed.

2.4 Test #4 – Issue Set-Point Update to the DER System

Many grid support services need to change a set point of the DER device. This test will verify the transmission of set points using the IEEE 2030.5 protocol. The DER device output (e.g., real and reactive power) will be measured prior to and during a control command to verify the set point was properly executed.

2.5 Test #5 – Activation and Deactivation Commands to the DER System

Many grid support services need to activate/deactivate a DER Device. This test will verify the transmission of an activate/deactivate command using the IEEE 2030.5 protocol. The DER Device output (e.g., real and reactive power) will be measured prior to and during a control command to verify the activate/deactivate command was properly executed.

2.6 Test #6 – Simulate Multiple DER Systems

The performance of a system when connected to multiple DER Devices needs to be tested and analyzed. This data is needed to estimate system performance as the system is scaled to production levels. This test will verify the performance of the system when connected to multiple DER Devices that are simultaneously polling for DER controls and posting metrology data.

3.0 Project Results

SIWG has defined California Rule 21 Phase 1 functions to be:

1. High/Low Voltage Ride Through
2. High/Low Frequency Ride Through
3. Ramp Rate
4. Connect/Disconnect
5. Fixed Power Factor
6. Volt-Var Control
7. Real Power Output Control

Ideally, all Phase 1 functions should be demonstrated, but the DER Device utilized in this test system did not support all the Phase 1 functions. To be more specific, this DER device supported the ride through functions and ramp rate control, but these settings cannot be changed over Modbus. Therefore, the subset of testable Phase 1 functions were:

1. Connect/Disconnect
2. Fixed Power Factor
3. Volt-Var Control
4. Real Power Output Control

3.1 Test #1 – Register the DER System

3.1.1 Definitions

To understand IEEE 2030.5 registration, the definitions of a few terms may be helpful:

- **EndDevice** – An EndDevice is a resource on the Server that represents a unique physical client device. For this project, the physical client device is the DER client (i.e., the DER Protocol Translator). Information about the client device and specific commands to a client device are realized using this resource. An EndDevice is uniquely identified using its short-form device identifier (SFDI) that is unique to the device.
- **SFDI** (Short-Form Device Identifier) – Each EndDevice is uniquely identified by its SFDI. The SFDI is a 12-digit decimal number derived from hashing the device's unique Device Certificate. For these tests, the IEEE 2030.5 DER Protocol Translator contains the unique Device Certificate. The SFDI of this Device Certificate, which is used in all the tests, is "14336077324".
- **Device Certificate** – In IEEE 2030.5, all client devices must have a unique device certificate. For all tests in this report, the device certificate is in the IEEE 2030.5 DER Protocol Translator. The device certificate is an X.509 digital certificate that chains back to the Root Certificate Authority. The device certificate is used to authenticate the identity of the client device. The SFDI is derived from the device certificate. It is computed by taking the first 36-bits of the SHA-256 Hash of the device certificate.
- **Registration** – In IEEE 2030.5, there are two sides to registration
  - **Server Registration** – Server registration refers to the creation of the EndDevice resource for "registered" devices. This is an out-of-band process where the client information (e.g., SFDI) is used to

create the corresponding EndDevice resource on the IEEE 2030.5 server. In the project, server registration is performed using the “create inverter” function on the server webpage.
    - **Client Registration** – Client registration occurs when the DER client device finds its EndDevice information on the server and verifies the registration PIN is correct. If registration is confirmed, the DER client continues with normal operation. If registration is not-confirmed, the DER client ceases operation with the server.
- **Registration PIN** – The registration PIN is a resource associated with the EndDevice entry. It contains a 6-digit code that the DER client uses to verify registration. This code is shared between the server and DER client via an out-of-band process. In this project, the PIN that is used is “111115” and is provisioned into the server and DER client prior to the start of testing.

3.1.2 Description

Registration is an important step in managing and controlling DER devices. In IEEE 2030.5, server registration is used to maintain a list of authorized EndDevices, and client registration is used to verify that a specific EndDevice is permitted to access the server. To verify server and client registrations, the initial communications between the server and DER client was captured and analyzed to confirm the DER client successfully retrieved its EndDevice resource and verified the registration PIN.

3.1.3 Procedure

The test procedure was:

1. Configure the DER client to use unencrypted HTTP to allow for Ethernet sniffer captures.
2. Start the Ethernet sniffer trace.
3. Start the DER client.
4. Wait 2 minutes.
5. Stop the DER client.
6. Stop the Ethernet sniffer trace.

3.1.4 Results

The full trace is captured in the Ethernet sniffer file: “Real-80.pcapng”

The packet in Figure 2 shows the EndDevice instance of the DER device containing the correct SFDI value of 14336077324. This verifies server registration.

```
GET /sep2/edev HTTP/1.1
Accept: application/sep+xml
Host: 52.35.96.64:8080

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Content-Type: application/sep+xml; charset=utf-8
Content-Length: 544
Date: Wed, 16 Aug 2017 21:55:02 GMT
Connection: keep-alive

<EndDeviceList href="/sep2/edev" subscribable="1" all="1" results="1" xmlns="http://zigbee.org/sep"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <EndDevice href="/sep2/edev/31" subscribable="1">
                <sFDI>14336077324</sFDI>
                <RegistrationLink href="/sep2/edev/31/rg"/>
                <DERListLink href="/sep2/edev/31/der" all="1"/>
                <LogEventListLink href="/sep2/edev/31/lel" all="0"/>
                <SubscriptionListLink href="/sep2/edev/31/sub" all="0"/>
                <FunctionSetAssignmentsListLink href="/sep2/fsagrp/22/fsa" all="1"/>
        </EndDevice>
</EndDeviceList>
```

Figure 2 - Server Registration

The packet in Figure 3 shows the correct registration PIN of 111115 is retrieved. This verifies Client Registration.

```
GET /sep2/edev/31/rg HTTP/1.1
Accept: application/sep+xml
Host: 52.35.96.64:8080

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Content-Type: application/sep+xml; charset=utf-8
Content-Length: 210
Date: Wed, 16 Aug 2017 21:55:03 GMT
Connection: keep-alive

<Registration href="/sep2/edev/31/rg" xmlns="http://zigbee.org/sep"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <dateTimeRegistered>1502495010</dateTimeRegistered>
        <pIN>111115</pIN>
</Registration>
```

Figure 3 - Client Registration

3.2 Test #2 – Monitor the Output of the DER system

3.2.1 Description

This purpose of this test is to verify the reporting of the output of the DER system. The DER device is capable of reporting real power and reactive power. This test verifies the reporting of this data. The DER device is configured to post real and reactive power readings roughly every 10 seconds. This test is run using a fixed power-factor control to enable both real and reactive power output.

3.2.2 Procedure

Test procedure was:

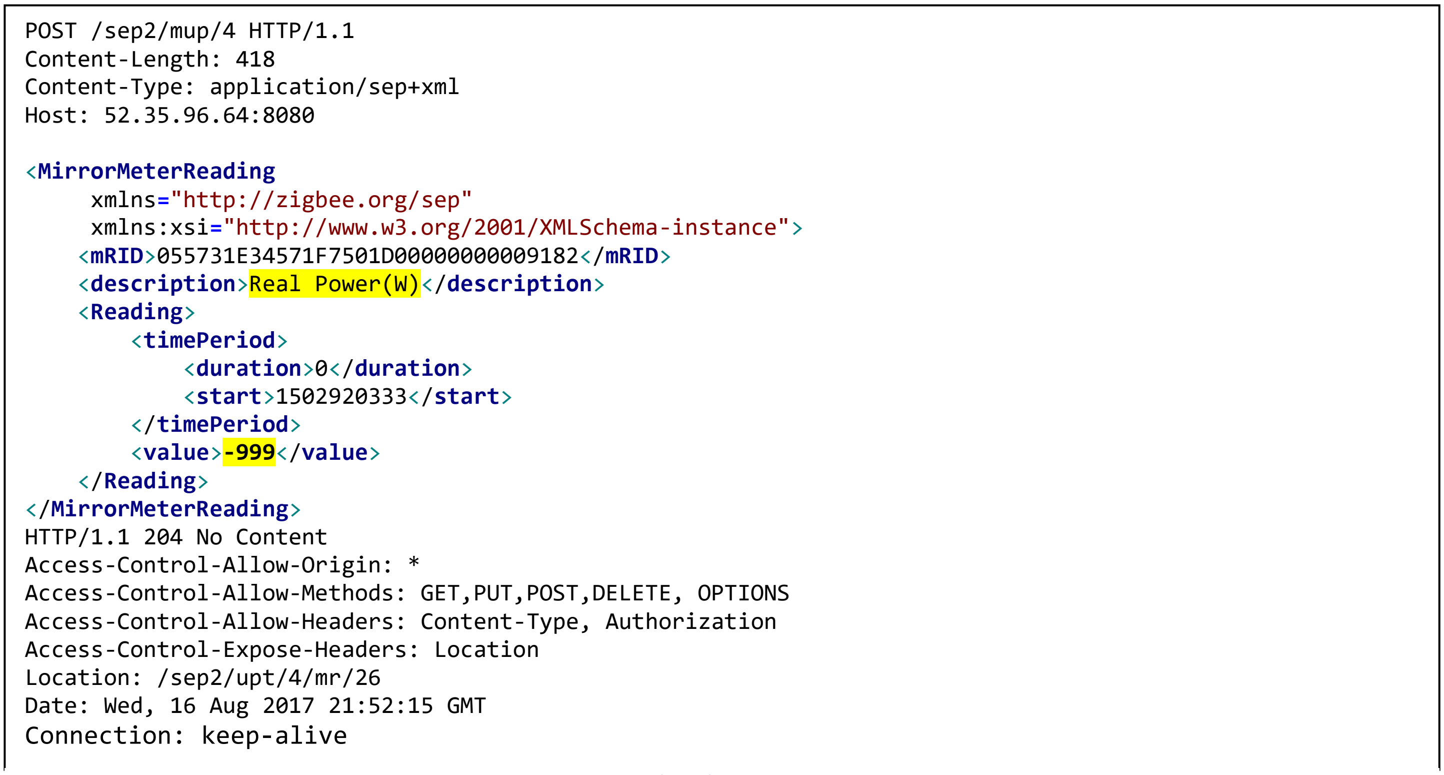
1. Configure the DER device to use unencrypted HTTP to allow for Ethernet sniffer captures.
2. Start the Ethernet sniffer trace.
3. Start the DER client.
4. Schedule a fixed power-factor control for 2 minutes.
5. Wait 3 minutes.
6. Stop the DER client.
7. Stop the Ethernet sniffer trace.

3.2.3 Results

The full trace is captured in the Ethernet sniffer file: “PF-90-30.pcapng”

Verify that the DER client is periodically reporting real and reactive power. The relevant packets are shown below.

The packet in Figure 4 shows the reported real power output prior to the start of the DER control event. The reported value is **-999** which indicates the DER device is disconnected (i.e., no real power exported).



```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 418
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501D00000000009182</mRID>
    <description>Real Power(W)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920333</start>
        </timePeriod>
        <value>-999</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/26
Date: Wed, 16 Aug 2017 21:52:15 GMT
Connection: keep-alive
```

Figure 4 - Reported Real Power prior to Event Start

The packet in Figure 5 shows the reported reactive power output prior to the start of the DER control event. The reported value is **-999** which indicates the DER device is disconnected (i.e., no reactive power exported).

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 424
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501A00000000009182</mRID>
    <description>Reactive Power(VAr)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920333</start>
        </timePeriod>
        <value>-999</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/29
Date: Wed, 16 Aug 2017 21:52:16 GMT
Connection: keep-alive
```

Figure 5 - Reported Reactive Power prior to Event Start

The packet in Figure 6 shows the reported real power output after the start of the DER control event. The reported value is **443000** which represents 44,300 Watts.

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 420
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501D00000000009182</mRID>
    <description>Real Power(W)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920383</start>
        </timePeriod>
        <value>443000</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/26
Date: Wed, 16 Aug 2017 21:53:05 GMT
Connection: keep-alive
```

Figure 6 - Reported Real Power after Event Start

The packet in Figure 7 shows the reported reactive power output after the start of the DER control event. The reported value is **150000** which is 15,000 VArs.

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 426
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501A00000000009182</mRID>
    <description>Reactive Power(VAr)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920383</start>
        </timePeriod>
        <value>150000</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/29
Date: Wed, 16 Aug 2017 21:53:06 GMT
Connection: keep-alive
```

Figure 7 - Reported Reactive Power after Event Start

3.3 Test #3, #4 – Issue Control Commands, Issue Set Point Updates

3.3.1 Description

In IEEE 2030.5, there is no distinction between "control commands" and "set point updates". Both are considered a DER control in IEEE 2030.5 parlance, so test case #3 and test case #4 are the same tests with different control commands. A DER control is an IEEE 2030.5 event that has a start time, duration, and a control value. Prior to a control event, the control is either "off" or operating under a default control value. At the start time of the event, the control is enabled at a certain set point value for the specified duration. Once the duration has expired, the control reverts to "off" or its default control value. The following Phase 1 functions were tested: Fixed Power-Factor and Volt-Var.

3.3.2 Fixed Power-Factor Procedure

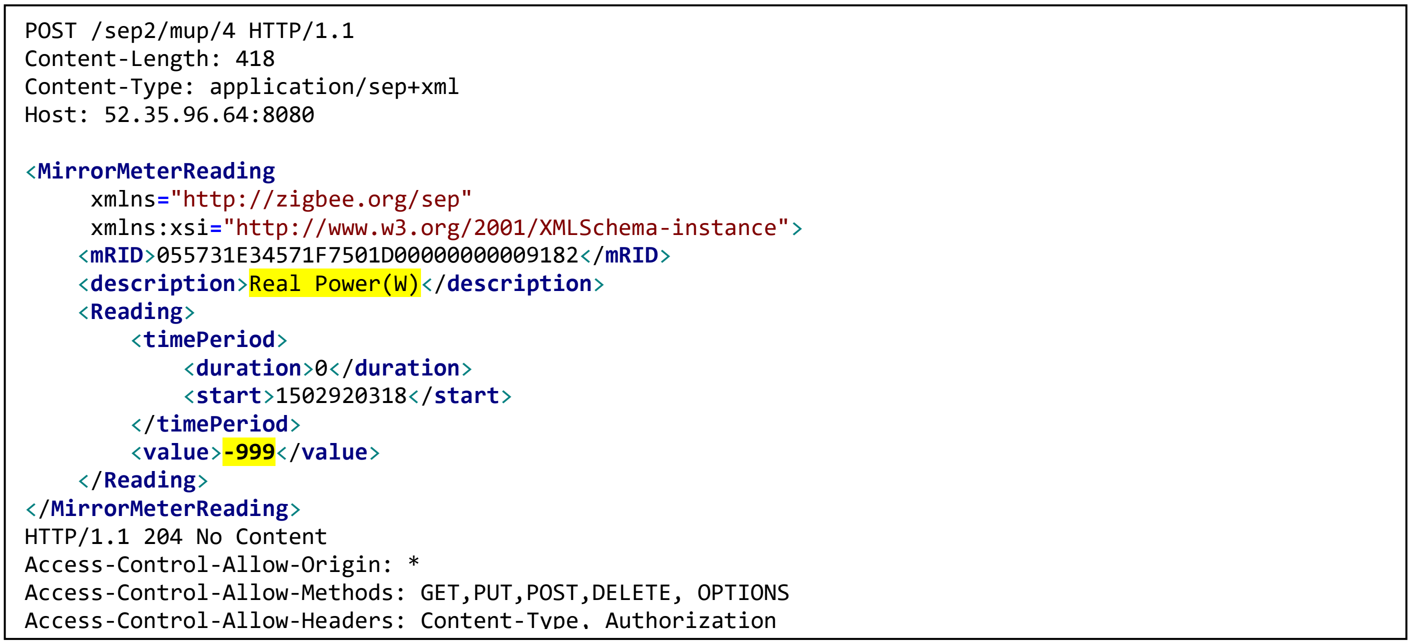
The purpose of this test was to verify that a fixed power factor DER control function was successfully communicated to the DER device. The DER device under test did not directly support the fixed power factor function, so the server converts the power factor setting to a real and reactive power setting based on the nameplate power rating. In this test, the nameplate power setting is 50000 Watts. The test sequence was:

1. Configure the DER client to use unencrypted HTTP to allow for Ethernet sniffer captures.
2. Start the Ethernet sniffer trace.
3. Start the DER client.
4. Schedule a power factor control for 2 minutes.
5. Wait 3 minutes.
6. Stop the DER client.
7. Stop the Ethernet sniffer trace.

3.3.3 Results

The full trace is captured in the Ethernet sniffer file: “PF-90-30.pcapng”. The relevant packets from that file are provided below.

The packet in Figure 8 shows the reported real power output prior to the start of the DER control event. The reported value is **-999** which indicates the DER device is disconnected (i.e., no real power exported).

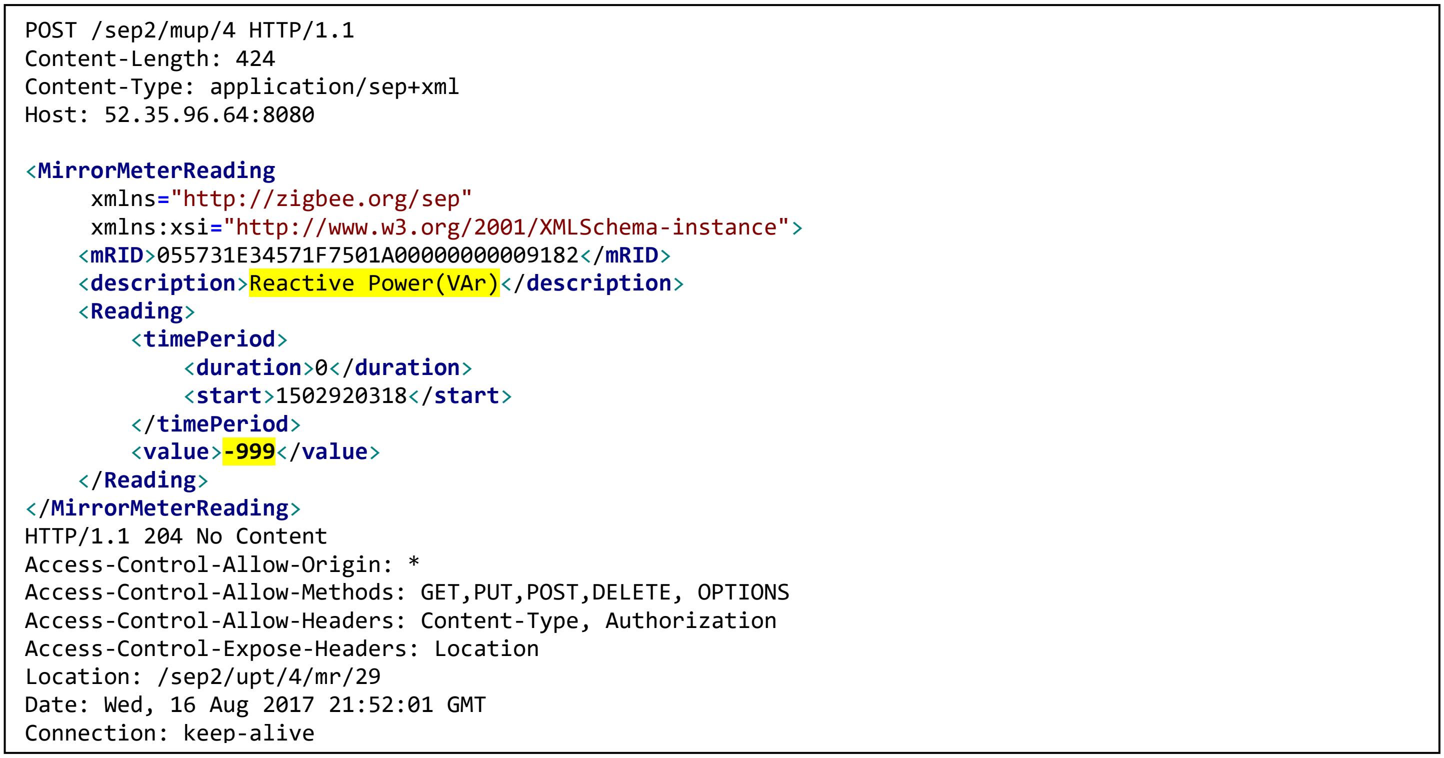


```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 418
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501D00000000009182</mRID>
    <description>Real Power(W)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920318</start>
        </timePeriod>
        <value>-999</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
```

Figure 8 - Reported Real Power prior to Event Start

The packet in Figure 9 shows the reported reactive power output prior to the start of the DER control event. The reported value is **-999** which indicates the DER device is disconnected (i.e., no reactive power exported).



```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 424
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501A00000000009182</mRID>
    <description>Reactive Power(VAr)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920318</start>
        </timePeriod>
        <value>-999</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/29
Date: Wed, 16 Aug 2017 21:52:01 GMT
Connection: keep-alive
```

Figure 9 - Reported Reactive Power prior to Event Start

The packet in Figure 10 shows the DER control event. The “opModFixedW” is the real power output control and the “opModFixeVAr” is the reactive power control. Real power output is set to 90% (**9000**) of its rated value and the reactive power output is set to 30% (**3000**) of its rated value. The rated value for the DER device in this test is 50000 Watts, so the target real output level is 45,000 Watts and the target reactive output power level is 15,000 VArs.

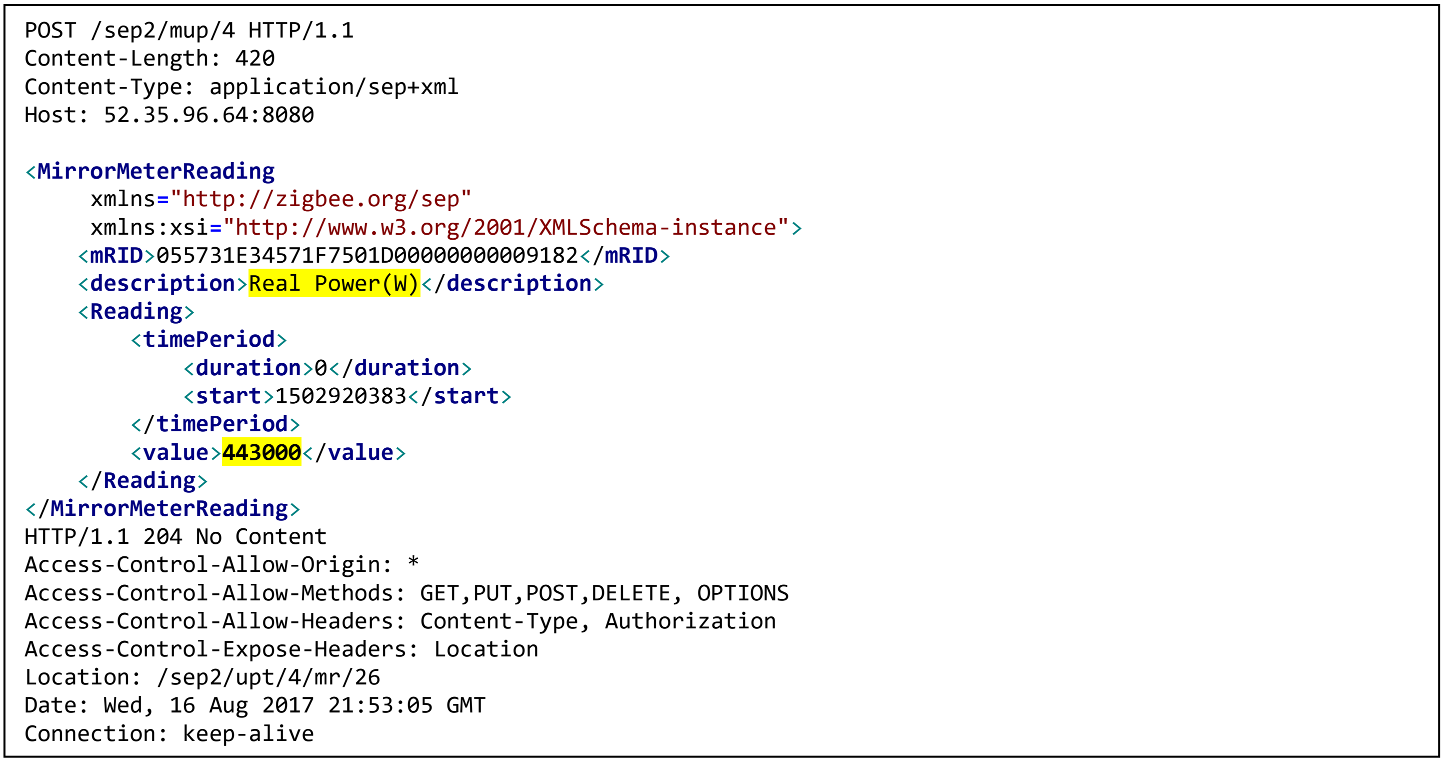
```
GET /sep2/derp/20/derc HTTP/1.1
Accept: application/sep+xml
Host: 52.35.96.64:8080

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Content-Type: application/sep+xml; charset=utf-8
Content-Length: 763
Date: Wed, 16 Aug 2017 21:52:43 GMT
Connection: keep-alive

<DERControlList href="/sep2/derp/20/derc" subscribable="1" all="1" results="1"
xmlns="http://zigbee.org/sep" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <DERControl href="/sep2/derp/20/derc/77" subscribable="1">
    <mRID>150292036095</mRID>
    <description>PF</description>
    <creationTime>1502920359</creationTime>
    <interval>
      <duration>90</duration>
      <start>1502920368</start>
    </interval>
    <EventStatus>
      <currentStatus>0</currentStatus>
      <dateTime>1502920361</dateTime>
      <potentiallySuperseded>false</potentiallySuperseded>
    </EventStatus>
    <DERControlBase>
      <opModFixedVAr>
        <refType>0</refType>
        <value>3000</value>
      </opModFixedVAr>
      <opModFixedW>9000</opModFixedW>
    </DERControlBase>
  </DERControl>
</DERControlList>
```

Figure 10 - DER Control, Real and Reactive

The packet in Figure 11 shows the reported real power output during to the DER control event. The reported value is **443000**, which is close to the targeted real output level of 45,000 Watts. At the time the power reading was captured, the DER device was still ramping up its output to match the target set point, which is why the reading is a little less that the target value.



```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 420
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501D00000000009182</mRID>
    <description>Real Power(W)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920383</start>
        </timePeriod>
        <value>443000</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/26
Date: Wed, 16 Aug 2017 21:53:05 GMT
Connection: keep-alive
```

Figure 11 - Real Power output during DER Control Event

The packet in Figure 12 shows the reported reactive power output during to the DER control event. The reported value is **150000**, which is exactly matches the targeted reactive output level of 15,000 VArs.

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 426
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501A00000000009182</mRID>
    <description>Reactive Power(VAr)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920383</start>
        </timePeriod>
        <value>150000</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/29
Date: Wed, 16 Aug 2017 21:53:06 GMT
Connection: keep-alive
```

Figure 12 - Reactive Power output during DER Control Event

3.3.4 Volt-VAr Procedure

The objective of this test was to verify the Volt-VAr function was successfully communicated to the DER device using IEEE 2030.5. IEEE 2030.5 uses a curve-based model for specifying reactive power behavior based on voltage. The DER device uses a voltage-droop model. The DER client translates IEEE 2030.5 curve-based parameter to voltage-droop parameters. The test procedure was:

1. Configure the DER client to use unencrypted HTTP to allow for Ethernet sniffer captures.
2. Start the Ethernet sniffer trace.
3. Start the DER client.
4. Schedule a Volt-VAr control for 2 minutes.
5. After the start of the Volt-VAr control, create a voltage disturbance and observe the resulting reactive power behavior.
6. Stop the DER client.
7. Stop the Ethernet sniffer trace.

3.3.5 Results

The full trace is captured in the Ethernet sniffer file: “volt-var.pcapng”. The relevant packets from that file are provided below.

The packet in Figure 13 shows the reported reactive power output prior to the start of the DER control event. The reported value is **-999** which indicates the DER device is disconnected (i.e., no reactive power exported).

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 424
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501A00000000009182</mRID>
    <description>Reactive Power(VAr)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502922283</start>
        </timePeriod>
        <value>-999</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/29
Date: Wed, 16 Aug 2017 22:24:45 GMT
Connection: keep-alive
```

Figure 13 - Reported Reactive Power prior to Event Start

The packet in Figure 14 shows the DER control event. The “opModVoltVAr” is the Voltage-VAr curve control. The DER client will translate this control to a Voltage-Droop control for the DER device.

```
GET /sep2/derp/20/derc HTTP/1.1
Accept: application/sep+xml
Host: 52.35.96.64:8080

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Content-Type: application/sep+xml; charset=utf-8
Content-Length: 679
Date: Wed, 16 Aug 2017 22:24:57 GMT
Connection: keep-alive

<DERControlList href="/sep2/derp/20/derc" subscribable="1" all="1" results="1"
xmlns="http://zigbee.org/sep" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <DERControl href="/sep2/derp/20/derc/81" subscribable="1">
    <mRID>150292228620</mRID>
    <description>vv</description>
    <creationTime>1502922284</creationTime>
    <interval>
      <duration>210</duration>
      <start>1502922299</start>
    </interval>
    <EventStatus>
      <currentStatus>0</currentStatus>
      <dateTime>1502922286</dateTime>
      <potentiallySuperseded>false</potentiallySuperseded>
    </EventStatus>
    <DERControlBase>
      <opModVoltVAr href="/sep2/dc/29"/>
    </DERControlBase>
  </DERControl>
</DERControlList>
```

Figure 14 - Volt-VAr Curve DER Event

The packet in Figure 15 shows the reported reactive power output during a voltage disturbance. The reported value is **286000**, which translates to 28,600 VArs. The reported value matched the value displayed on the DER device's front-panel screen.

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 426
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501A00000000009182</mRID>
    <description>Reactive Power(VAr)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502922405</start>
        </timePeriod>
        <value>286000</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/29
Date: Wed, 16 Aug 2017 22:26:47 GMT
Connection: keep-alive
```

Figure 15 - Reported Reactive Power during Voltage Disturbance

3.4 Test #5 – Activation and Deactivation Mode Commands

3.4.1 Description

There is no explicit "Activation/Deactivation" command in either IEEE 2030.5 or the Phase 1 functions. However, the Phase 1 connect/disconnect control serves the same purpose as Activation/Deactivation, so it will be used for this test.

The Phase 1 connect/disconnect control verifies the DER system exports zero power when commanded to disconnect. However, zero power does not mandate a physical disconnect – just no power exported. Therefore, this connect/disconnect control is already an inherent part of the real power output control. When the real power output control is not active, it is already in the zero power (disconnected) state. The bottom line is that the real power output control demonstrates both the connect/disconnect function and the real power output function.

Therefore, the purpose of this test was to verify the connect/disconnect DER control function was successfully communicated to the DER device by using the real power output control.

3.4.2 Connect/Disconnect and Real Power Output Procedure

The test procedure was:

1. Configure the DER client to use unencrypted HTTP to allow for Ethernet sniffer captures.
2. Start the Ethernet sniffer trace.
3. Start the DER client.
4. Schedule a real power output control for 2 minutes.
5. Wait 3 minutes.
6. Stop the DER client.
7. Stop the Ethernet sniffer trace.

3.4.3 Results

The full trace is captured in the Ethernet sniffer file: "Real-80.pcapng". The relevant packets from that file are provided below. The packet in Figure 16 shows the reported real power output prior to the start of the DER control event. The reported value is -999 which indicates the DER device is disconnected (i.e., no real power exported).

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 418
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501D00000000009182</mRID>
    <description>Real Power(W)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920542</start>
        </timePeriod>
        <value>-999</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/26
Date: Wed, 16 Aug 2017 21:55:45 GMT
Connection: keep-alive
```

Figure 16 - Reported Real Power prior to Event Start

The packet in Figure 17 shows the DER control event. This “opModFixedW” control is the real power output control that sets the real power output level to 80% (**8000**) of its rated value. The rated value for the DER device in this test is 50000 Watts, so the target output level is 40,000 Watts.

```
GET /sep2/derp/20/derc HTTP/1.1
Accept: application/sep+xml
Host: 52.35.96.64:8080

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Content-Type: application/sep+xml; charset=utf-8
Content-Length: 679
Date: Wed, 16 Aug 2017 21:56:27 GMT
Connection: keep-alive

<DERControlList href="/sep2/derp/20/derc" subscribable="1" all="1" results="1"
xmlns="http://zigbee.org/sep" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <DERControl href="/sep2/derp/20/derc/78" subscribable="1">
                <mRID>150292055895</mRID>
                <description>Real W</description>
                <creationTime>1502920557</creationTime>
                <interval>
                        <duration>90</duration>
                        <start>1502920569</start>
                </interval>
                <EventStatus>
                        <currentStatus>1</currentStatus>
                        <dateTime>1502920569</dateTime>
                        <potentiallySuperseded>false</potentiallySuperseded>
                </EventStatus>
                <DERControlBase>
                        <opModFixedW>8000</opModFixedW>
                </DERControlBase>
        </DERControl>
</DERControlList>
```

Figure 17 - Reported Reactive Power prior to Event Start

The packet in Figure 18 shows the reported real power output during to the DER control event. The reported value is **394000**, which translates to 39,400 W and is close to the targeted output level of 40,000 W.

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 420
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501D00000000009182</mRID>
    <description>Real Power(W)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920619</start>
        </timePeriod>
        <value>394000</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/26
Date: Wed, 16 Aug 2017 21:57:02 GMT
Connection: keep-alive
```

Figure 18 - Reported Real Power after Event Start

The packet in Figure 19 shows the reported real power output after to the DER control event has completed. The reported value is **-999** which indicates the DER device is back to the disconnected (i.e., no real power exported).

```
POST /sep2/mup/4 HTTP/1.1
Content-Length: 418
Content-Type: application/sep+xml
Host: 52.35.96.64:8080

<MirrorMeterReading
     xmlns="http://zigbee.org/sep"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <mRID>055731E34571F7501D00000000009182</mRID>
    <description>Real Power(W)</description>
    <Reading>
        <timePeriod>
            <duration>0</duration>
            <start>1502920665</start>
        </timePeriod>
        <value>-999</value>
    </Reading>
</MirrorMeterReading>
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,PUT,POST,DELETE, OPTIONS
Access-Control-Allow-Headers: Content-Type, Authorization
Access-Control-Expose-Headers: Location
Location: /sep2/upt/4/mr/26
Date: Wed, 16 Aug 2017 21:57:48 GMT
Connection: keep-alive
```

Figure 19 - Reported Real Power after Event Completion

3.5 Test #7 – Cyber Security Tests

3.5.1 Description

Security is an important part of any communications system. For grid support services, security is especially important as breaches can lead issues with grid safety, stability, and reliability. This test examines and tests the cyber security features of the system. Cyber security is based on the underlying security of the IEEE 2030.5 protocol. IEEE 2030.5 uses the following cipher suite to protect communications between end points: *TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8*. This cipher suite is compliant with NSA Suite B requirements for security at the SECRET level. It is helpful to understand the security components of the cipher suite.

- **TLS (Transport Layer Security)** – The TLS part of the cipher suite indicates that TLS is used. TLS is a well-known and well-supported security transport layer. For this cipher suite, the TLS version used is 1.2.
- **ECDHE** – The ECDHE part of the cipher suite indicates the key exchange algorithm used. ECDH stands for "elliptic-curve Diffie-Hellman".
    - The "EC" part indicates that elliptic curve cryptography is used instead of RSA. For this cipher suite, the exact curve is the well-known NIST P-256 curve, with provides 128 bits of security protection.
    - The "DH" part indicates that the Diffie-Hellman algorithm, as applied to elliptic curves, is used to generate the shared secret between the client and the server.
    - The final "E" part indicates that ephemeral keys are used. This means that a new set of elliptic curve keys are generated for every new TLS session. This feature provides "perfect forward secrecy", a property of secure communication protocols in which compromise of long-term keys does not compromise past session keys.

- **ECDSA** – This part indicates that elliptic-curve digital signatures are used for the authentication of certificates and other data. Each TLS end point contains a unique digital certificate for authentication.
- **AES_128** – This part indicates that the Advanced Encryption Standard (AES) algorithm is used for bulk traffic encryption using 128-bit keys derived from the Diffie-Hellman shared secret. The 128-bit AES key provides 128 bits of security protection.
- **CCM_8** – This part indicates the use of the cipher block chaining (CBC)-Counter Mode for the Message Authentication Check (MAC).

The secure channel is between the server and the DER client. They are the end points of the TLS protocol. With the Ethernet sniffer, you can capture the TLS handshaking prior to the switch to encrypted mode. Once this happens, the Ethernet sniffer trace only shows encrypted payload data.

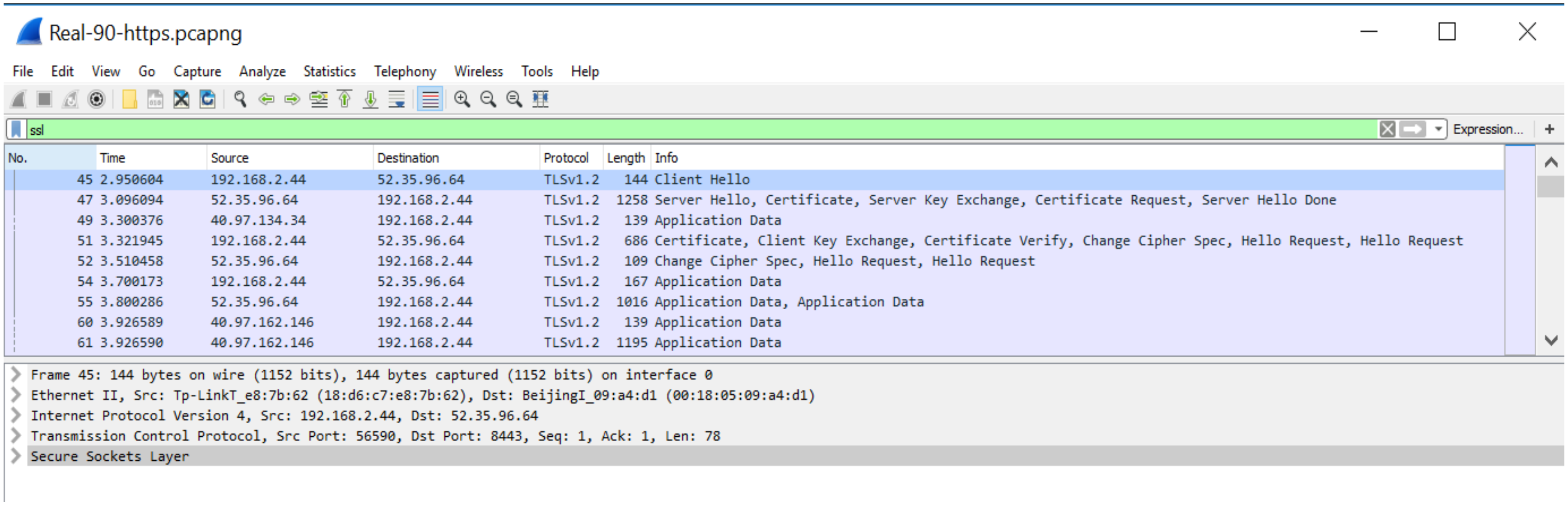
3.5.2 Basic TLS Handshake

The purpose of this test was to verify the basic TLS handshake using the IEEE 2030.5 cipher suite. The test procedure was:

1. Configure the DER client to use encrypted HTTPS to capture the TLS transactions. The TLS port is 8443.
2. Start the Ethernet sniffer trace. The TLS port is 8443, so use this as an Ethernet sniffer filter
3. Start the DER client.
4. Schedule a real power output control for 2 minutes.
5. Wait 3 minutes.
6. Stop the DER client.
7. Stop the Ethernet sniffer trace.

3.5.3 Results

The full trace is captured in the Ethernet sniffer file: “Real-90-https.pcapng”. The screen capture in Figure 20 shows the TLS handshake between the client and server. Note that after the “Change Cipher Spec” packet, all subsequent packets are fully encrypted.



Real-90-https.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression…
+

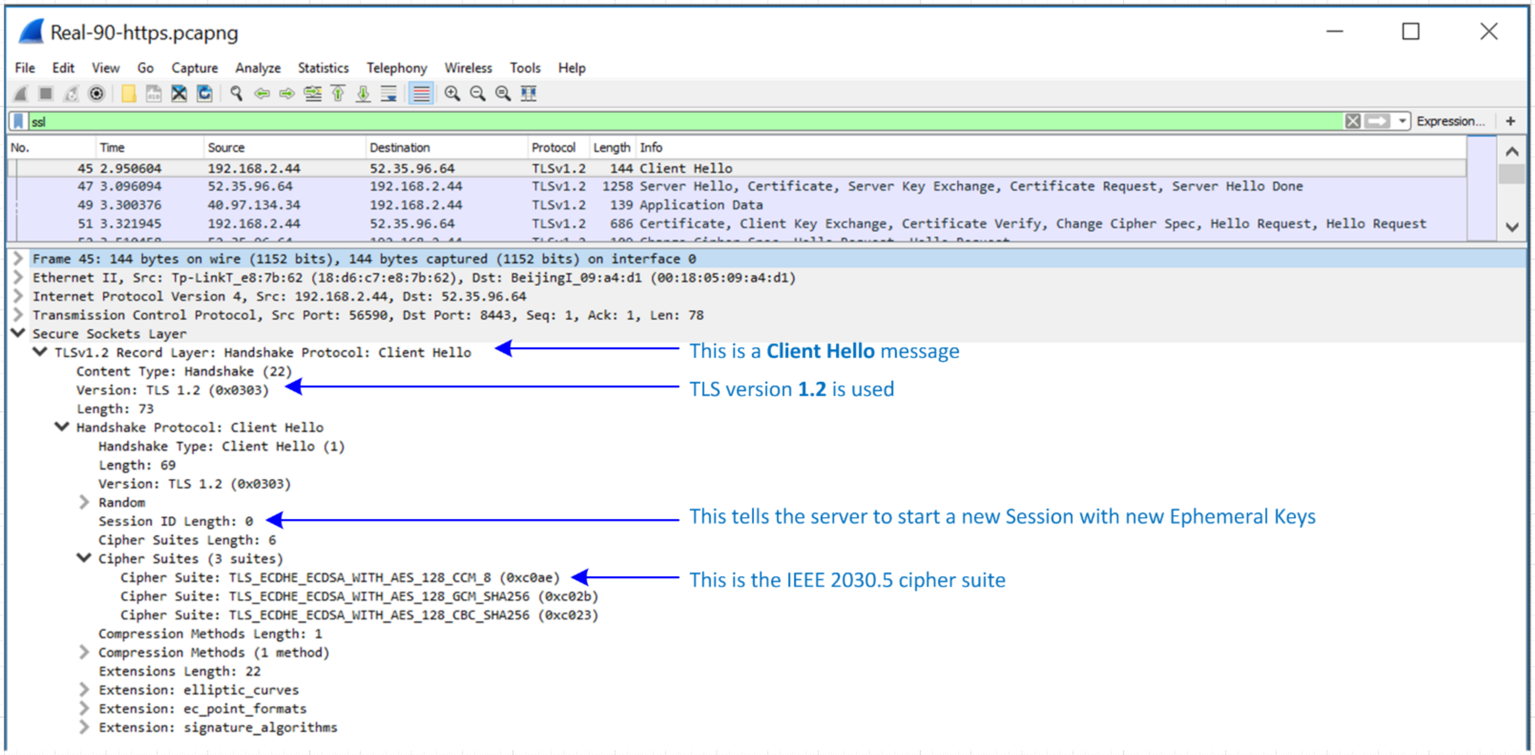
No.	Time	Source	Destination	Protocol	Length	Info
45	2.950604	192.168.2.44	52.35.96.64	TLSv1.2	144	Client Hello
47	3.096094	52.35.96.64	192.168.2.44	TLSv1.2	1258	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
49	3.300376	40.97.134.34	192.168.2.44	TLSv1.2	139	Application Data
51	3.321945	192.168.2.44	52.35.96.64	TLSv1.2	686	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Hello Request, Hello Request
52	3.510458	52.35.96.64	192.168.2.44	TLSv1.2	109	Change Cipher Spec, Hello Request, Hello Request
54	3.700173	192.168.2.44	52.35.96.64	TLSv1.2	167	Application Data
55	3.800286	52.35.96.64	192.168.2.44	TLSv1.2	1016	Application Data, Application Data
60	3.926589	40.97.162.146	192.168.2.44	TLSv1.2	139	Application Data
61	3.926590	40.97.162.146	192.168.2.44	TLSv1.2	1195	Application Data

```
> Frame 45: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_e8:7b:62 (18:d6:c7:e8:7b:62), Dst: BeijingI_09:a4:d1 (00:18:05:09:a4:d1)
> Internet Protocol Version 4, Src: 192.168.2.44, Dst: 52.35.96.64
> Transmission Control Protocol, Src Port: 56590, Dst Port: 8443, Seq: 1, Ack: 1, Len: 78
> Secure Sockets Layer
```

Figure 20 - TLS Handshake

The screen capture in Figure 21 shows the Client Hello packet in detail.

- Note that the client sets the Session ID to 0 to start a new session with new ephemeral keys.
- Note that the client offers to use the IEEE 2030.5 cipher suite.



Real-90-https.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...

```
No.  Time      Source          Destination     Protocol  Length  Info
  45 2.950604  192.168.2.44    52.35.96.64     TLSv1.2    144 Client Hello
  47 3.096094  52.35.96.64     192.168.2.44    TLSv1.2   1258 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
  49 3.300376  40.97.134.34    192.168.2.44    TLSv1.2    139 Application Data
  51 3.321945  192.168.2.44    52.35.96.64     TLSv1.2    686 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Hello Request, Hello Request

> Frame 45: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_e8:7b:62 (18:d6:c7:e8:7b:62), Dst: BeijingI_09:a4:d1 (00:18:05:09:a4:d1)
> Internet Protocol Version 4, Src: 192.168.2.44, Dst: 52.35.96.64
> Transmission Control Protocol, Src Port: 56590, Dst Port: 8443, Seq: 1, Ack: 1, Len: 78
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 73
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 69
        Version: TLS 1.2 (0x0303)
      > Random
        Session ID Length: 0
        Cipher Suites Length: 6
      v Cipher Suites (3 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 22
      > Extension: elliptic_curves
      > Extension: ec_point_formats
      > Extension: signature_algorithms
```

This is a **Client Hello** message

TLS version **1.2** is used

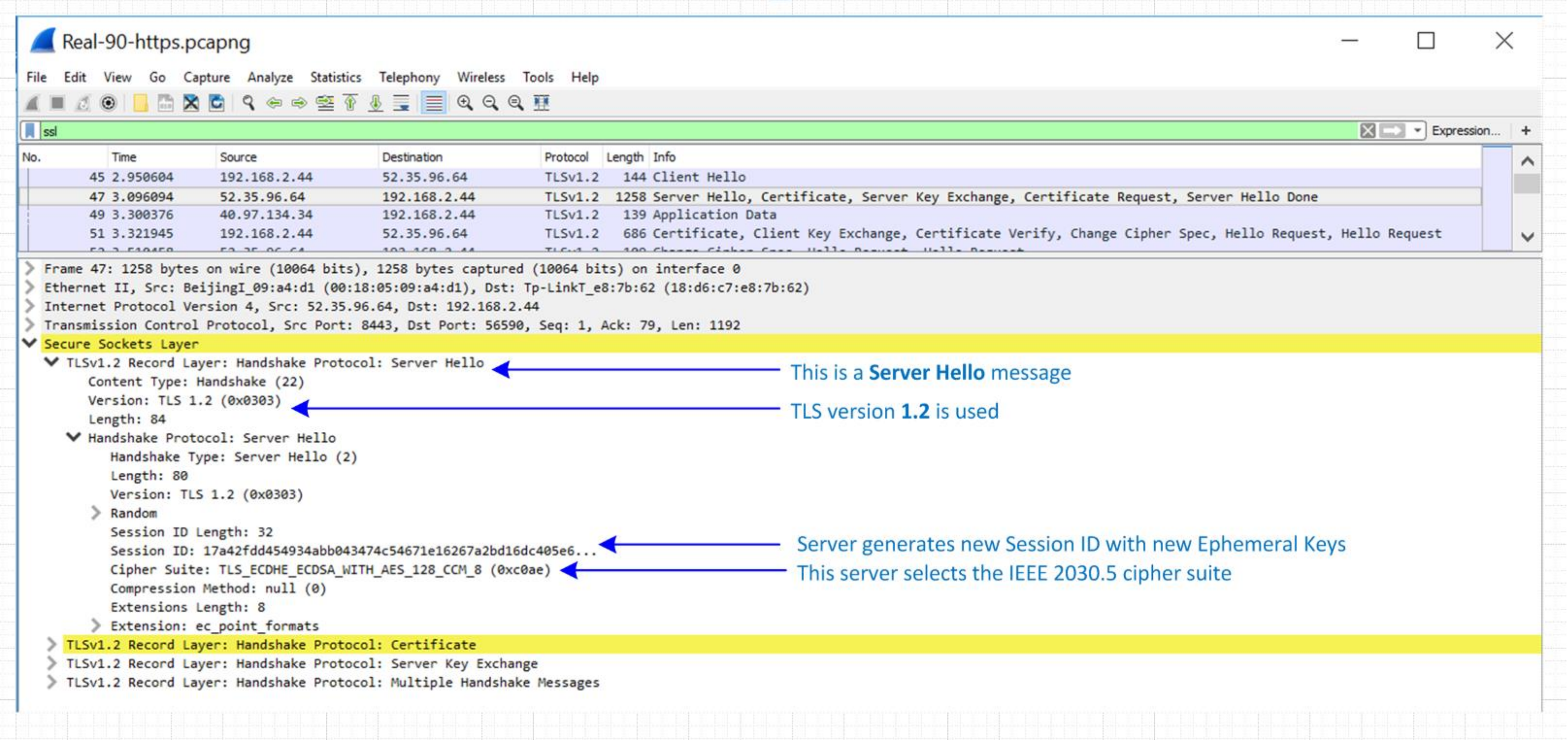
This tells the server to start a new Session with new Ephemeral Keys

This is the IEEE 2030.5 cipher suite

Figure 21 - TLS Client Hello

The screen capture in Figure 22 shows the Server Hello packet in detail.

- Note that the server sets the Session ID to a new random value to start a new session with new keys.
- Note that the server selects the IEEE 2030.5 cipher suite for this session.


Real-90-https.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...
+

```
No.  Time        Source          Destination     Protocol  Length  Info
  45 2.950604    192.168.2.44    52.35.96.64     TLSv1.2    144  Client Hello
  47 3.096094    52.35.96.64     192.168.2.44    TLSv1.2   1258  Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
  49 3.300376    40.97.134.34    192.168.2.44    TLSv1.2    139  Application Data
  51 3.321945    192.168.2.44    52.35.96.64     TLSv1.2    686  Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Hello Request, Hello Request
```

```
> Frame 47: 1258 bytes on wire (10064 bits), 1258 bytes captured (10064 bits) on interface 0
> Ethernet II, Src: BeijingI_09:a4:d1 (00:18:05:09:a4:d1), Dst: Tp-LinkT_e8:7b:62 (18:d6:c7:e8:7b:62)
> Internet Protocol Version 4, Src: 52.35.96.64, Dst: 192.168.2.44
> Transmission Control Protocol, Src Port: 8443, Dst Port: 56590, Seq: 1, Ack: 79, Len: 1192
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 84
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 80
        Version: TLS 1.2 (0x0303)
      > Random
        Session ID Length: 32
        Session ID: 17a42fdd454934abb043474c54671e16267a2bd16dc405e6...
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)
        Compression Method: null (0)
        Extensions Length: 8
      > Extension: ec_point_formats
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
  > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  > TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
```

This is a **Server Hello** message

TLS version **1.2** is used

Server generates new Session ID with new Ephemeral Keys

This server selects the IEEE 2030.5 cipher suite

Figure 22 - TLS Server Hello

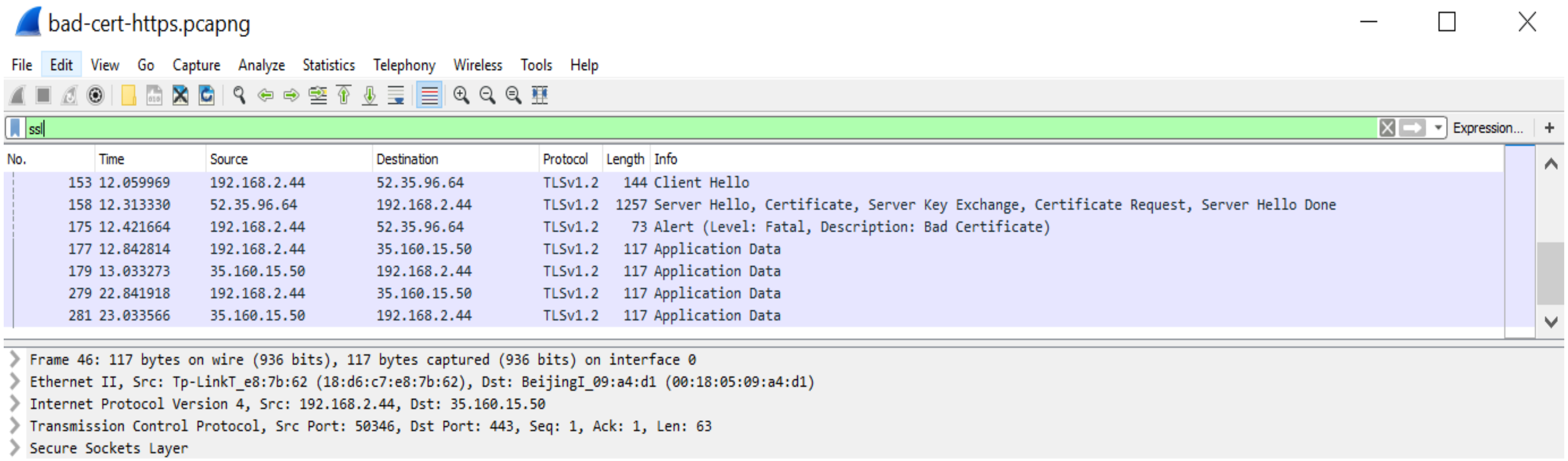
3.5.4 Bad TLS Handshake

This test verifies a bad certificate causes the TLS session to abort

1. Configure the DER client to use encrypted HTTPS to capture the TLS transactions. The TLS port is 8443.
2. Configure the DER client to use a certificate that chains to a different root CA than the server. The client will reject the Server’s certificate during the TLS handshake.
3. Start the Ethernet sniffer trace. The TLS port is 8443, so use this as an Ethernet sniffer filter.
4. Start the DER client.
5. Schedule a real power output control for 2 minutes.
6. Wait 3 minutes.
7. Stop the DER client.
8. Stop the Ethernet sniffer trace.

3.5.5 Results

The full trace is captured in the Ethernet sniffer file: “bad-cert-https.pcapng”. The screen capture in Figure 23 shows the TLS handshake between the client and server. Note that after receiving the Server’s certificate, the client issues a “TLS Alert” indicating it has received a Bad Certificate.



bad-cert-https.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...

```
No.   Time         Source          Destination     Protocol  Length Info
  153 12.059969    192.168.2.44    52.35.96.64     TLSv1.2    144 Client Hello
  158 12.313330    52.35.96.64     192.168.2.44    TLSv1.2   1257 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
  175 12.421664    192.168.2.44    52.35.96.64     TLSv1.2     73 Alert (Level: Fatal, Description: Bad Certificate)
  177 12.842814    192.168.2.44    35.160.15.50    TLSv1.2    117 Application Data
  179 13.033273    35.160.15.50    192.168.2.44    TLSv1.2    117 Application Data
  279 22.841918    192.168.2.44    35.160.15.50    TLSv1.2    117 Application Data
  281 23.033566    35.160.15.50    192.168.2.44    TLSv1.2    117 Application Data
```

```
> Frame 46: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_e8:7b:62 (18:d6:c7:e8:7b:62), Dst: BeijingI_09:a4:d1 (00:18:05:09:a4:d1)
> Internet Protocol Version 4, Src: 192.168.2.44, Dst: 35.160.15.50
> Transmission Control Protocol, Src Port: 50346, Dst Port: 443, Seq: 1, Ack: 1, Len: 63
> Secure Sockets Layer
```

Figure 23 - TLS Bad Certificate

4.0 Conclusions and Recommendations

4.1 Conclusions

Following statements are concluded from different tests cases performed in this effort:

4.1.1 Test #1 – Registration

In this effort, correct registration of the DER device to the IEEE 2030.5 server, from both the client-side and the server-side, was demonstrated. Furthermore, successful client-side registration was verified by providing the DER device with the correct registration PIN. The DER device matched the PIN and continued with normal operation.

Server-side registration is the process where the server authenticates the DER device's certificate during a TLS exchange and authorizes the DER device to find and act upon the DER controls (control commands). Successful server-side registration is implicitly verified by the fact that the DER device was able to receive the DER controls and act upon them. Test case #7 (cybersecurity) provided a negative test for server-side registration. In this test, the DER device provided a bad certificate and the server successfully detected it and terminated the TLS session, thus denying access to the unauthenticated device.

4.1.2 Test #2 – Monitor of the Output of the DER System

The correct reporting of real and reactive output power of the DER System was verified prior to a DER control, during the DER control, and after the DER control for Test #3, Test #4, and Test #5. No issues were found using IEEE 2030.5 for monitoring.

4.1.3 Test #3 – Issue Control Commands, Test #4 Issue Set-Point Update

IEEE 2030.5 does not make any distinction between a control command and a set-point update – they are both DER controls. The correct operation of the fixed-power-factor and volt-VAr DER controls was verified. No issues were found using IEEE 2030.5 for these controls.

4.1.4 Test #5 – Issue Activation and Deactivation

Neither IEEE 2030.5 nor Phase 1 (SWIG) has an "Activation/Deactivation" command. Instead, the real output power control was used to achieve the same functionality. The correct operation of the real power output control was verified. No issues were found using IEEE 2030.5 for this control.

4.1.5 Test #7 – Cybersecurity

IEEE 2030.5 communications is secured using the *TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8* cipher suite. The cipher suite provides end-to-end security between the IEEE 2030.5 server and the DER protocol translator. The Ethernet packet sniffer was utilized to verify the TLS handshake in normal operation. The Ethernet packet sniffer was used to verify that the TLS session generated a TLS alert when the DER protocol translator used an invalid certificate.

4.1.6 Learning from Success

The pre-commercial demonstration showed that IEEE 2030.5 can successfully send Phase 1 DER controls to DER devices and successfully monitor their output.

4.2 Recommendations

The objective of EPIC-1, Project 4, Demonstration of Grid Support Functions of Distributed Energy Resources (DER) was to demonstrate grid support functions of DER, which can improve distribution system operations. The chosen project modules quantified the value of specific grid support functions in specific application situations and provided a basis for SDG&E to determine which functions it wants to pursue commercially in advanced distribution system automation. This project module addressed pre-commercial demonstration of communication standards for grid support functions of DER. Recommendations for future commercial adoption are described in the following:

4.2.1 Evaluation of the IEEE 2030.5 Protocol

This pre-commercial demonstration proved that the IEEE 2030.5 protocol can successfully communicate Phase 1 functions. Thus, it is highly probable that it will be able to communicate Phase 3 functions, once those functions have been finalized.

At this time, the SIWG has agreed that the Phase 3 functions will be specified in the IEEE 1547 standards update. In conjunction, the IEEE 2030.5 standard is also being revised an updated to support all IEEE 1547, and therefore, all Phase 3 functions. When complete, CA Rule 21, IEEE 1547, and IEEE 2030.5 will be harmonized.

In parallel, the CSIP Implementation Guide version 2 is being revised to conform with the updated standards. The CSPI Implementation Guide is a document commissioned by the California IOUs that describes how to use the IEEE 2030.5 protocol to provide interoperable CA Rule 21 grid support functions. Version 1 of the CSIP Implementation Guide, based on the IEEE 2030.5-2013 was published in August 2016. Version 2 is expected in early 2018.

Also, in parallel, the CSIP Conformance Test Procedure document as well as a certification program is being developed to allow for certification of devices conforming to CSIP and IEEE 2030.5 specification. When complete, this certification program will insure the proper operation an interoperability of certified devices.

By early 2018, it is expected that the IEEE 2030.5 protocol will have:

1. A comprehensive specification supporting all IEEE 2030.5 and CA Rule 21 functions
2. An implementation guide explaining how to use IEEE 2030.5 for grid support services to promote interoperability across utilities
3. A test and certification process for validating functionality and interoperability

Although CA Rule 21 specifies IEEE 2030.5 as the default communications protocol, it does not preclude the use of other protocols. For example, DNP3 is being evaluated for real-time grid support applications. However, any proposed protocol, must provide support for the three criteria listed above. In the foreseeable future, IEEE 2030.5 is the only protocol that fully supports the three criteria.

4.2.2 Recommendations Associated with the IEEE 2030.5 Protocol

Some recommendations for future steps are:

1. At this time, this pre-commercial demonstration could only test a subset of the CA Rule 21 Phase 1 functions. When the standard updates have been completed, perform similar tests on all Phase 1 and Phase 3 functions.
2. For this pre-commercial demonstration, a single DER device was used. The performance of the IEEE 2030.5 protocol was not tested with a multitude of DER devices, so estimates on how the protocol would behave at production scale could not be determined. Lab tests with simulated devices or a field test with real devices would be useful in estimated performance at production scale.
3. As CA Rule 21 does not preclude the use of other protocols, and as the CA Rule 21 standard or international standards change from time to time, the successful performance of the intended functions for the new protocols should be re-demonstrated for certification by a qualified organization to validate the suitability of the new standard each time. This validation process should verify that the updated IEEE 2030.5 protocol (or any other alternative that may be adopted in CA Rule 21 or international standards) could successfully transport all Phase 1 and Phase 3 functions.

4.2.3 Evaluation of IEEE 2030.5 Security in Production

IEEE 2030.5 uses a powerful TLS cipher suite providing NSA SECRET level security. Normally, more security is desirable, but this TLS cipher suite uses ephemeral keys (which provides for perfect forward secrecy but may not play well with existing firewalls and packet inspection tools). In many utility IT environments, inbound packets from the internet are required to be decrypted and inspected by a Web Application Firewall (WAF). The WAF normally has a copy of the server's static private key so that it can decrypt and inspect the inbound packets. With the use of ephemeral keys, the WAF can no longer decrypt the packet thus making the WAF useless.

For the reasons listed above, it is possible that a utility's information technology (IT) policy precludes the use of the IEEE 2030.5 TLS cipher suite. In the upcoming revision of the CSIP implementation guide, provisions are being made to allow for the use of a less secure but WAF-friendly cipher suite. When defined, this WAF-friendly cipher suite needs to be tested for cyber security vulnerabilities.

Another cybersecurity consideration is the end points of the TLS connection. In this pre-commercial demonstration, the end points were the IEEE 2030.5 server and the DER protocol translator. The IEEE 2030.5 server exists on the internet and the DER protocol translator was located deep inside the utility lab. In a production environment, IT policy may require TLS connections to terminate at a demilitarized-zone (DMZ) at the edge of the utility network. If this is the case, there is a need for a proxy-like device to terminate the TLS connection in the DMZ and create a new TLS connection from the proxy to the DER protocol translator. If there are multiple security zones, the use of proxies and firewalls may need to be repeated.

4.2.4 Recommendations Associated with Security

In general, designing for security is very sophisticated topic to address. Many factors come into play from the cipher suite used, to compatibility with existing equipment, to IT security policies. There is no one size fits all, and the proper security architecture may be site dependent. Providing general recommendations is difficult, but some recommendations for future steps are:

1. If an alternate cipher suite is required because of IT policy, re-evaluate the overall security of the entire system.
2. If the use of a TLS proxy is required because of IT policy, test the overall system performance as adding a proxy will necessarily increase the latency of the system.

4.2.5 Evaluation of DER Device Interoperability

The DER device in this pre-commercial demonstration used a proprietary Modbus register map for control and status. For single-device testing, this is acceptable, but for large-scale multi-vendor commercial deployments, the DER protocol translator cannot be expected to have to communicate with an unbounded number of proprietary DER device control protocols. Instead, DER devices should all conform to a single, standardized, control protocol (e.g., Modbus), and an open and standardized information model (e.g., SunSpec Alliance Models).

4.2.6 Recommendations Associated with DER Device Interoperability

1. Promote the standardization of a common DER device control mechanism. The SunSpec Alliance's DER Models appears the most suitable, but there may be others.
2. For large-scale deployments (i.e., utility scale), it is recommended that all DER devices implement a standardized DER Modbus model.

5.0 Technology Transfer Plan

A primary benefit of the EPIC program is the technology and knowledge sharing that occurs both internally within SDG&E and across the industry. To facilitate this knowledge sharing, SDG&E will share the results of this project by widely announcing the availability of this report to industry stakeholders on its EPIC website, by submitting papers to technical journals and conferences, and by presentations in EPIC and other industry workshops and forums. Additionally, presentations will be given to internal stakeholders at SDG&E.

6.0 Metrics and Value Proposition

6.1 Metrics

The following metrics (discussed in Table 1) were identified for this project as potential project benefits at larger scale deployment. Given the pre-commercial nature of this EPIC project, these metrics would apply in future scenarios after widespread commercial adoption. The following statements are potential benefits that are concluded from different tests cases performed in this effort:

Table 1. EPIC metrics for pre-commercial demonstration of communications performance of the IEEE 2030.5 protocol

D.13-11-025, Attachment 4. List of Proposed Metrics and Potential Areas of Measurement (as applicable to a specific project or investment area in applied research, technology demonstration, and market facilitation)
1. Potential energy and cost savings
b. Total electricity deliveries from grid-connected distributed generation facilities
e. Peak load reduction (MW) from summer and winter programs
f. Avoided customer energy use (kWh saved)
g. Percentage of demand response enabled by automated demand response technology (e.g. Auto DR)
3. Economic benefits
b. Maintain/reduce operations and maintenance costs
c. Reduction in electrical losses in the transmission and distribution system
5. Safety, power quality, and reliability (equipment, electricity system)
a. Outage number, frequency, and duration reductions
b. Electric system power flow congestion reduction
7. Identification of barriers or issues resolved that prevented widespread deployment of technology or strategy
b. Increased use of cost-effective digital information and control technology to improve reliability, security, and efficiency of the electric grid (PU Code § 8360)
c. Dynamic optimization of grid operations and resources, including appropriate consideration for asset management and utilization of related grid operations and resources, with cost-effective full cyber security (PU Code § 8360)
d. Deployment and integration of cost-effective distributed resources and generation, including renewable resources (PU Code § 8360)

6.2 Value Proposition

The purpose of EPIC funding is to support investments in R&D projects that benefit the electricity customers of California IOUs. The primary principles of EPIC are to invest in technologies and approaches that promote greater reliability, lower costs, and increased safety. Table 2 represents the value that "pre-commercial demonstration of EPRI DRIVE DER hosting capacity" project provides to the overall system operation. Primary and secondary benefits are presented wherever applicable to demonstrate the value of the function for commercial adoptability.

As it is shown in Table 2 and was discussed in the result and conclusion section of this report, pre-commercial demonstration of communications performance of the IEEE 2030.5 protocol primarily can enhance systems reliability by enabling dynamic optimization of grid operations and resources. Furthermore, this could be utilized by appropriate consideration for asset management and utilization of related grid operations and resources, with cost-effective full cyber security. Additionally, it can contribute to optimized and cost-effective integration of DER to distribution system.

Table 2. Value proposition (primary and secondary) for pre-commercial demonstration of EPRI DRIVE DER hosting capacity tool

Primary Principals			Secondary Principals					
Reliability	Affordability	Safety	Societal Benefits	GHG Emissions Mitigation / Adaptation	Loading Order	Low-Emission Vehicles / Transportation	Economic Development	Efficient Use of Ratepayers Monies
X								X

7.0 References

[1] IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard," in IEEE Std 2030.5-2013, vol., no., pp.1-348, Nov. 11 2013.

[2] IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems," in IEEE Std 1547-2003, vol., no., pp.1-28, July 28 2003.

[3] IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters, California Smart Inverter Implementation Working Group, August 31, 2016.