Pacific Gas and Electric Company

EPIC Final Draft Report

Program	***Electric Program Investment Charge (EPIC)***
Project	***EPIC 2.26 Customer and Distribution Automation Open Architecture Devices***
Reference Name	***EPIC 2.26 – Cust-Dist Automation Devices***
Department	*Metering Services and Engineering*
Project Sponsor	Earle Davis
Project Business Lead	Young Nguyen
Contact Info	EPIC_Info@pge.com
Date	February 19, 2019
Version Type	
Version	Final Report

Table of Contents

List of Tables

List of Figures

Table of Acronyms (Alphabetized)

AMI	Advanced Metering Infrastructure
AP	Access Point
API	Application Programming Interface
ATS	Applied Technology Services
AWS	Amazon Web Services
CEC	California Energy Commission
CPUC	California Public Utilities Commission
D.	Decision
DER	Distributed Energy Resource
DER Class	Distributed Energy Resource Class is defined by Size and Grid Voltage Level (Transmission 60 kV and above. Distribution below 60 kV) as follows: Class 1: DER at 1 MW and above on Distribution Grid Class 2: DER under 1 MW on Distribution Grid Class 3: DER at 1 MW and above on Transmission Grid Class 4: DER under 1 MW on Transmission Grid
DG	Distributed Generation
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol
EPIC	Electric Program Investment Charge
EXI	Efficient XML Interchange
FAN	Field Area Network
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IED	Intelligent Energy Devices
IEEE	Institute of Electrical and Electronics Engineer
IEEE 2030.5	Client-Server protocol developed for management of Smart Energy devices.
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
kW	Kilowatt
LLRP	Low-Level Reader Protocol
MW	Megawatt
ODN	Operations Data Network
OTA	Over-the-Air
PG&E	Pacific Gas and Electric Company
PV	Photovoltaic

RF	Radio Frequency
RFID	Radio Frequency Identification
RT SCADA	Real-time SCADA
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison Company
SDG&E	San Diego Gas & Electric Company
SLO	San Luis Obispo
SSH	Secure Shell
TD&D	Technology Demonstration and Deployment
UDN	User Data Network
UI	User Interface
VAR	Volt Ampere Reactive
VPC	Virtual Private Cloud
VPG	Vitual Private Network Gateway
VPN	Virtual Private Network
XML	Extensible Markup Language

1. Executive Summary

Pacific Gas and Electric Company's (PG&E) Electric Advanced Metering Infrastructure (AMI) Network, which was designed for customer billing applications, is one of the largest private Internet Protocol Version 6[1] (IPv6) networks in the Unites States, covering 99.5% of its 70,000 square mile service territory. While the network is successfully being used for customer billing purposes, it is also delivering substantial benefits to PG&E in other areas such as improved outage notification, faster restoration following outages, and power theft identification. An evaluation conducted in 2016 determined the current set of AMI operations accounted for only 15-20 percent[2] of the available bandwidth and additional data could be routed without impacting current operations.

The objective of this demonstration was to investigate the use of the AMI network for purposes beyond the collection of electricity usage data, such as, control of Distributed Energy Resources (DER), monitoring of sensors and Radio Frequency Identification (RFID) tags, and Supervisory Control and Data Acquisition (SCADA) communication and control. The key issue investigated was whether the command and control of the end devices would be successful, meaning that devices and applications are AMI compatible, highly secured, interoperable, and meet all PG&E requirements with regards to speed and latency.

Project Objectives

The key objective of this project was to demonstrate the capability of using the AMI network as a communication medium for diverse, non-AMI use cases involving a variety of end devices. The project objectives were as follows:

- Identify and/or develop methodologies, protocols and standards for customers and vendors to connect with the AMI network;
- Conduct testing that will certify that PG&E, customer and 3rd Party open architecture devices and applications are AMI compatible, highly secured, interoperable, and meet all PG&E requirements;
- Prove PG&E can communicate with and control the devices remotely over the AMI network; and
- Ensure that the solution is scalable and meets cybersecurity standards.

Project Scope and Tasks

The scope of work for this project included tasks that support the development of the Client-Server[3] platform using AMI as the interconnection medium and the Institute of Electrical and Electronics

[1] IPv6 is the most recent version of the IP, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

[2] PG&E EPIC-1.14, *Next Generation SmartMeter^{TM} Telecom Network Functionalities* Final Report, Nov. 30, 2016 p.9.

[3] Client/Server architecture is a computing model in which the Server hosts, delivers and manages most of the resources and services to be consumed by the Client. This type of architecture has one or more Client computers connected to a central Server over a network or internet connection.

Engineers (IEEE) 2030.5[4] protocol for communication between the Client and the Server, as well as lab and field testing of the access device for specific use applications. To meet the scope mentioned above, the project consisted of the following tasks:

- **Task 1: Develop Solution Architecture:** Develop a solution architecture that defined hardware, software, communications medium, and end-to-end communication protocols for each use case in both the lab and field testing environments.
- **Task 2: Develop Solution Software:** Develop the EPIC 2.26 Client and Server software and the IEEE 2030.5 interface that allows for maximum control of data flow over the AMI network.
- **Task 3: Perform Lab Testing:** Perform lab testing to prove the feasibility as well as performance of each use case. The lab testing solution architecture developed in Task 1 was used in this Task.
- **Task 4: Perform Field Testing:** Perform field testing to prove the feasibility as well as performance of select use cases. The field testing solution architecture developed in Task 1 was used in this Task.

Selection of Use Cases

Five use cases were developed for lab and/or field testing to prove the feasibility as well as performance of the Client-Server architecture for various applications. The total seven use cases were selected because of their potential to improve system reliability, reduce utility costs or both and were prioritized based on the needs of PG&E and the industry, of which two use cases did not move forward. Use Case 1 – Electric Smart Meters that was aimed to test the meter firmware download capability Over-the-Air (OTA) along with other new functions was stopped because of the SmartMeter™ technology limitation with no possible solutions (See Section 3.4.1. Identification of use cases and Section 3.4.2. Prioritization of use cases). Use Case 4 – Smart Thermostat had lower priority, as it was found to be deployed using customer's Wi-Fi technology, which presents cybersecurity issues, and was not pursued for lab or field testing (See Section 3.4.1. Identification of use cases and Section 3.4.2. Prioritization of use cases). The following final five use cases were tested and demonstrated.

- ***Use Case #2 – Solar Smart Inverter:*** Demonstration of the use of PG&E's AMI network to communicate with and control solar smart inverters. This use case was selected because of its potential to improve system reliability and was tested in both lab and field environments.
- ***Use Case #3 – Sensors:*** Demonstration of the use of PG&E's AMI network to communicate with seismic sensors located in PG&E's system. This use case was selected because of its potential to provide visibility into electric grids and improve system reliability. It was tested in the lab environment only.
- ***Use Case #5 – Distribution Automation/SCADA Overhead and Underground Intelligent Electric Devices (IED):*** Demonstration of the use of PG&E's AMI network to communicate with, control, transmit data of, and upgrade firmware over-the air onto overhead and underground devices in PG&E's system. This use case was selected because of its potential to improve system reliability and was tested in the lab environment.

[4] IEEE 2030.5 is the internationally adopted standard for providing encrypted smart grid communications from energy management systems to end users and devices.

- ***Use Case #6 – Radio Frequency Identification Tags (RFID tags) Over AMI Network:*** Demonstration of the use of PG&E's AMI network to communicate with RFID equipment (readers and taggers) over the network. This use case was selected because of its potential to reduce costs and was tested in both lab and field environments.
- ***Use Case #7 – Direct Acquisition and Control Telemetry Solution:*** Demonstration of a direct acquisition and control telemetry solution using PG&E's AMI network for medium-sized energy generation projects under 1 Megawatt (MW) (i.e., 200 Kilowatt (kW)). This use case was selected because of its potential to reduce costs and was tested in both lab and field environments. While Use Case #5 monitors and controls SCADA devices, Use Case #7 monitors and controls Distributed Generation (DG) equipment, even if both SCADA device and DG equipment are at the same location of customer.

Project Activities, Results and Findings

The project was performed under four key tasks mentioned previously. These were:

- **Task 1: Develop Solution Architecture:** The first task was to develop a solution architecture that defined hardware, software, communications medium, and end-to-end communication protocols for each use case in both the lab and field testing environments. The architecture developed under this project comprised of a Client-Server application that enabled secure communication between the operator and the end devices over the AMI network. A key component of this architecture was the Internet of Things (IoT) router that served as the Client. The IoT router is a low-cost edge device with computing power and capacity that will facilitate the integration of DER devices. These DER devices can now interconnect to the grid using the AMI network as long as the DER device can respond to command instructions, allow remote monitoring via an Ethernet or USB ports. The IEEE 2030.5 standard data model was used for communications between the Client and the Server. After considering several options for testing the architecture in a lab setting, PG&E chose the "On-premises" model for the lab tests using the PG&E San Ramon Applied Technology Services (ATS) lab since this provided a secure and controlled test environment that was easy to set up. For the field tests, PG&E elected to install the EPIC Server on the Virtual Private Cloud (VPC).
- **Task 2: Develop Solution Software:** A core piece of this project was the development of the Client-Server software for communication between the Server and the end devices. Under this task, both the Server and Client were developed as web services using Java to maximize the use of open source frameworks and libraries. The Server contains the Graphical User Interfaces (GUI) that the operators use for communicating with the end devices, as well as the IEEE 2030.5 interface for transmitting the information over the AMI network using IEEE 2030.5 specification model elements and processes. The Server software was designed for and deployed on a virtual machine running a Linux-based operating system. The Client was deployed on IoT Routers that were designed to support multiple end devices. In addition to the Client-Server software, protocol adapters required for communicating with the end devices were also developed in this project.
- **Task 3: Perform Lab Testing:** Under this task, lab tests were performed to evaluate the performance of the five use cases described earlier. High-level connectivity tests were first performed to test the performance of the connection between the Server and the IoT router. Use-case specific tests were also performed to test the capability and performance of specific functions in each use case. Lab test results proved the feasibility of using an IoT router to

command and control various third-party end devices such as smart inverters, sensors, SCADA devices, RFID readers and DG controls over the AMI network using the IEEE 2030.5 protocol.

- **Task 4: Perform Field Testing:** Under this task, field tests were performed to evaluate the performance of three use cases (use case #2, 6 and 7). Field test were performed with the Server installed on PG&E's VPC that communicated with the IoT router on a non-production AMI with a single-hop connection between the router and the Access Point (AP). Test results showed that throughput and latency requirements of the use cases could be met. Field test results successfully demonstrated the ability of a Client-Server architecture consisting on an IoT router to establish communication, command and control of various third-party end devices such as smart inverters, sensors, SCADA devices, RFID readers and DG controls over the AMI network using the IEEE 2030.5 protocol.
- **Cybersecurity Assessment:** Cybersecurity penetration tests were performed to identify potential risks and mitigation strategies at the product-level, as well as the site-level. These tests showed the need for properly hardened infrastructure leveraging secure-boot functionality, device encryption and a strong password complexity policy. Gap in cybersecurity between systems was hardened and completed.
- **Network Performance Assessment:** Network performance performed by PG&E showed that the latency and other performance requirements of the use cases could be met in a single-hop environment.
- **Recommendations for the Lab and Field Tests:** Several recommendations for improving the Client-Server architecture and associated software and cybersecurity performance were developed based on the lab and field tests. In addition to the general recommendations, specific use case-related recommendations were also developed to improve the performance of each use case.
- **Next Steps:** Based on the test findings and recommendations, the key next steps that PG&E may explore include:
    - Performing Network Tests in a Production Environment – Test the performance of the client-server architecture in a production environment for applicable use cases. Measure latency, packet loss, throughput and reliability and compare with the use case requirements.
    - Production Evaluation for Use Case #6 – Develop a production project for use case #6 after performing additional field tests using number of yards to refine the to be process, develop lessons-learned, and understand how to use the data being generated for long term operational benefits.
    - Disseminate Demonstration Findings – Disseminate the finding of the EPIC 2.26 Demonstration in relevant regulatory proceedings, industry engagement meetings and conferences.

Accomplishments and Recommendations

The key accomplishments of this project are as follows:

- Developed the solution architecture that defined the hardware, software, communications equipment, communication standards and protocols for secure control of various end devices using the AMI infrastructure;
    - Successfully integrated IPv6 traffic through the AMI Network and into the PGE Amazon Web Services (AWS). This was a first in handling IPv6 within PG&E.
    - Successfully hardened Cybersecurity issue between systems from PG&E cloud to headend server.
    - Successfully integrated data traffic between the AWS Cloud and distribution SCADA and SCADA -Master, a first for PG&E.
- Developed the EPIC 2.26 Client and Server software and the IEEE 2030.5 interface that allows for maximum control of data flow over the AMI network.
- Successfully demonstrated in laboratory and field tests, the ability to communicate with, monitor, and control PG&E and third-party devices in five use cases. These use cases involved Smart Inverters, sensors, SCADA and other distribution IEDs, RFID equipment and Direct Acquisition and Control Telemetry.

Intellectual Property

This project was successful in demonstrating that PG&E's AMI network can be leveraged for these additional use cases and is suitable for connecting and transmitting data from customer and utility devices. The key to transitioning the EPIC 2.26 project from demonstration to production scale will be operational readiness, further definition of maintenance and operations work, and budget funding for each use case. Other utilities seeking to explore similar work will also need to consider this prioritization, as while this project proved these use cases can be feasible, how it is used needs to be prioritized just like any other Radio Frequency (RF) networks.

PG&E looks forward to working with the other California utilities, and the industry at large, to realize the benefits of this approach. This intellectual property is owned and held by PG&E, and can be commercialized for the company's and customer's benefit, in accordance with all appropriate laws and regulations (including Decision (D.) 13-11.025).

Conclusions

The EPIC 2.26, *Customer and Distribution Automation Open Architecture Devices* project successfully developed a cloud-based Client-Server architecture using the IEEE 2030.5 protocol, APIs for the command and control of various end devices and protocol adapters to communicate with a multitude of end devices. Lab tests for five use cases and field tests for three use cases were also successfully completed. PG&E was able to successfully connect to, monitor, communicate with, and control these devices during the use case evaluations.

Cybersecurity penetration tests showed the need for properly hardened infrastructure leveraging secure-boot functionality, device encryption and a strong password complexity policy, which needs an upgrade and hardening of the IoT-Router software, before moving to a production environment. The cybersecurity for the systems between PG&E cloud and headend server was hardened and resolved, which is using IPsec VPN over PG&E Data pipe to replace IPsec VPN over internet.

The latency requirements for DER telemetry and SCADA use cases can be met with a single hop by designing the AMI network and having a few endpoints transmit data directly through a network node, as described further in the following bullets:

- DER telemetry: Depending on the Distributed Energy Resource Class (DER Class) (see Table of Acronyms), various latency requirements can be determined and applied (e.g., slower latency for DER Class 2), and the AMI network design can be done accordingly.
- SCADA Use: SCADA over AMI solution can potentially be a complementary solution to SCADA in areas that other SCADA solutions are not available.

The AMI network has additional bandwidth available and can be used for other purposes beyond billing. The project demonstrated the possibility of installing or interconnecting devices to the AMI network and could ultimately reduce equipment installation costs. Since the AMI network coverage is 99.5% of PG&E’s service territory, it is seen as a reliable, lower cost network solution, specifically, network capital spending, maintenance operation spending, and especially telecommunications costs. The AMI mesh network has built in redundancy, and therefore may improve the ability to monitor field devices, identify problems or incidents more quickly and improve response time to events.

2. Introduction

This report documents the EPIC 2.26, *Customer and Distribution Automation Open Architecture Devices* project achievements, highlights key learnings from the project that have industry-wide value, and identifies future opportunities for PG&E to leverage this project.

The California Public Utilities Commission (CPUC) passed two decisions that established the basis for this demonstration program. The CPUC initially issued D.11-12-035, *Decision Establishing Interim Research, Development and Demonstrations and Renewables Program Funding Level,*[5] which established the EPIC on December 15, 2011. Subsequently, on May 24, 2012, the CPUC issued D.12-05-037, *Phase 2 Decision Establishing Purposes and Governance for Electric Program Investment Charge and Establishing Funding Collections for 2013-2020,*[6] which authorized funding in the areas of applied research and development, Technology Demonstration and Deployment (TD&D), and market facilitation. In this later decision, CPUC defined TD&D as "the installation and operation of pre-commercial technologies or strategies at a scale sufficiently large and in conditions sufficiently reflective of anticipated actual operating environments to enable appraisal of the operational and performance characteristics and the financial risks associated with a given technology."[7]

The decision also required the EPIC Program Administrators[8] to submit Triennial Investment Plans to cover three-year funding cycles for 2012-2014, 2015-2017, and 2018-2020. On November 1, 2012, in Application 12-11-003, PG&E filed its first triennial EPIC Application at the CPUC, requesting $49,328,000 including funding for 26 TD&D Projects. On November 14, 2013, in D.13-11-025, the CPUC approved PG&E's EPIC plan, including $49,328,000 for this program category. Pursuant to PG&E's approved EPIC triennial plan, PG&E initiated, planned and implemented the following project: EPIC 2.26*, Customer and Distribution Automation Open Architecture Devices*. Through the annual reporting process, PG&E kept CPUC staff and stakeholder informed on the progress of the project. The following is PG&E's final report on this project.

[5] http://docs.cpuc.ca.gov/PublishedDocs/WORD_PDF/FINAL_DECISION/156050.PDF.

[6] http://docs.cpuc.ca.gov/PublishedDocs/WORD_PDF/FINAL_DECISION/167664.PDF.

[7] D.12-05-037, p. 37.

[8] PG&E, San Diego Gas & Electric Company (SDG&E), Southern California Edison Company (SCE), and the California Energy Commission (CEC).

3. Project Summary

PG&E has invested over $2 billion in a robust AMI network for its electric and gas systems. PG&E's AMI Network is one of the largest private IPv6[9] networks in the Unites States, with more than 5 million AMI devices connected across its electric network. While the network is successfully being used for customer billing purposes, it is also delivering substantial benefits to PG&E in other areas such as meter-reading savings, improved outage notification, faster restoration following outages and power theft identification. Currently, the AMI network is being used exclusively for meeting PG&E's billing needs. However, it was designed and built to accommodate future non-billing applications by third parties once successfully demonstrated and funded.

There are some potential benefits to opening the AMI network to external, non-billing applications. These include:

- Affordability:
  - Enhance DER capabilities as a flexible grid and energy resource; and
  - Enable potential applications such as local load disaggregation for distribution modeling and load forecasting and manage various devices and DERs during outages or loss of communications.
- Reliability:
  - Provide greater visibility into third-party devices for demand response, and contribution to energy efficiency; and
  - Provide a reliable and highly secured communication network to third-party devices for DER, SCADA monitoring and control, and telemetry.

This project demonstrates the suitability of the PG&E AMI network for use as a Server-Client interconnection medium across a variety of use cases using a multitude of remote end devices. This effectively opens up the large, low-bandwidth, wireless network to both internal and external uses.

3.1. Issues Addressed

There are no projects underway at PG&E or other utilities that purport to be able to use the AMI network and its IPv6 protocol to command and control devices not provided by the AMI Network vendor. Other EPIC projects[10] that are investigating the use of the AMI network in new ways are using the network to obtain data already available in the meters in new and innovative ways. However, this project aims to use the AMI network for purposes beyond the collection of electricity usage data, such as, control of DERs, monitoring of sensors and RFIDs tags, and SCADA communication and control. As such, the use cases in this project cover performing proof of concept testing across a multitude of third party devices including consumer devices, PG&E-owned RFID device(s), PG&E-owned distribution-grid devices, and solar aggregator-managed/individually-managed devices that use various communication protocols. The key issue investigated is whether the command and control of the end devices is

[9] IPv6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

[10] EPIC 1.19 – Enhanced Data Techniques and Capabilities via the SmartMeter™ Platform, EPIC 1.21 – Auto Identification of Photovoltaic (PV) Resources, and EPIC 2.04 – Distributed Generation Monitoring and Voltage Tracking.

successful, meaning that devices and applications are AMI compatible, highly secured, interoperable, and meet all PG&E requirements with regards to speed and latency.

Another issue that this project initially aimed to address was the interoperability of the network platform by including two other Networks (Wi-Fi and Wi-SUN[11] Field Area Network (FAN)) in addition to AMI. However, this issue was not addressed through this project due to the lack of availability of the Wi-Fi and Wi-SUN FAN products during the timeframe of the project.

3.2. Project Objectives

The overall objective of EPIC 2.26, *Customer and Distribution Automation Open Architecture Devices,* was to evaluate whether PG&E can configure an access device or router that could serve as the on-ramp to the smart meter network for a relatively low cost. It was to test an open system architecture with defined methodology, protocols, and standards using the IPv6 AMI network and evaluate how to potentially allow customers and vendors to connect their devices and applications in a way that allows PG&E to communicate with and control them.

To accomplish this objective, the project aimed to:

- Identify and/or develop methodologies, protocols and standards for customers and vendors to connect with the AMI network;
- Conduct laboratory and field testing to confirm the devices are secure, interoperable and meet PG&E standards;
- Ensure PG&E can communicate and control the end devices remotely over the AMI network; and
- Ensure that the solution is scalable and meets cybersecurity standards.

3.3. Scope of Work and Project Tasks

The scope of work for this project included tasks that supported the development of the Client-Server[12] platform using AMI as the interconnection medium and the IEEE 2030.5[13] protocol for communication between the Client and the Server, as well as lab and field testing of the access devices for specific use applications. This included the testing of several use cases discussed in Section 3.4.

[11] Wi-SUN stands for Wireless Smart Utility Network, a secure mesh network promoted by Wi-SUN Alliance.

[12] Client/Server architecture is a computing model in which the Server hosts, delivers and manages most of the resources and services to be consumed by the Client. This type of architecture has one or more Client computers connected to a central Server over a network or internet connection.

[13] IEEE 2030.5 is the internationally adopted standard for providing encrypted smart grid communications from energy management systems to end users and devices.

3.3.1. Tasks and Milestones

To complete the Scope of Work for the project, the following tasks were developed:

Task 1: Develop Solution Architecture

Develop a solution architecture that defined hardware, software, communications medium, and end-to-end communication protocols for each use case in both the lab and field testing environments.

Task 2: Develop Solution Software

Develop the EPIC 2.26 Client and Server software and the IEEE 2030.5 interface that allows for maximum control of data flow over the AMI network.

Task 3: Perform Lab Testing

Perform lab testing to prove the feasibility as well as performance of each use case. The lab testing solution architecture developed in Task 1 was used in this Task.

Task 4: Perform Field Testing

Perform field testing to prove that the designed architecture and solution software will work in the field. The field testing solution architecture developed in Task 1 was used in this Task.

3.4. Key AMI-Leveraged Applications

As part of the proof of concept testing, various use cases covering a multitude of devices including third party consumer devices, PG&E-owned RFID device(s), PG&E-owned distribution-grid devices, and solar aggregator-managed/individually-managed devices were identified and tested in the lab and in some instances in the field. The use cases were identified and prioritized based on importance to PG&E's needs, as well as the needs of the industry.

3.4.1. Identification of Use Cases

Seven use cases were identified for this project. They were:

Use Case #1 – Electric Smart Meters

The purpose of this use case was to evaluate whether third party vendors could use the AMI network to diagnose electric meters, set/reset soft switches, perform/track software and firmware upgrades and other configuration changes on meters without PG&E dispatching a field meter technician. This ability could reduce PG&E electric meter operating costs by eliminating the firmware bugs OTA (remotely) and avoiding truck rolls.

Use Case #2 – Solar Smart Inverter and Behind-the-Meter Battery Storage

The purpose of this use case was to demonstrate the use of a third-party communication router to provide the ability to communicate with, transmit data of, control settings of, and upgrade firmware OTA onto solar smart inverters over the networks. The objective of the demonstration was to develop physical and application interfaces on PG&E Servers that will allow operators to remotely control the smart inverters and BTM battery storage using the PG&E AMI network. This use case supports the Rule 21 Working Group activities associated with control of roof top solar facilities. The ability to communicate with and control solar smart inverters would improve PG&E's ability to operate the electric system, regulate electric stability, and improve reliability.

Use Case #3 – Sensors

The purpose of this use case was to demonstrate the use of a third-party communication router to provide the ability to communicate with sensors (seismic sensors) over the AMI Network. The objective of the demonstration was to develop physical and application interfaces on PG&E Servers that will allow operators to communicate with these devices for command, control and data collection through the PG&E AMI Network. The ability to communicate with these types of sensors would result in public safety improvement and hazard exposure reduction.

Use Case #4 – Smart Thermostat

The purpose of this use case was to demonstrate the use of a third-party communication router to provide the ability to communicate with, control and transmit temperature data and relevant information of smart thermostats over the network, to provide reliability and visibility of third-party devices, provide relevant temperature data for grid operation and demand response, and support energy efficiency.

Use Case #5 – Distribution Automation /SCADA Overhead and Underground Intelligent Electric Devices (IED)

The purpose of this use case was to demonstrate the use of a third-party communication router to provide the ability to communicate with, control, transmit data of, and upgrade firmware over-the air onto overhead and underground devices over the Network. For this demonstration, PG&E chose its standard line recloser, controller, and underground switch controller. The objective of this demonstration was to develop physical and application interfaces on PG&E Servers that will allow operators to remotely communicate with and control overhead and underground SCADA using the PG&E AMI network. Because the AMI network covers 99.5% of the PG&E electric service territory (compared to 66 to 81% 4G coverage from the major telecom companies in California), having the ability to communicate and control electric equipment has the potential to cost-effectively improve electric system safety and reliability, especially in those areas that have no cell phone coverage.

Use Case #6 – Radio Frequency Identification Tags (RFID tags) Over AMI Network

The purpose of this use case is to demonstrate the use of a third-party communication router to provide the ability to communicate with RFID equipment (readers and taggers) over the network. The objective of this demonstration was to develop physical and application interfaces on PG&E Servers that will allow operators to interface and communicate with RFID Reader for interrogation and data collection using the PG&E AMI network. The ability communicate with RFID tags would improve the ability to initially manage PG&E meters and metering devices and in the long term, provide an option to manage PG&E's other assets.

Use Case #7 – Direct Acquisition and Control Telemetry Solution

The purpose of this use case was to demonstrate a Direct Acquisition and Control Telemetry solution with Enhanced Security and Cyber Isolation using the Network for medium-sized energy generation projects under 1 MW (i.e. 200 kW) and ultimately generation project sizes greater than 1 MW. The objective of this demonstration was to develop physical and application interfaces on PG&E Servers that will allow operators to communicate with DERs using the PG&E AMI network. The ability to use Telemetry via the AMI network would be a more cost-effective than PG&E's current methods. While Use Case #5 monitors and controls SCADA devices, Use Case #7 monitors and controls DG equipment, even if both the SCADA device and DG equipment are at the same location of customer.

3.4.2. Prioritization of Use Cases

The use cases were prioritized based on their potential impacts. Below is a summary of the prioritization.

- Use case #1 was not tested because the existing SmartMeter™ technology was limited to only certain configuration changes over the AMI network. Secondarily, the existing SmartMeters™ in the field were becoming obsolete and no longer needed the enhanced capability.
- Use case #2 was selected for lab and field testing because its potential to improve system reliability and was tested in both lab and field environments. Only the smart inverter was selected for testing.
- Use case #3 was selected because of its potential to improve system reliability but was tested in the lab environment only.
- Use case #4 was assigned a lower priority as the Smart Thermostat was found to be deployed using customer's Wi-Fi technology, which presents cybersecurity issues, and was not pursued for lab or field testing.
- Use case #5 was selected because of its potential to improve system reliability and was tested in the lab environment. However, the demonstration for use case #5 was limited to distribution SCADA devices. Originally, the demonstration of Fault location, isolation, and service restoration was also included in this use case.
- Use case #6 was selected because of its potential to reduce costs and was tested in both lab and field environments.
- Use case #7 was selected because of its potential to improve system reliability and was tested in both lab and field environments.

4. Project Activities, Results, and Findings

This section describes the four project tasks and associated results.

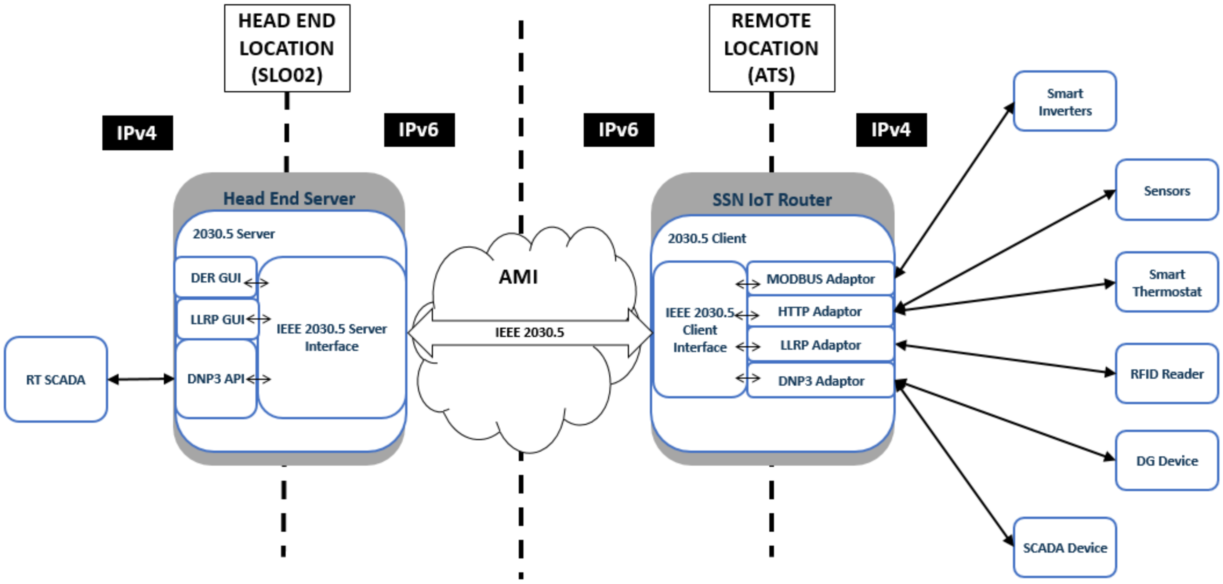
4.1. Task 1: Solution Architecture for Use Case Implementation

The first step in this project was to develop the overall solution architecture that defined hardware, software, communications medium, communication standards and protocols for secure control of various end devices using the AMI infrastructure. Information on the Client-Server architecture that was developed by PG&E for these use cases is provided in Section 4.1.1. The custom Client-Server software developed using the IEEE 2030.5 protocol for secure communication over the AMI network is described in Section 4.1.2. Detailed information on the specifics of the solution architecture developed for lab and field testing of use cases is provided in Sections 4.1.3 and 4.1.4 respectively.

4.1.1. High-Level Solution Architecture

A key step of this project was to develop the high-level solution architecture that leveraged PG&E's AMI infrastructure as a means for facilitating communication between various end devices. A high-level, functional network diagram for the solution architecture is shown in Figure 1.

Figure 1: High-Level, Functional Network Diagram



The architecture comprises of a Client-Server application that enables secure communication between the operator and the end devices over the AMI network. A key component of this architecture is the IoT router that serves as the Client hardware. The IoT router is an edge computing device with limited computing power and capacity that is integrated with an AMI network card and has Ethernet and USB ports to support integration with other end devices. Custom software in the AMI head end (Server) and on the IoT router enables communication between a centralized Server and remote end devices for the purposes of command and control or data transfer. The solution architecture employs the IPv6 IP and Transport Layer Security 1.2 for secure communication over the AMI network. Any communication that is not on the AMI, employs a Virtual Private Network (VPN) and Internet Protocol version 4 (IPv4) IP.

The IEEE 2030.5 standard is used for communications between the Client and the Server. This standard is independent of the underlying physical transport designed to work over any technology that supported the IP. The IEEE 2030.5 standard through its application layer defines a complete set of functions that provides many energy management function such as demand response, load control, time of day pricing, management of DG, electric vehicles, etc. This standard defines the mechanisms for exchanging application messages, the exact messages exchanged including error messages, and the security features used to protect the application messages. The California Public Utility Commission has adopted the IEEE 2030.5 standard as the default communications protocol in California for grid integration of DERs.

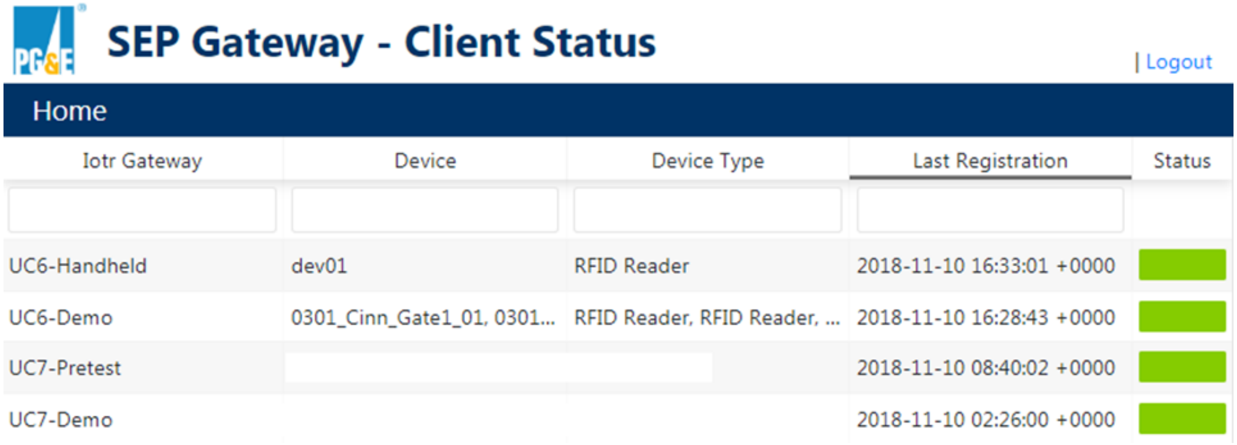
While the Client interface with the Server used the IEEE 2030.5 protocol, the Client is also equipped with different protocol interfaces or adapters to communicate with a multitude of end devices. The protocol adapters include MODBUS for communication with smart inverters, Distributed Network Protocol (DNP3) for communication with SCADA devices, Low-Level Reader Protocol (LLRP) for communication with RFID devices and Hypertext Transfer Protocol (HTTP)/Secure Shell (SSH) for communication with end devices using standard HTTP messaging or to pull data files from the Client using SSH.

4.1.2. Client-Server Software Development

A significant part of this project was the development of the Client-Server software for communication between the Server and the end devices. Both the EPIC 2.26 Server and Client were written as web services using Java to maximize the use of open source frameworks and libraries. The EPIC 2.26 Server contains the GUIs that the operators use for communicating with the end devices, as well as the IEEE 2030.5 interface for transmitting the information over the AMI network using IEEE 2030.5 specification model elements and processes. The Server software was designed for and deployed on a virtual machine running a Linux-based operating system. The EPIC 2.26 Client was deployed on IoT Routers that were designed to support multiple end devices.

The Client software is programmed to launch automatically and start the IEEE 2030.5 Client registration process upon initial power up of an IoT Router containing the EPIC 2.26 Client software. This registration process includes the Client finding the Server automatically through a service discovery process followed by the Client sending authentication credentials to the Server. Figure 2 shows the Client status dashboard on the Server that displays the devices that were registered with the Server.

Figure 2: Client Status Dashboard



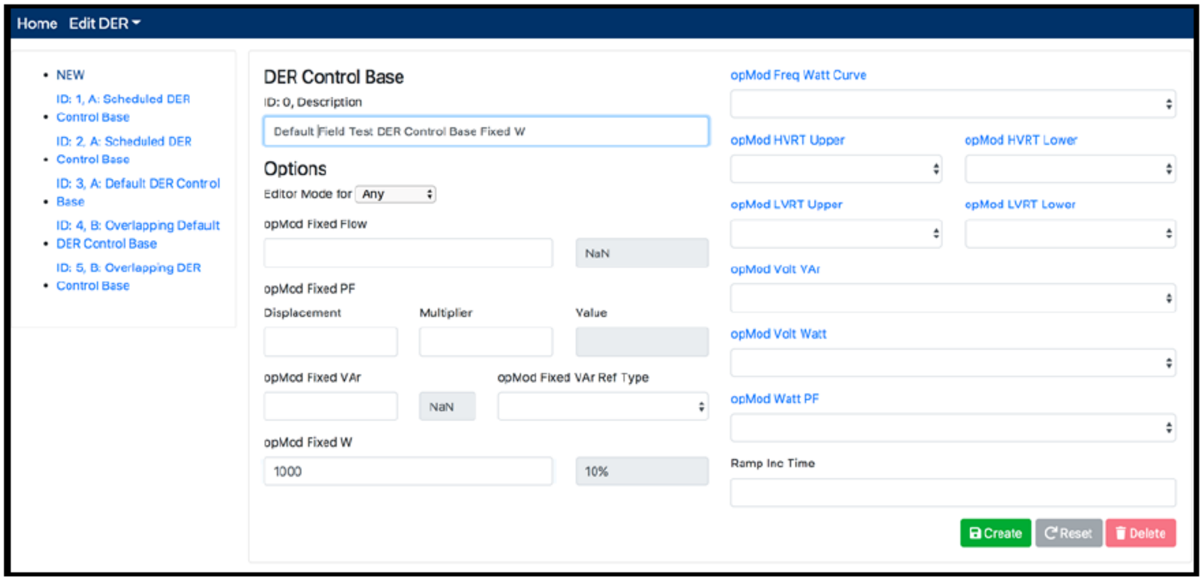
SEP Gateway - Client Status

Iotr Gateway	Device	Device Type	Last Registration	Status
UC6-Handheld	dev01	RFID Reader	2018-11-10 16:33:01 +0000	🟩
UC6-Demo	0301_Cinn_Gate1_01, 0301...	RFID Reader, RFID Reader, ...	2018-11-10 16:28:43 +0000	🟩
UC7-Pretest			2018-11-10 08:40:02 +0000	🟩
UC7-Demo			2018-11-10 02:26:00 +0000	🟩

Once the Server validates the Client's credentials, it informs the Client of the Server functions it may access and to which the Client may subscribe. The Subscription/Notification process is important for communicating over AMI because it is more bandwidth efficient than the Client having to poll the Server for changes. Another important facet of IEEE 2030.5 for use on the AMI network is the use of Efficient Extensible Markup Language (XML) Interchange or compressed XML between the Server and Client which also conserves bandwidth. Also included within the Client registration process are messages to synchronize the Client clock with the Server and reporting of Client common resource information reflecting network status and end device configuration.

Following successful registration, the Server and Client perform additional IEEE 2030.5-compliant messaging as required by the type of end device being managed by the Client. For DER devices such as smart inverters, the Server User Interface (UI) can be used to define specific details of DER Programs such as start time, duration, and operational mode settings. Figure 3 shows the DER Control Base Creation for an UI to control the voltage, real and reactive power settings of a DER. For other use cases that require messaging outside of the smart energy space, the proprietary extension portion of IEEE 2030.5 is used to send custom messaging between Server and Client.

Figure 3: DER Control Base Creation



- NEW
- ID: 1, A: Scheduled DER Control Base
- ID: 2, A: Scheduled DER Control Base
- ID: 3, A: Default DER Control Base
- ID: 4, B: Overlapping Default DER Control Base
- ID: 5, B: Overlapping DER Control Base

DER Control Base

ID: 0, Description: Default Field Test DER Control Base Fixed W

Options

Editor Mode for: Any

opMod Fixed Flow: NaN

opMod Fixed PF

Displacement | Multiplier | Value

opMod Fixed VAr: NaN

opMod Fixed VAr Ref Type

opMod Fixed W: 1000 | 10%

opMod Freq Watt Curve

opMod HVRT Upper

opMod HVRT Lower

opMod LVRT Upper

opMod LVRT Lower

opMod Volt VAr

opMod Volt Watt

opMod Watt PF

Ramp Inc Time

In addition to the Client-Server software, the following protocol adapters required for communicating with the end devices were also developed in this project.

- MODBUS – Used to read and write information from and to smart inverters. While some adherence to the SunSpec standard existed across smart inverters of different vendors, the Client had some customizations for each supported make and model as required by the vendor. IEEE 2030.5 DER Program, Control, and Curve messages had to be translated to the appropriate MODBUS register commands.
- DNP3 – Used to communicate with devices in power transmission and distribution grid that can be remotely monitored and/or controlled. For this protocol, no vendor-specific handling was required and all DNP3 messages received from the Server were forwarded to the end device directly by the Client.
- LLRP – A vendor-agnostic, XML-based protocol used to communicate to RFID readers. The Server was capable of storing and sending individual or batches of LLRP messages to the Client which were relayed directly to the RFID readers being managed by the Client. LLRP messages containing RFID tag read data were received from the RFID readers and aggregated within the Client in a cache and held until requested by the Server to limit the amount of data sent between the Client and Server.
- HTTP/SSH – The Client also had generic adapter capabilities to communicate to end devices using standard HTTP messaging or to pull data files from the Client using SSH.

The Server also has an Application Programming Interface (API) for receiving and interpreting inbound DNP3 messages from a SCADA Master software. The Server decodes the SCADA address of the message and forwards it to the IoT router that is hosting the end device for which the message is intended. The Server can be configured with multiple inbound DNP3 channels as required by the number of managed SCADA devices.

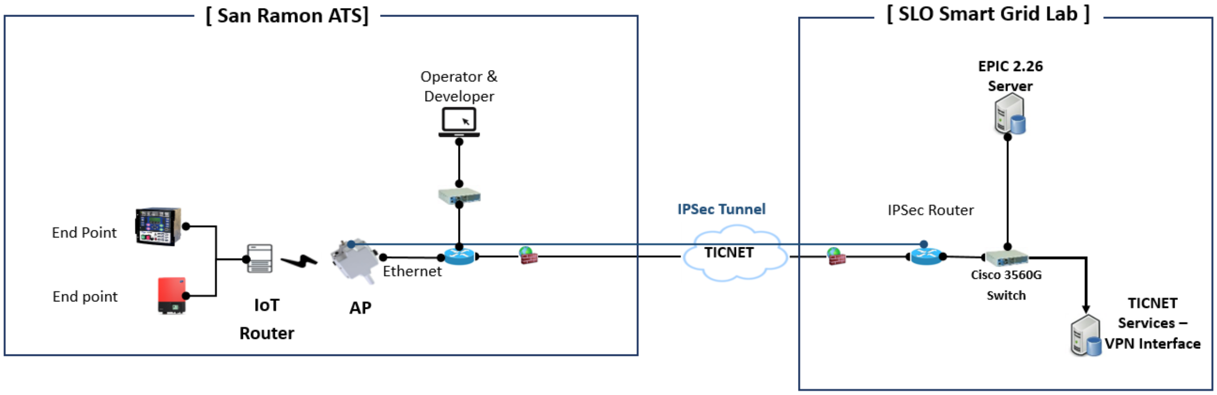
4.1.3. Architecture for Lab Testing

The high-level architecture described earlier was implemented in both lab and field settings. After considering several options for testing the architecture in a lab setting, PG&E chose the "On-premises" model with PG&E's San Ramon ATS lab since this provided a secure and controlled test environment that was easy to set up. Figure 4 shows the lab test architecture.

The testing network was located at two sites. The local site was in San Ramon and it included the AP to the AMI network, the IoT Router, and the endpoint (end devices) being tested. The remote site was in San Luis Obispo (SLO) and had the EPIC 2.26 Server and the VPN access to the TICNET testing network. TICNET is the network operated and managed within PG&E and is located in the SLO lab, as well as at the ATS facility in San Ramon. The AP communicates to the EPIC 2.26 Server via an IPv6 tunnel.

An operator can connect to the network by being onsite in San Ramon or through the VPN. Communication flows from the endpoint, to the IoT Router, to the AP, to the EPIC 2.26 Server and vis-a-versa. User access to the EPIC 2.26 Server was provided by a web interface which was made available anywhere inside the testing network.

Figure 4: Lab Test Architecture

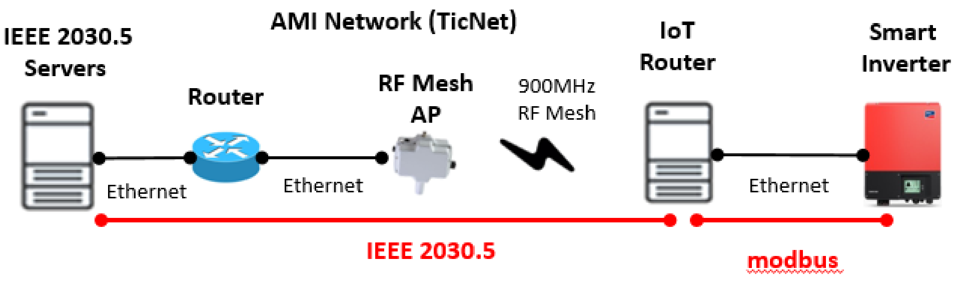


The end devices for each use case and how they communicate with the IoT router is discussed next.

Use Case #2 – Solar Smart Inverter

For this demonstration, PG&E chose smart inverters manufactured by two manufacturers. The primary method of reading data from and performing control on the smart inverter is through a MODBUS interface. Modbus is a serial communications protocol often used to connect a supervisory computer with a remote terminal unit in SCADA systems. All messaging to the end device were forwarded by or translated locally within the Client to MODBUS for communication to the end device.

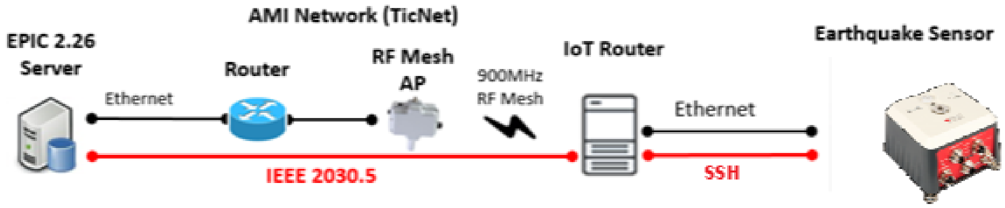
Figure 5: Network Diagram for Use Case #2



Use Case #3 – Sensors

For this demonstration, PG&E chose an off-the-shelf earthquake sensor from a vendor. All messaging to the sensors were translated locally within the Client to HTTP for communication. Data retrieval from seismic devices was supported locally by using the SSH protocol.

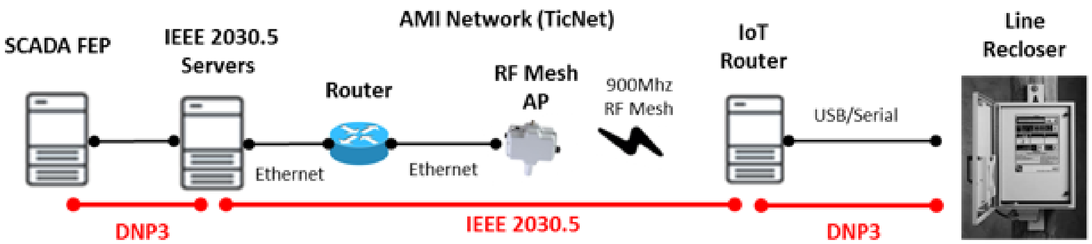
Figure 6: Network Diagram for Use Case #3



Use Case #5 – Distribution Automation /SCADA Overhead and Underground Intelligent Electric Devices (IED)

For this demonstration, PG&E chose a line recloser controller, an automatic capacitor controller and an underground switch controller normally used in its distribution system. For this use case, all messaging to the end devices were forwarded by or translated locally within the Client to DNP3 for communication. The DNP3 API was used to receive DNP3 control commands from the SCADA Master software. DNP3 is a set of communications protocols used between components in process automation systems.

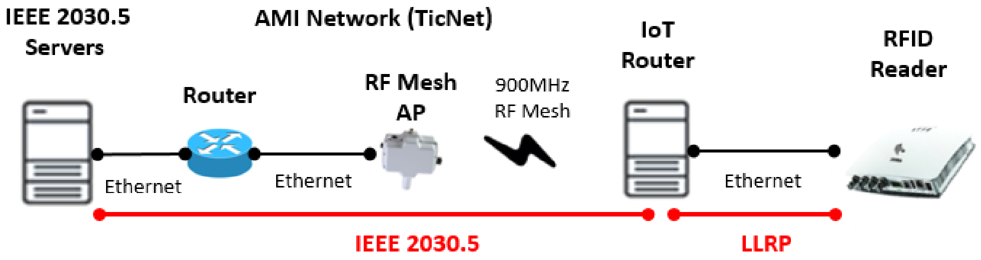
Figure 7: Network Diagram for Use Case #5



Use Case #6 – Radio Frequency Identification Tags (RFID tags) Over AMI Network

For this demonstration, PG&E chose RFID readers and tags manufactured by two different vendors. All messaging to the RFIDs were translated locally within the Client to LLRP. LLRP is the RFID-aware protocol that is intended to standardize the network interface of the RFID readers. It is designed as a standard for developers to have a common programmatic interface to RFID readers from different manufacturers.

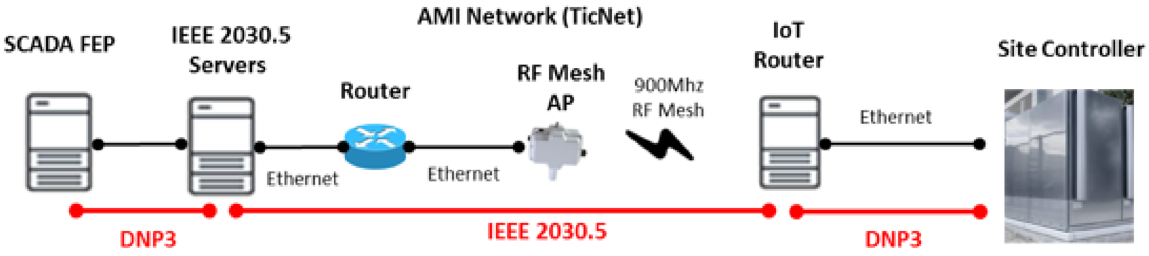
Figure 8: Network Diagram for Use Case #6



Use Case #7 – Direct Acquisition and Control Telemetry Solution Use Case

For this demonstration PG&E chose a DG site that uses fuel cells as the DC source for the inverters. All messaging to and from the meter and inverter were DNP3 and were forwarded by the Client to the Server and vis-a-versa.

Figure 9: Network Diagram for Use Case #7



4.1.4. Architecture for Field Testing

After evaluating several options, PG&E decided to go with the option of the EPIC Server installed on the VPC. One of the main reasons for choosing this option is that PG&E has already planned to move its data center to the VPC platform. In addition to offering a cost advantage over other platforms, another reason that the VPC is attractive is the fact that it enables easier scaling up since there are inherently no capacity limitations in a cloud-based platform. Another advantage of choosing the VPC platform is that it can be leveraged for other projects that need access to the AMI network.

Figure 10 shows the solution architecture for the field tests for use cases #2, #6 and #7. Two field tests were conducted for use case #7 – on a fuel cell controller (use case #7a) and a PV plant controller (use case #7b). The solution architecture for these two use cases are shown inFigure 11 Figure 11. The key components of the field test architecture are described below.

- **PG&E EPIC VPC**: PG&E EPIC IPv4/6 VPC was created as a virtual network under the existing PG&E VPC as shown in (1) of Figure 10. Two subnet zones were created for the EPIC Servers – a Pre-test zone for validating the use cases and a Demonstration Zone for demonstrating the use cases.
- **PG&E Transit VPC**: The Transit VPC (2) is used for routing traffic from the VPC to other PG&E systems that use IPV4 protocol such as the Real-time SCADA (RT SCADA). This is achieved using a new VPN connection between PG&E VPC and User Data Network (UDN) and an existing connection between UDN and Operations Data Network (ODN) on which RT SCADA is installed. The UDN connectivity allows PG&E operators to access the EPIC 2.26 Server.
- **VPC Peering Connection**: The VPN Peering connection (3) is used for shared services from PG&E Management VPCs such as cybersecurity services.
- **AMI Test Environment**: The AMI test environment (4) is used for validating new services or new products to avoid service impact of Production environment.
- **F5 Virtual Private Network Gateway**: The F5 Virtual Private Network Gateway (VPG) (5) is used to provide a secure connection between the VPC and the Smart Meter Data Center using a VPN connection.
- **ODN-Dimilitarized Zone (DMZ) Router**: The ODN-DMZ router (6) creates a “Demilitarized Zone” for restricted access to the UDN network.

The field architecture used the Code Drop (CD03) AMI Test Environment Server with a single hop-count[14] between the AP and the IoT router. The field test set up and the communication method between the IoT router and the end device for the uses cases are discussed next.

[14] The hop count refers to the number of intermediate devices through which data must pass between source and destination.

Figure 10: Field Test Architecture for Use Cases #2, #6 and #7

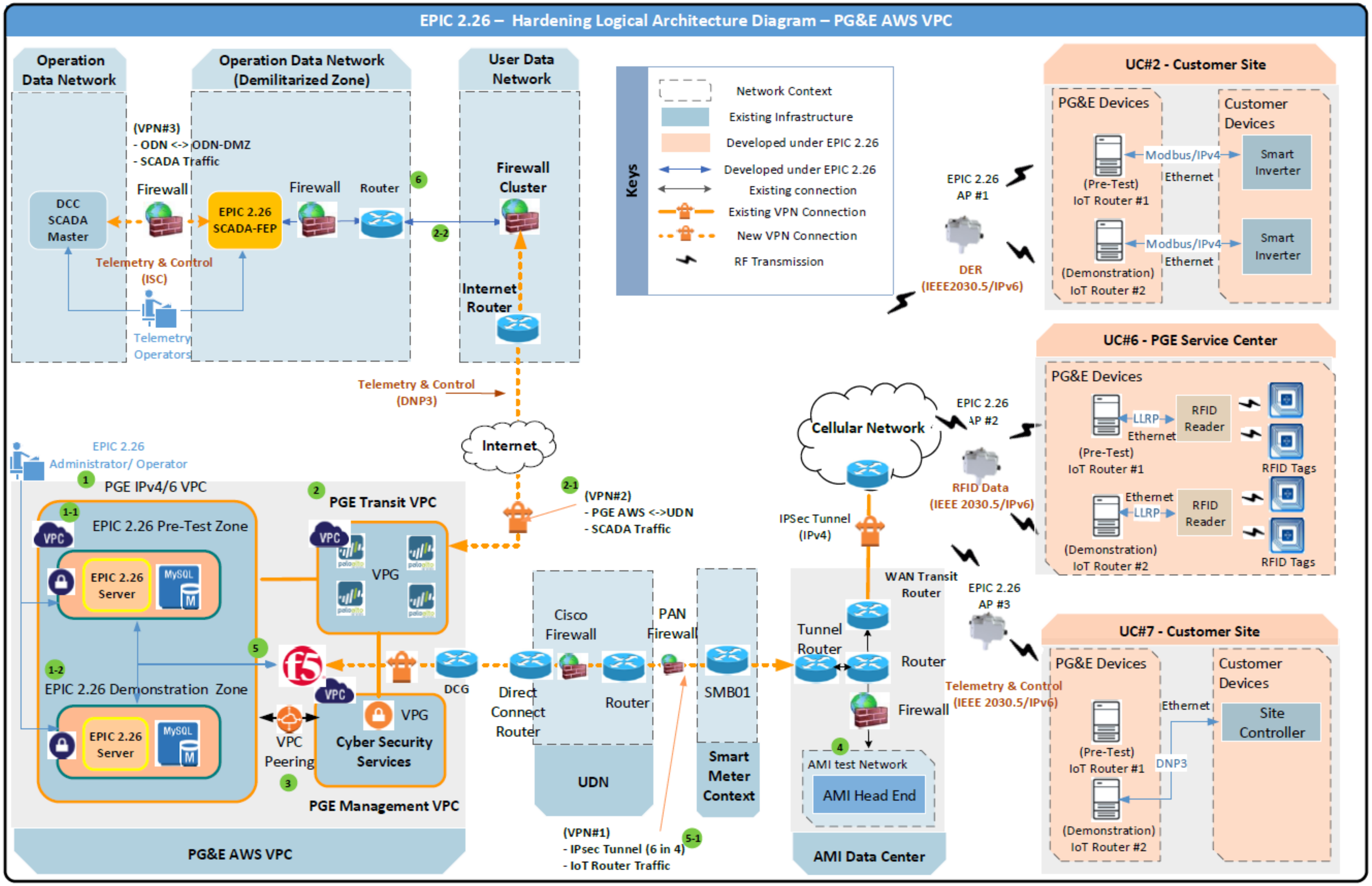
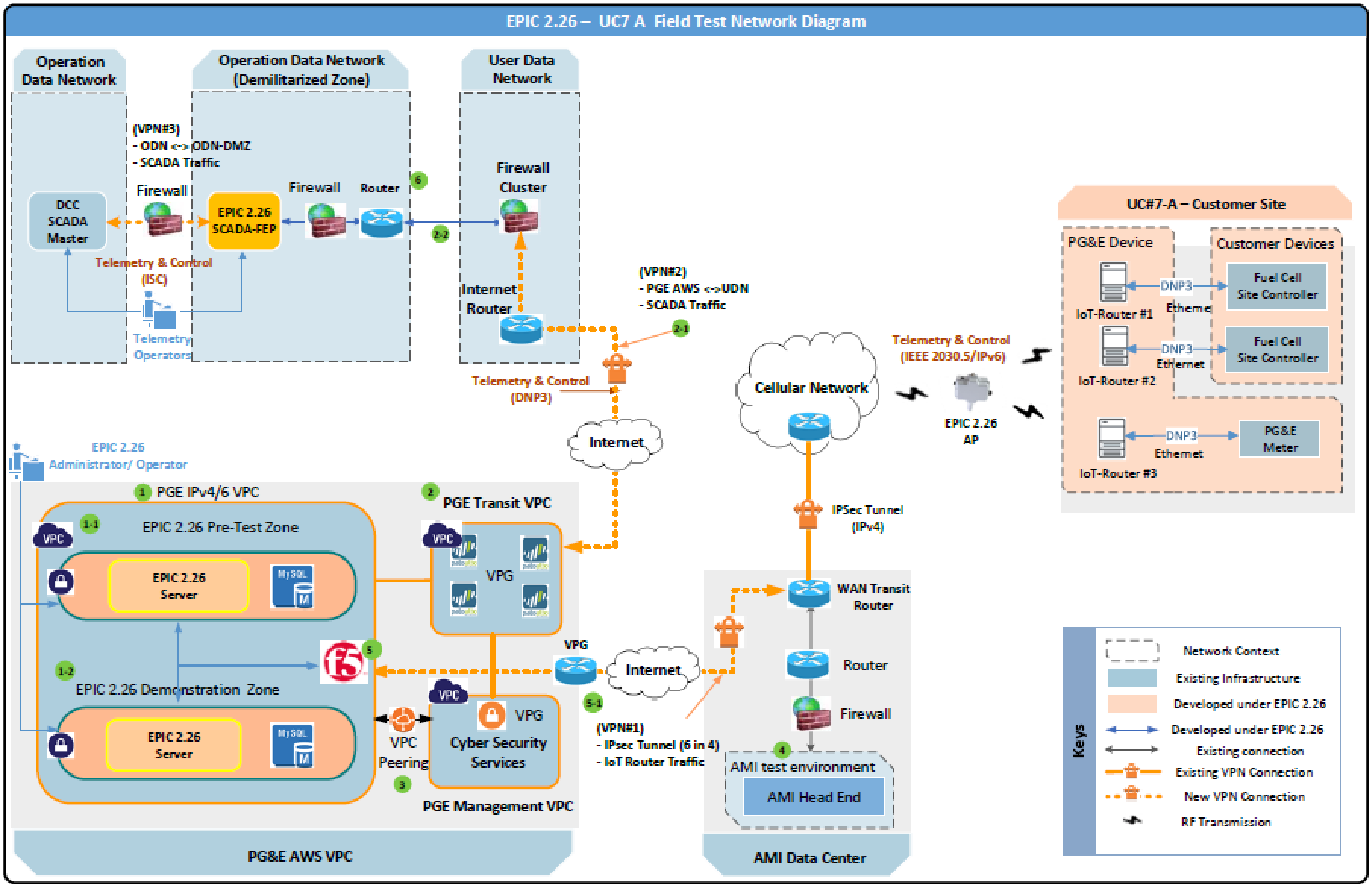


Figure 11: Field Test Architecture for Use Case #7a



Use Case #2 – Solar Smart Inverter
Figure 12 and Figure 13 show the field installation setup and the network diagram for use Case #2. The two smart inverters were installed at a test facility in San Ramon. The smart inverters communicate with the IoT routers over the Ethernet using the Modbus interface. Two IoT routers were installed at each site – a pre-test router for testing purposes and a demonstration router for use case demonstration purposes. The IoT router communicates with a CD03 AP over the AMI Network. The EPIC Server was able to monitor and control the smart inverters via the F5 VPG and the AMI network using IEEE 2030.5 interface.

Figure 12: Field Test Setup for Use Case #2

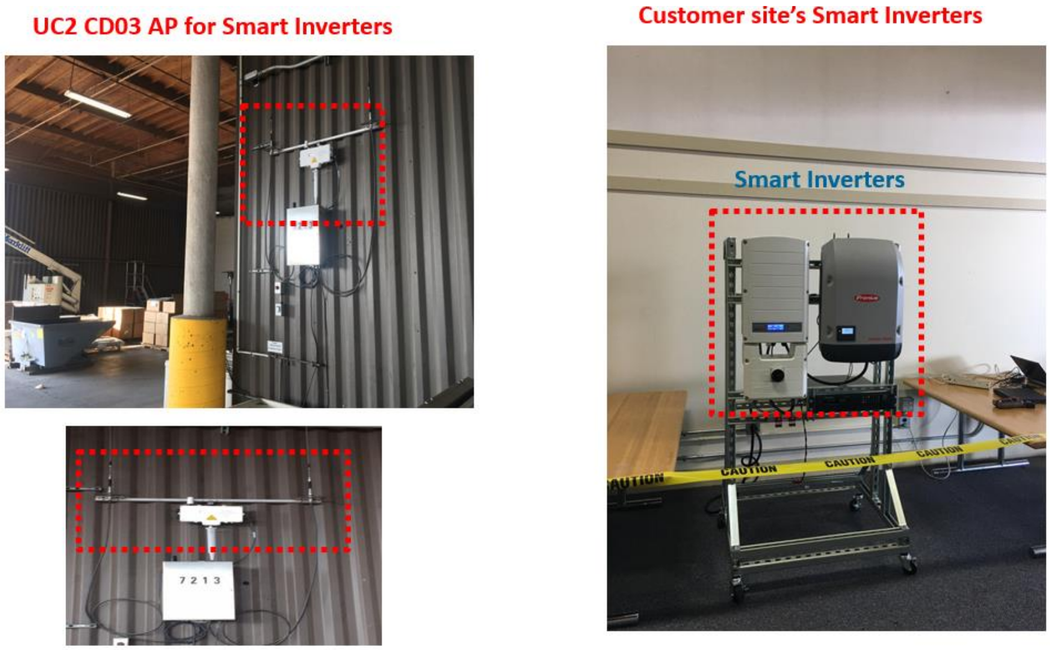
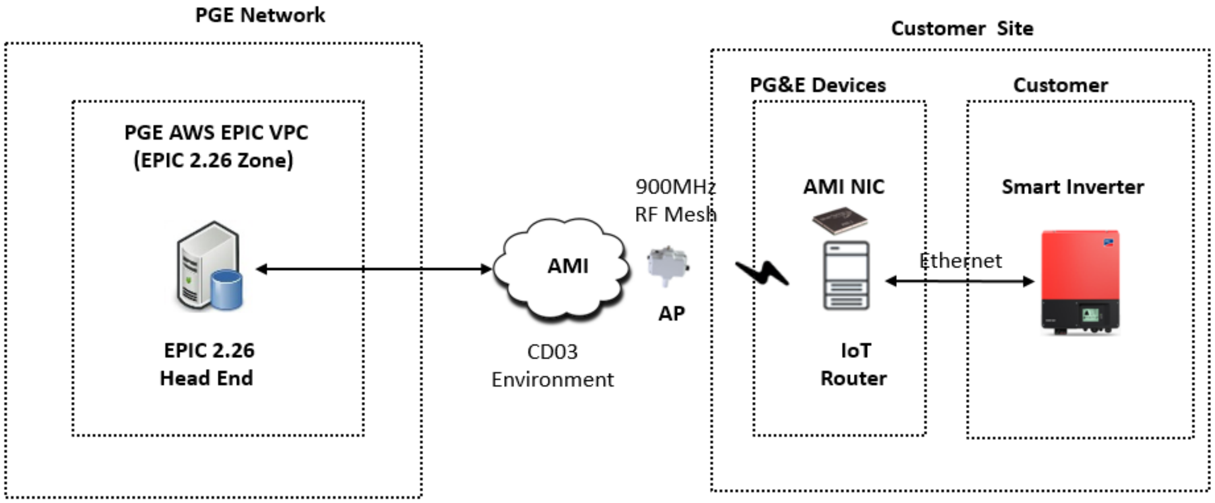

UC2 CD03 AP for Smart Inverters
Customer site's Smart Inverters
Smart Inverters
7213
CAUTION

Figure 13: Network Diagram for Use Case #2



Use Case #6 – Radio Frequency Identification Tags (RFID tags) Over AMI Network

Figure 14 and Figure 15 show the field installation setup and the network diagram for use Case #6. The RFID devices were located at PG&E’s Cinnabar service center in San Jose. The RFID readers were placed in trucks, gates and other key locations within the facility. The RFID readers were connected to a Local Area Network switch which was then connected to the IoT routers. Two IoT routers were installed at each site – a pre-test router for testing purposes and a demonstration router for use case demonstration purposes. The LLRP interface was used for communication between IoT router and RFID Readers. LLRP is composed of almost 100 standard commands and provides an interface to low level functionality that is uniform across different reader vendors. The IoT router communicates with a CD03 AP over the AMI Network. The EPIC Server was able to monitor the RFID readers via the F5 VPG and the AMI network using IEEE 2030.5 interface.

Figure 14: Field Test Set Up for Use Case #6

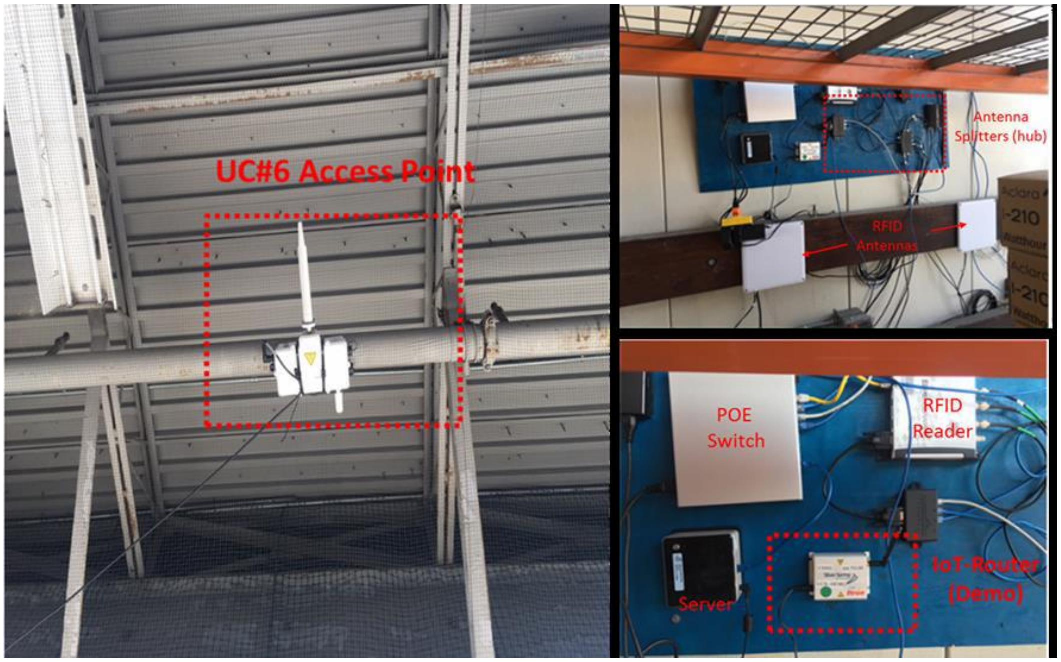
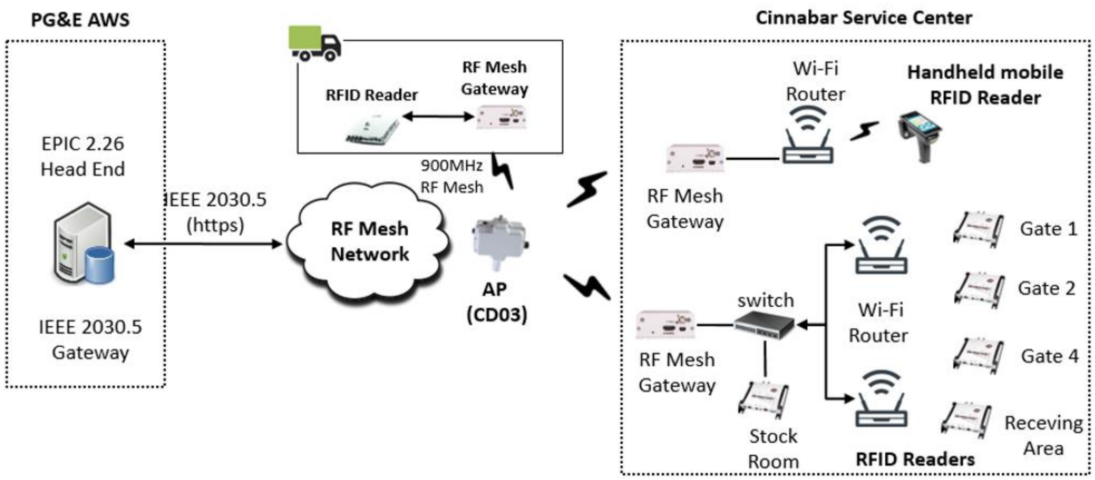
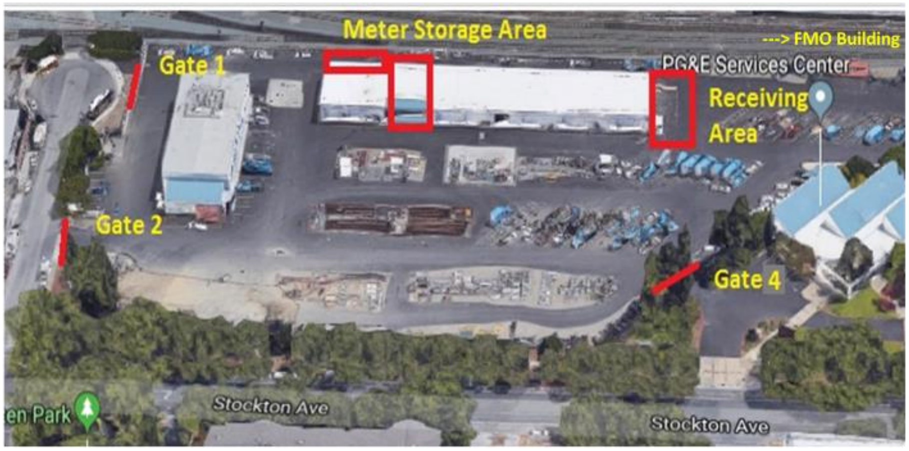


Figure 15: Network Diagram for Use Case #6



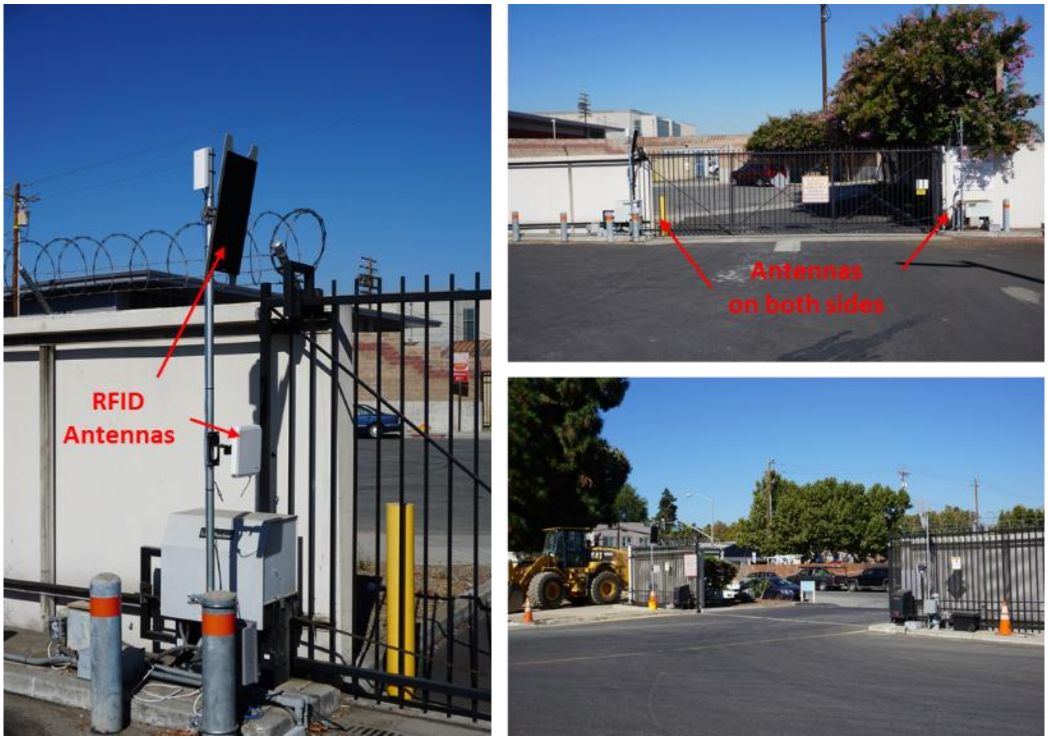
One of the primary goals of this use case was to test RFID's ability to track meter assets located in PG&E service centers and on the back of service vehicles, an area in a meter's lifecycle where PG&E has the least amount of visibility to the asset. With that goal in mind, RFID readers were strategically installed at known areas in the Cinnabar Service Center where meter assets consistently travel as they are delivered, transported and stored.

Figure 16: Yard Gates and Receiving and Storage Areas



Yard Gates: At the Cinnabar Service Center, there are three main service gates where meters enter and exit the yard during normal operation. RFID readers were installed on both side of each gate to capture the ingress and egress of meters.

Figure 17: RFID Readers on Yard Gates

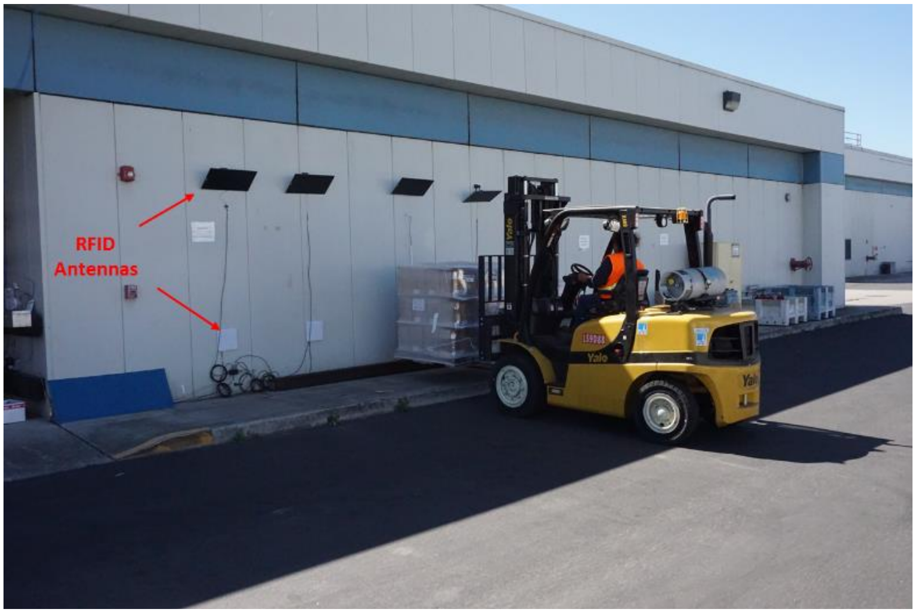


Receiving Area: Nearly all the meters that are shipped from PG&E's distribution centers are first delivered to the receiving area making it an important area to place RFID readers. The receiving area serves as a handoff point between Supply Chain's distribution operations and Cinnabar's material operations team.

Meter Storage Area: Once received by the service center team, meters are put away in the storage area and allows field technicians to take meters for their scheduled work.

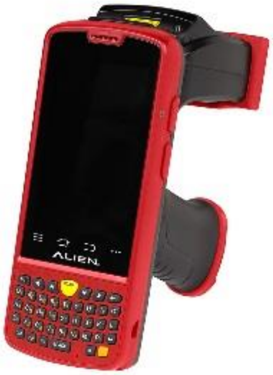
Service Vehicles: The service truck use case is twofold 1) prove RFID readers can track meters on PG&E service vehicles and 2) from the service vehicle, communicate meter data through the AMI network via mesh network APs. For this use case, two PG&E vehicles were outfitted with RFID Readers. The RFID reader and IoT routers were installed behind the passenger seat of each truck.

Figure 18: Meter Storage Area



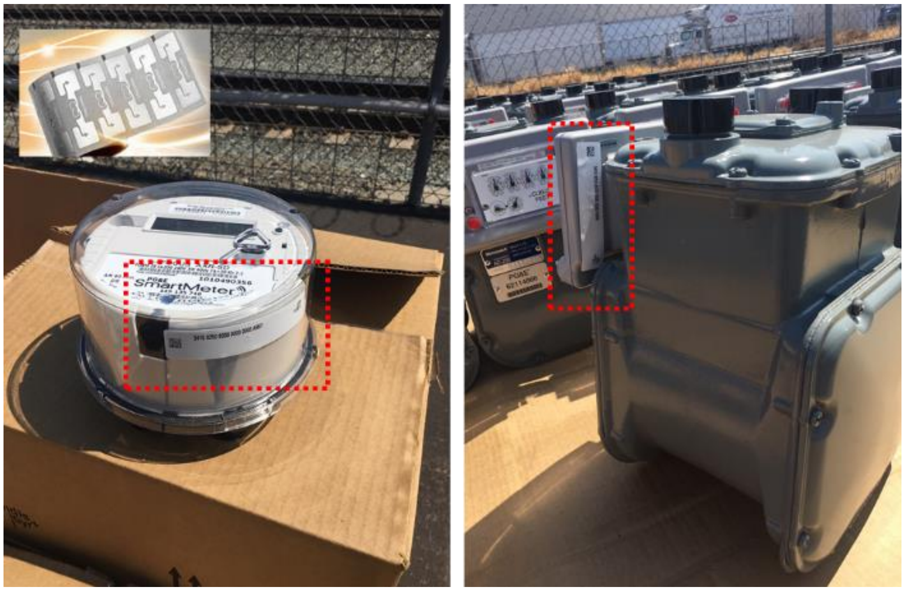
RFID Handheld Devices: A mobile RFID handheld use case was added to fill the gaps where meter assets need to be captured beyond gates and storage areas.

Figure 19: Handheld RFID Reader



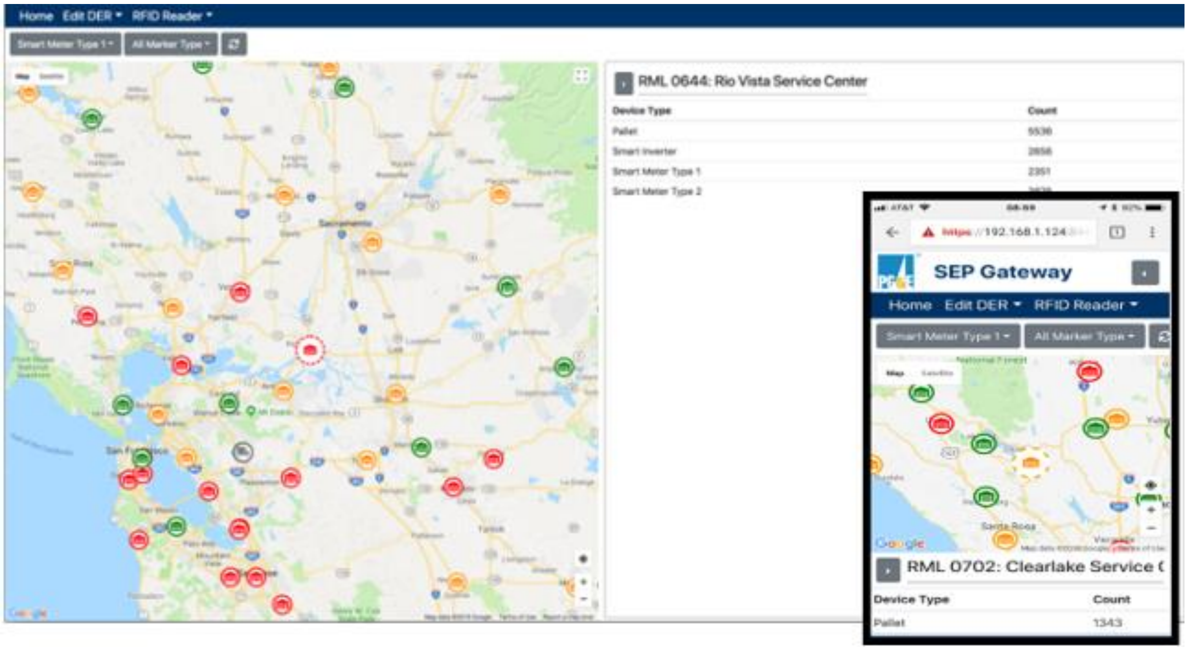
Meter Tags: RFID tags perform the best on non-metallic surfaces. For the field testing, RFID tags were placed on the outside of plastic surfaces on the meters, see below. It is recommended that in production, the RFID tags be installed during the assembly process and placed inside the meter's body.

Figure 20: RFID Tags on Electric and Gas Meters



Software: To support field testing and provide visualizations, a graphical user interface (GUI) was developed by PG&E. This GUI is currently limited to Cinnabar and two service vehicles, however once fully deployed the GUI will provide all PG&E employees access to near-real time inventory of meter assets located at 50+ service yards. This real-time inventory data would help PG&E streamline processes such as scheduling, dispatch and inventory replenishment.

Figure 21: Graphical User Interface Showing the Location of Assets



RML 0644: Rio Vista Service Center

Device Type	Count
Pallet	5536
Smart Inverter	2856
Smart Meter Type 1	2351
Smart Meter Type 2	[illegible]

RML 0702: Clearlake Service (

Device Type	Count
Pallet	1343

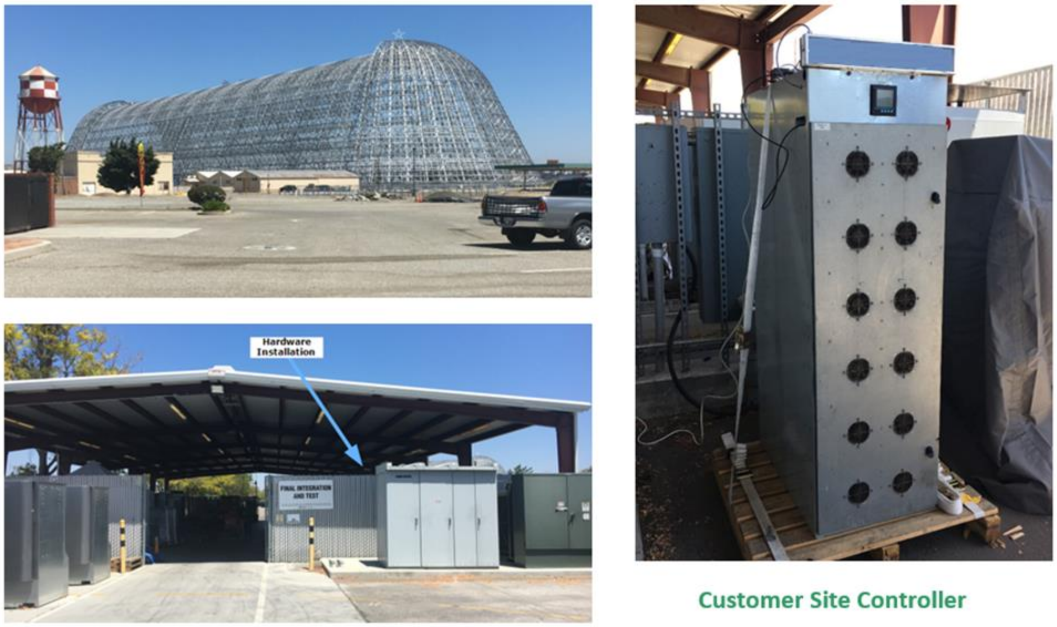
Use Case #7 – Direct Acquisition and Control Telemetry Solution

Figure 22 and FigureFigure 23 show the field installation setup for use Cases #7 and #7a respectively. Figure 24 and FigureFigure 25 show the network diagrams for use Cases #7 and #7a respectively.

For use Case #7, the fuel cell simulator and the site controller were located at the customer's facility. Two IoT routers were installed at each site – a pre-test router for testing purposes and a demonstration router for use case demonstration purposes.

Use Case #7a consists of two tests with two fuel cell site controllers on fuel cell generators and a PG&E meter located at the customer's facility. While the fuel cell site controllers measure the fuel cell generation, the PG&E meter monitors the total net energy usage of the customer's facility. Each of the two site controllers and the PG&E meter are connected to three separate IoT routers. All the IoT routers are connected over Ethernet using the DNP3 protocol and communicate with a separate CD03 AP over the AMI Network. The EPIC Server works as a protocol Gateway to transfer the DNP3 data with IEEE 2030.5 interface. SCADA systems were used to manage and control the Site Controller through EPIC 2.26 Server to use AMI Network.

Figure 22: Field Test Set Up for Use Case #7



Customer Site Controller

Figure 23: Field Test Set Up for Use Case #7a

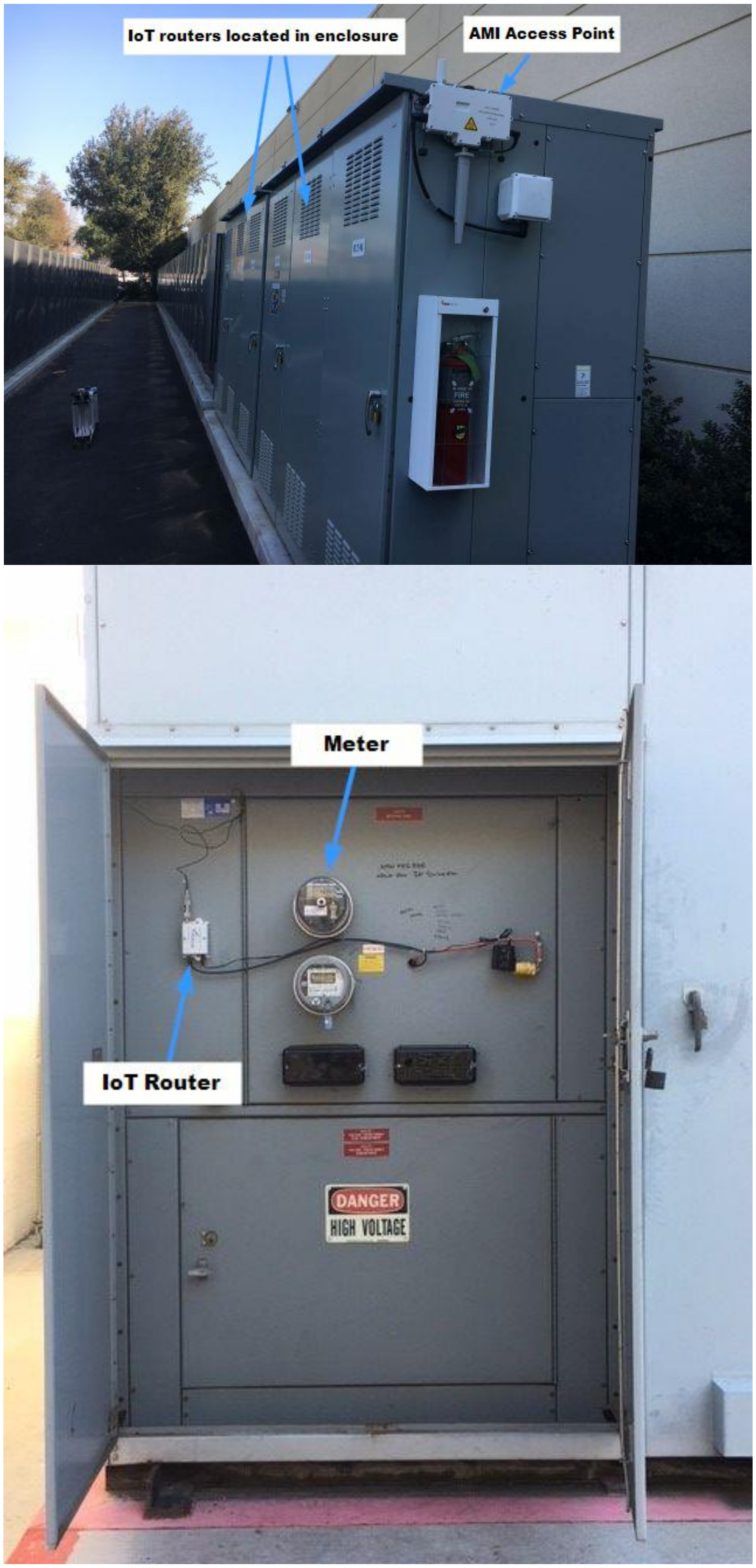


Figure 24: Network Diagram for Use Case #7

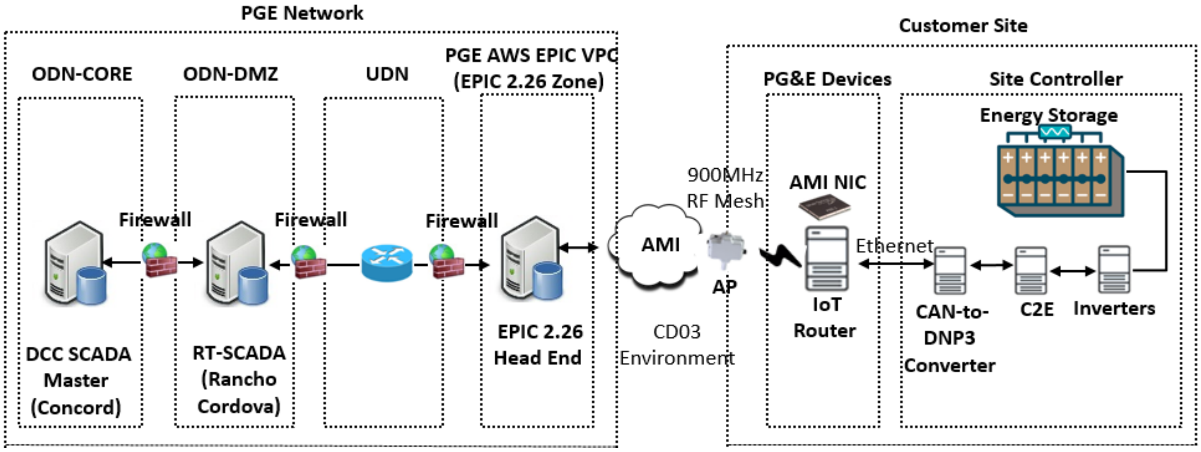
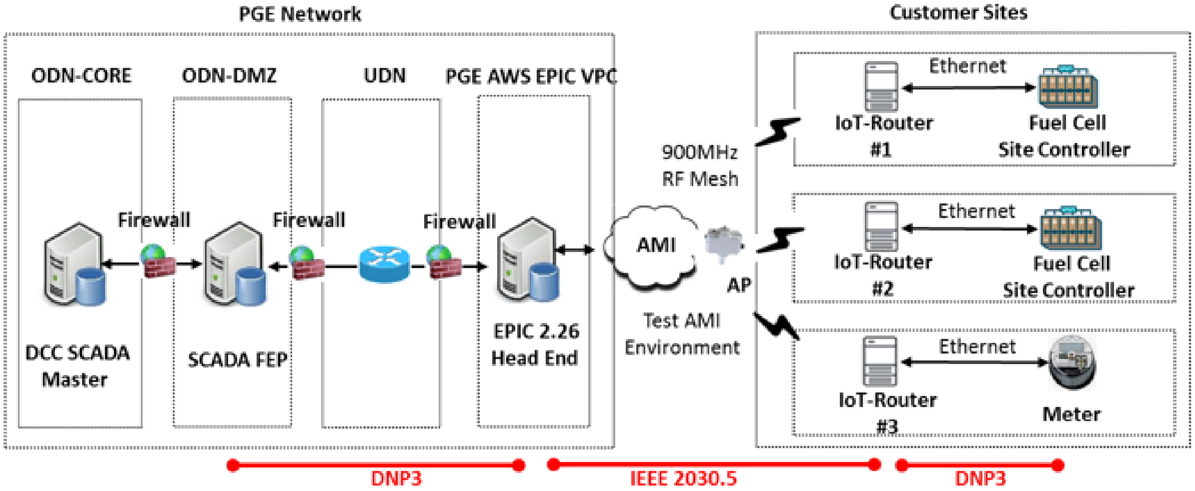


Figure 25: Network Diagram for Use Case #7a

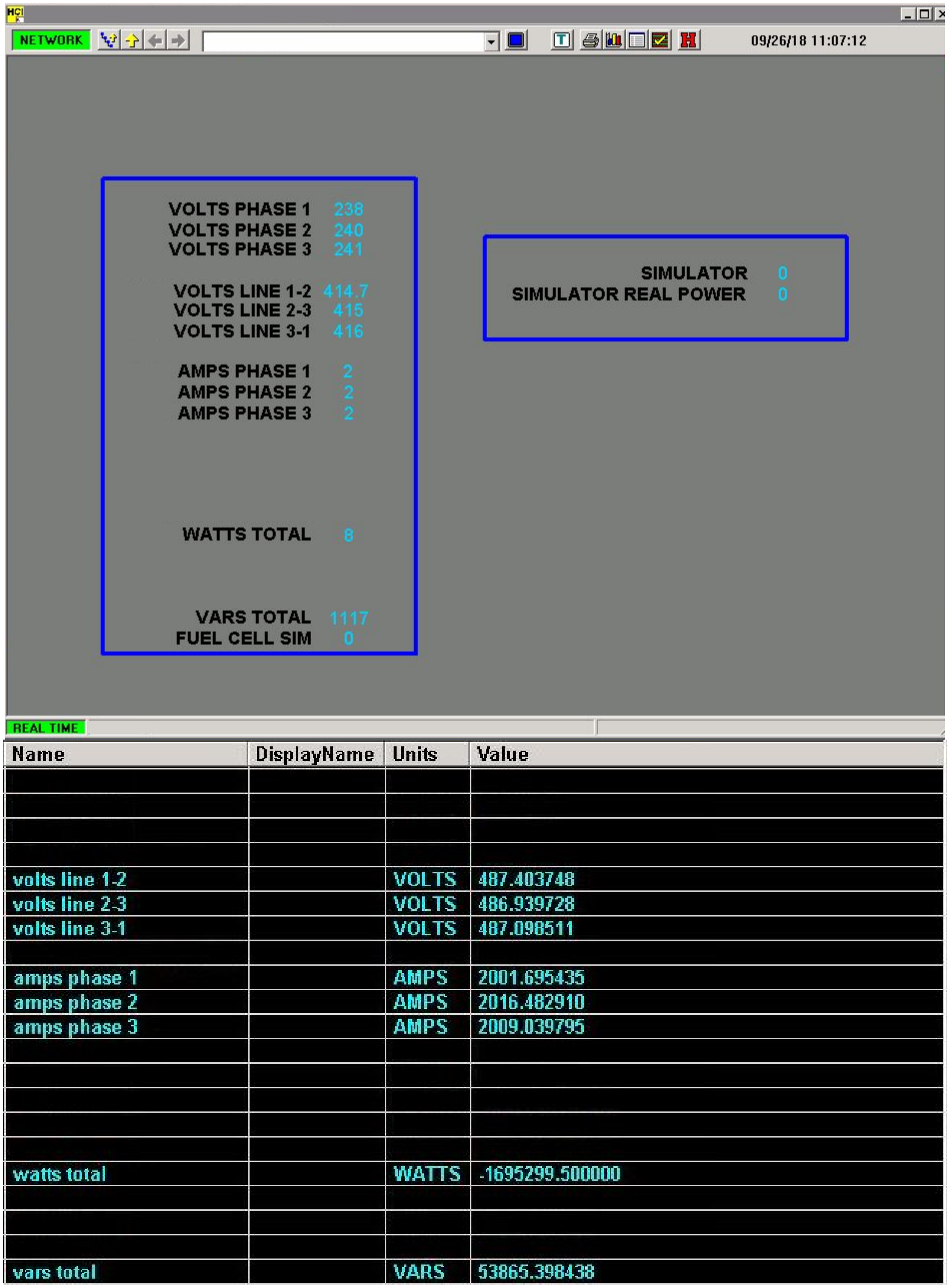


The field testing for use Case #7 and #7a consisted of two phases (phases 2 & 3) as follows:

- Phase 1 testing: This testing was performed in the lab as a baseline for Phase 2 & 3 testing
- Phase 2 testing: This testing was performed with the focus of polling and controlling physical site controller equipment from the third-party vendor to PG&E distribution SCADA in ODN-DMZ
- Phase 3 testing: This phase of testing is the extension of Phase 2 testing with the addition of Distribution Control Center SCADA Master in ODN Core

Two screenshots of the fuel Cell telemetry data and control display developed for use Case #7 and #7a are shown in Figure 26.

Figure 26: Use Case #7 and #7a Fuel Cell Telemetry Data and Control Screenshots



VOLTS PHASE 1 238
VOLTS PHASE 2 240
VOLTS PHASE 3 241

VOLTS LINE 1-2 414.7
VOLTS LINE 2-3 415
VOLTS LINE 3-1 416

AMPS PHASE 1 2
AMPS PHASE 2 2
AMPS PHASE 3 2

WATTS TOTAL 8

VARS TOTAL 1117
FUEL CELL SIM 0

SIMULATOR 0
SIMULATOR REAL POWER 0

Name	DisplayName	Units	Value
volts line 1-2		VOLTS	487.403748
volts line 2-3		VOLTS	486.939728
volts line 3-1		VOLTS	487.098511
amps phase 1		AMPS	2001.695435
amps phase 2		AMPS	2016.482910
amps phase 3		AMPS	2009.039795
watts total		WATTS	-1695299.500000
vars total		VARS	53865.398438

To continue supporting the implementation and deployment of the Direct Acquisition and Control Telemetry solution, the network infrastructure needs to be designed to manage the data traffic in the AMI network and scaled accordingly to move this use case from demonstration to production. The network design for the new VPN connection was completed. Provisioning and establishing the new VPN connection to harden the cybersecurity for the systems between PG&E cloud and headend server was also completed.

4.2. Task 2: Lab Testing of Use Cases

Several tests were performed in the laboratory to evaluate the performance of the use cases. High-level connectivity tests involved testing the performance between the EPIC 2.26 Server and the IoT router. These tests did not involve any interaction with the end devices. Specific tests were also performed to test the capability and performance of specific functions in each use case. This section presents the results of the high-level connectivity tests followed by those from the use case-specific functional tests.

4.2.1. High-Level Connectivity Testing

The purpose of the high-level connectivity testing was to demonstrate the capabilities of the IoT Router and the IEEE 2030.5 communication protocol. The testing in the PG&E lab ran between a workstation, AP and the IoT router for initial communications tests. On this test network, PG&E used a local copy of EPIC 2.26 IEEE 2030.5 Server to control a smart inverter.

The results of the key connectivity test are summarized below.

Table 1: Test Results for High-Level Connectivity Testing

Test	Result
DNS testing – Server and Client use correct IP addresses, port, domain, etc. when listening for responding to queries	Pass
Certificate management testing – Server and Client support IEEE 2030.5 Public Key Infrastructure (PKI) Certificates	Pass
All Functionality testing – Server and Client testing for application support, design patterns and security	Pass
Specific Functionality testing – Server and Client testing for Device Capability, Time, Metering, Download File, Distributed Energy Resources Program, Power Status, Network Status, Log Event List, Configuration, Function Set Assignments	Pass

4.2.2. Use Case-Specific Connectivity Testing

The performance of the communication network was tested for each use case using one-way and roundtrip latency as indices. The results of these performance tests indicate the performance of the underlying hardware and establish a baseline for measuring the performance of the various use cases in the field tests. A brief description of each index is provided below.

- One-way latency (milliseconds): The length of time it takes for a packet of information to travel from the source to destination; and
- Round-trip latency (milliseconds): The length of time it takes for a packet of information to travel from the source to destination and back.

For comparison, the following SCADA latency information was measured:

- 12 Seconds to 60 Seconds on a normal day
- 15 Seconds to 300 Seconds on a stormy day

It is provided in a range because SCADA uses various radios and networks such as 900 megahertz band (slower) and Cellular (faster) technologies. Because SCADA equipment and devices depend on the available RF network and radio technologies, utility industry has not yet established the latency standards or requirements. It is expected that shorter latency means better technology.

Table 2 shows the average one-way and roundtrip average latency values in milliseconds. End-to-end network latency was measured with 4 different payload sizes (1 thousand (K) – 1024 Bytes, 10K, 100K, 1 million (M)) using the same communication path.

Table 2: Lab Test Results for Connectivity Testing

	One-way Latency				Roundtrip Latency			
	Payload (64 bytes)	Payload (124 bytes)	Payload (512 bytes)	Payload (1024 bytes)	Payload (64 bytes)	Payload (124 bytes)	Payload (512 bytes)	Payload (1024 bytes)
UC #2	149.9	192.2	256.3	363.9	299.7	384.4	512.7	727.8
UC #3	147.3	228.0	267.4	375.0	294.6	456.0	534.8	749.3
UC #5	190.8	259.0	334.2	507.1	381.5	518.1	668.3	1014.2
UC #6	167.0	230.1	333.9	492.9	334.0	460.3	667.8	985.8
UC #7	302	513.8	696.8	1974.3	604.0	1032.1	1376.5	3899.8

The latency presented in Table 2 provides, as mentioned before, a baseline communication latency of the network. During the use case testing, any latency above this baseline will be due to the application itself. Use Case #7 was the only use case that presented a strict latency requirement and this baseline is low enough that there is adequate headroom for the application. The baseline network latency for Use Case #7 is higher than the other use cases because the IoT Router and the corresponding endpoint were in a different building from the AP.

When comparing to the SCADA latency above, the latency information in Table 2 appear to be better.

4.2.3. Use Case #2 – Solar Smart Inverter

The purpose of this lab test was to evaluate the ability of a Third-Party Vendor using an IoT router to establish communication, command and control of a Smart Inverter over the AMI network and demonstrate operational communications to the Smart Inverter.

Smart Inverters provide additional functionality when compared to traditional inverters. The additional functionality includes but is not limited to autonomous voltage control using real and reactive power, multiple forms of reactive power control including fixed power factor and fixed Volt Ampere Reactive (VAR), and communications to a remote system operator. In the lab test, the capability to remotely perform several of these functions was evaluated for both the two test inverters. Table 3 shows the results from these tests. The test results prove the ability of using an IoT router to establish communication, command and control of a Smart Inverter over the AMI network.

Table 3: Lab Test Results for Use Case #2

Functionality Test	Result
Demonstrate the capability to schedule reactive power dispatch; 1 hour and 24 hours prior to action	Pass
Demonstrate the capability to schedule real power curtailment; 1 hour and 15 minutes prior to action	Pass
Demonstrate the capability to change control points for Volt-Watt curve of the smart inverter	Pass
Demonstrate the capability to change control points for Volt-VAR curve of the smart inverter	Pass
Demonstrate the capability to gather the metering information such as AC Voltage, AC Current, reactive power, active power, frequency, apparent power and DC power.	Pass
Demonstrate the capability to synchronize the Smart Inverter's internal clock with the AMI network's clock	Pass
Demonstrate the capability to receive diagnostic codes, error codes, and/or alarms from Smart Inverter over AMI network	Pass
Demonstrate the capability to perform firmware upgrades	The EPIC 2.26 Server does not support firmware updates

4.2.4. Use Case #3 – Sensors

The purpose of this lab test was to evaluate the ability of a Third-Party Vendor using an IoT router to establish communication with environmental sensors over the AMI network. This lab testing consists of two phases:

Several tests were performed to evaluate the capability of remotely performing various functions on earthquake sensors. The test results are summarized in Table 4 below. The test results prove the ability of using an IoT router to establish communication, command and control of earthquake sensors over the AMI network.

Table 4: Lab Test Results for Use Case #3

Functionality Test	Result
Demonstrate the capability to read earthquake magnitude in real-time	Pass
Demonstrate the capability to collect and display last 2 hours of magnitude data	Pass
Demonstrate the capability to collect and display last 6 hours of magnitude data	Pass
Demonstrate the capability to collect and display last 24 hours of magnitude data	Pass

4.2.5. Use Case #5 – Distribution Automation/SCADA Overhead and Underground Intelligent Electric Devices (IED)

The purpose of the lab test was to evaluate the ability of a Third-Party Vendor using an IoT router to establish communication, command and control of SCADA devices over the AMI network and demonstrate operational communications to distribution equipment controllers.

Several tests were performed to evaluate the capability of remotely performing various functions on SCADA equipment. PG&E used a local copy of its distribution SCADA software to control a capacitor bank controller, a line recloser controller, and a subsurface switch controller. The equipment involved were subjected to point (Analog, Status, Control and Counter) validation tests via SCADA. Table 5 summarizes the results of the lab tests. The test results prove the ability of using an IoT router to establish communication, command and control of SCADA devices over the AMI network.

Table 5: Lab Test Results for Use Case #5

Functionality Test	Result
Demonstrate the capability of the AMI network to communicate the binary points of the line recloser	Pass
Demonstrate the capability of the AMI network to communicate the binary points of the capacitor bank controller	Pass
Demonstrate the capability of the AMI network to communicate the binary points of the subsurface switch controller	Pass
Demonstrate the capability of the AMI network to communicate the analog points of the line recloser	Pass
Demonstrate the capability of the AMI network to communicate the analog points of the capacitor bank controller	Pass
Demonstrate the capability of the AMI network to communicate the analog points of the subsurface switch controller	Pass
Demonstrate the capability of the AMI network to communicate the control points of the line recloser	Pass
Demonstrate the capability of the AMI network to communicate the control points of the capacitor bank controller	Pass
Demonstrate the capability of the AMI network to communicate the control points of the subsurface switch controller	Pass

4.2.6. Use Case #6 – Radio Frequency Identification Tags (RFID tags) Over AMI Network

The purpose of this lab test was to evaluate the ability of a Third-Party Vendor using an IoT router to establish communication and command of RFID devices over the AMI network.

Several tests were performed to evaluate the capability of remotely performing various functions on the RFID devices. For this test, PG&E used two different RFID readers. Results from the lab test are summarized in Table 6. Test results demonstrated the ability of using an IoT router to establish communication and command of RFID devices over the AMI network.

Table 6: Lab Test Results for Use Case #6

Functionality Test	Result
Demonstrate the capability to read information from RFID Reader 1	Pass
Demonstrate the capability to read information from RFID Reader 2	Pass
Demonstrate the capability to observe the radio transmission power and radio state of RFID Reader 1	Pass
Demonstrate the capability to observe the radio transmission power and radio state of RFID Reader 2	Pass
Demonstrate the capability to manage the firmware of RFID Reader 1	The EPIC 2.26 Server does not support firmware updates
Demonstrate the capability to manage the firmware of RFID Reader 2	The EPIC 2.26 Server does not support firmware updates
Demonstrate the capability to monitor RFID Tag location for RFID Reader 1	Pass
Demonstrate the capability to monitor RFID Tag location for RFID Reader 2	Pass

In the above tests, at least one of the RFID readers did not support running an RF survey, changing transmission power through LLRP or support firmware updates. In these cases, the tests were still a success as long as it was possible to perform these tests on the other RFID reader.

4.2.7. Use Case #7 – Direct Acquisition and Control Telemetry Solution Use Case

The purpose of this lab test was to evaluate the ability of a Third-Party Vendor using an IoT router to establish communication, command and control of a distribution connected generator over the AMI network and demonstrate operational communications to the distribution connected generator.

Several tests were performed to demonstrate telemetry and control of the site controller device using distribution SCADA software. For this demonstration, PG&E used a fuel cell site controller. Results from the lab test are summarized in Table 7. Lab test results demonstrate the ability of using an IoT router to establish communication, command and control of a distribution connected generator over the AMI network.

Table 7: Lab Test Results for Use Case #7

Functionality Test	Result
Demonstrate the capability of SCADA to read the telemetry points (3-ph voltages (phase-to-phase; line-to-line), 3-ph current, active and reactive power, fuel cell simulator status) of the customer site controller	Pass
Demonstrate the capability of SCADA to execute the control points of the customer site controller	Pass

4.3. Task 3: Field Testing of Use Cases

Several tests were performed in the field to evaluate the performance of the use cases. High-level connectivity tests involved testing the performance between the EPIC 2.26 Server and the IoT router. These tests did not involve any interaction with the end devices. Specific tests were also performed to test the capability and performance of specific functions in each use case. This section presents the results of the high-level connectivity tests followed by those from the use case-specific functional tests.

4.3.1. Use Case-Specific Connectivity Testing

The use case-specific connectivity testing involved both testing the network for connectivity, as well as performance.

The following tests were performed to verify connectivity:

- Configuring an AP and IoT Routers to connect with the CD03 test environment Server on the AMI Network. The IoT-Routers are directly connected with AP using single hop-count connection.
- Validating the AMI Network connectivity with the EPIC Server.
- Validating End-to-End communication connectivity between EPIC Server Head-End and IoT Routers in the Field.
- Validating AP was properly configured to communicate with the IOT router.
- Validating IEEE2030 Server is configured to communicate with the AP.
- Validating the IEEE 2030 Server is configured to communicate with VPC.
- Validating multi-port switches Unit effectively communicates with IOT router (seamless handover).

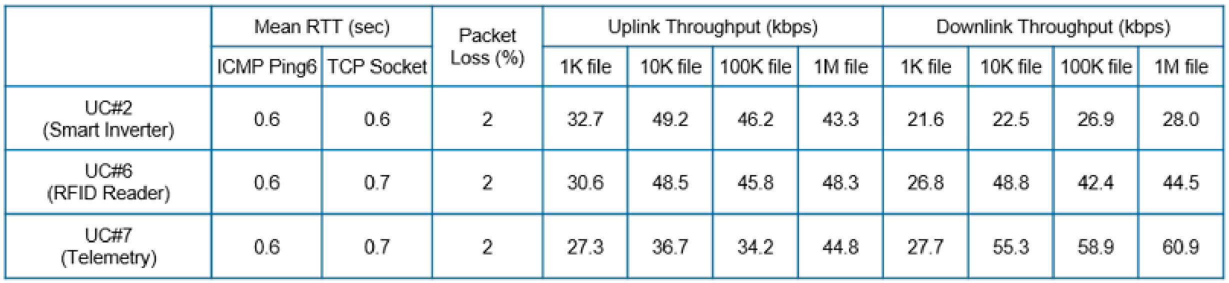
The performance of the communication network was tested for each use case using performance indices roundtrip time, packet loss and throughput. A brief description of each index is provided below.

- Round-trip-time (sec): The length of time it takes for a packet of information to travel from the source to destination and back.
- Packet Loss (%): The packets of data travelling across the network fail to reach destination. It is measured as a percentage of packets lost with respect to packets sent.
- Throughput: A typical method of performing a measurement is to transfer a ‘large’ file from one system to another system and measure the time required to complete the transfer the file. The unit of throughput is bit per second.

Two latency tests were performed to measure the latency on the Network Layer and Transport Layer. The packet loss and network throughput were measured to verify communication paths worked as expected. The first latency test was intended to transmit Internet Control Message Protocol version 6 packets from the EPIC 2.26 Server to the IoT router via an AP and return in round trip. The second latency test involved the same communication path; transmitting application layer IPv6 packets over Transmission Control Protocol. End-to-end application layer network uplink and downlink throughput was measured with four different payload sizes (1K – 1024 Bytes, 10K, 100K, 1M) using the same communication path.

Table 8 shows the results from the connectivity test for all the use cases.

Table 8: Field Test Results for Connectivity Testing



	Mean RTT (sec)		Packet Loss (%)	Uplink Throughput (kbps)				Downlink Throughput (kbps)			
	ICMP Ping6	TCP Socket		1K file	10K file	100K file	1M file	1K file	10K file	100K file	1M file
UC#2 (Smart Inverter)	0.6	0.6	2	32.7	49.2	46.2	43.3	21.6	22.5	26.9	28.0
UC#6 (RFID Reader)	0.6	0.7	2	30.6	48.5	45.8	48.3	26.8	48.8	42.4	44.5
UC#7 (Telemetry)	0.6	0.7	2	27.3	36.7	34.2	44.8	27.7	55.3	58.9	60.9

Note: Test performed in the CD03 AMI Environment with single hop-count between AP and IoT-Router.

4.3.2. Use Case #2: Solar Smart Inverter

The purpose of the field test was to evaluate the ability of a Third-Party Vendor using an IoT router to establish communication, command and control of a Smart Inverter over the AMI network and demonstrate operational communications to the Smart Inverter.

As with the lab test, the capability to remotely perform the functions given in Table 9 were evaluated for the two smart inverters. Test results demonstrate the ability of using an IoT router to establish communication, command and control of a Smart Inverter over the AMI network.

Table 9: Field Test Results for Use Case #2

Functionality Test	Result
Demonstrate the capability to schedule reactive power dispatch; 15 minutes prior to action	Pass
Demonstrate the capability to schedule real power curtailment; 15 minutes prior to action	Pass
Demonstrate the capability to change control points for Volt-Watt curve of the smart inverter	Pass for only one Inverter*
Demonstrate the capability to change control points for Volt-VAR curve of the smart inverter	Pass
Demonstrate the capability to gather the metering information such as AC Voltage, AC Current, reactive power, active power, frequency, apparent power and DC power.	Pass
Demonstrate the capability to synchronize the Smart Inverter's internal clock with the AMI network's clock	Pass
Demonstrate the capability to receive diagnostic codes, error codes, and/or alarms from Smart Inverter over AMI network	Pass
Demonstrate the capability to perform firmware upgrades	The EPIC 2.26 Server does not support firmware updates

* The IoT Router communicates to the Smart Inverter via Modbus. One of the Smart Inverters did not support changing the voltage control curves through the Modbus interface, so this test was not conducted.

4.3.3. Use Case #6: Radio Frequency Identification Tags (RFID tags) Over AMI Network

The purpose of the field tests is twofold: 1) to evaluate the capability of PG&E software, using IoT routers to establish communication and command of RFID devices over the AMI network, 2) to evaluate RFID technology and hardware to accurately track meter inventory movements within the San Jose Cinnabar Service Center. Test results demonstrate the ability of using an IoT router over the AMI network for this purpose.

Table 10: Field Test Results for Use Case #7

Functionality Test	Result
Demonstrate the capability to support multiple RFID Readers on a single IoT router	Pass
Demonstrate the capability to observe the radio transmission power and radio state of the RFID Reader	Pass
Demonstrate the capability to seamlessly transfer data between RFID readers and IEEE Server	Pass
Demonstrate the capability to differentiate between types of tags on any reader	Pass
Demonstrate the capability to command RFID readers from two vendors	Pass
Demonstrate the capability to track pallet tags accurately and autonomously when placed and removed from Cinnabar's receiving area	Pass
Demonstrate the capability to track meter individually accurately and autonomously when placed and removed from Cinnabar's stock room	Pass
Demonstrate the capability to track full pallets of meters accurately and autonomously when entering and exiting the Cinnabar Gates 1,2 and 4	Pass
Demonstrate the capability to track individual meters accurately and autonomously when placed and removed from PG&E gas & electric service trucks	Pass
Demonstrate the capability to track meters accurately and autonomously using a handheld reader	Pass
Demonstrate the capability of DC meter truck and Counting Logic Rules	Pass
Demonstrate the capability of tracking and recording DC truck assets	Pass

4.3.4. Use Case #7: Direct Acquisition and Control Telemetry Solution

The purpose of this field test was to evaluate the ability of a Third-Party Vendor using an IoT router to establish communication, command and control of a distribution connected generator over the AMI network and demonstrate operational communications to the distribution connected generator.

The results of the use Case #7, #7a and #7b field tests are shown in Table 11-Table 13. The results demonstrate the ability of a Third-Party Vendor using an IoT router to establish communication, command and control of a distribution connected generator over the AMI network.

Table 11: Field Test Results for Use Case #7

Functionality Test	Result
Demonstrate the capability of RT SCADA to read the telemetry points (3-ph voltages (phase-to-phase; line-to-line), 3-ph current, active and reactive power, fuel cell simulator status) of the site controller	Pass
Demonstrate the capability of RT SCADA to execute the control points of the site controller	Pass

Table 12: Test Results for UC #7a

Functionality Test	Result
Demonstrate the capability of RT SCADA to read the telemetry points (3-ph voltages (phase-to-phase; line-to-line), 3-ph current, active and reactive power) of the fuel cell site controller and meter	Pass

In the telemetry control verification test, execution latency was measured as the time interval between sending the command in SCADA and the device's physical response. Measurements were collected at the site controller and SCADA system as shown in Table 13.

Table 13: Latency Test for Use Case #7

Total Time (Seconds) = SCADA Master refresh time + AMI network roundtrip latency (0.6 Sec.) + controller's processing time

	One-way Latency (Seconds)				Round-trip Latency (Seconds)			
Control Point	Mean	Median	Max	Min	Mean	Median	Max	Min
Turn Off	6.80	5.75	12.00	4.50	18.55	17.00	24.00	14.50
Turn On	15.60	15.50	20.00	14.00	38.78	39.25	58.50	27.00

As a comparison with the SCADA latency information in Section 4.2.2. Use Case-Specific Connectivity Testing, the latency information in Table 13 appear to have a shorter latency.

4.4. Cybersecurity Evaluation

Cybersecurity attacks on AMI systems could potentially result in unauthorized access to systems, denial of service, propagation of malware, control system malfunction and loss of billing and customer data. These attacks can originate from external and internal sources. Cybersecurity penetration tests were performed to identify potential risks and mitigation strategies. The penetration tests were performed both at the product-level, as well as the site-level. The product-level assessments included hardware and system-level penetration tests, communication protocol assessment, web user interface assessment and API assessment. The site-level assessments were performed by a third-party vendor within the designated PG&E Lab with no access to Production Systems and/or data.

During the assessment, the Vendor was able to intercept the communication between the IoT Router and the PG&E backhaul Server because the IoT router was a development device and was not intended for production deployment. The assessment also identified the use of weak account passwords, password reuse across multiple devices and static encryption keys. Because of these application design and hardening practices, the Vendor was able to intercept communication traffic, decrypt SSL encrypted communications, and submit malicious data to the PG&E backhaul.

However, the Vendor was unable to compromise the PG&E backhaul Server or establish pivot access from one IoT Router to another, limiting the scope of impact resulting from a successful compromise. The assessment also showed some positive security practices; SSL certificate validation performed by both the IoT router and the PG&E backhaul Server; and wireless device isolation, where the IoT routers were unable to communicate between each other. However, some of these positive practices may have been a direct result of the limited functionality contained within the development environment.

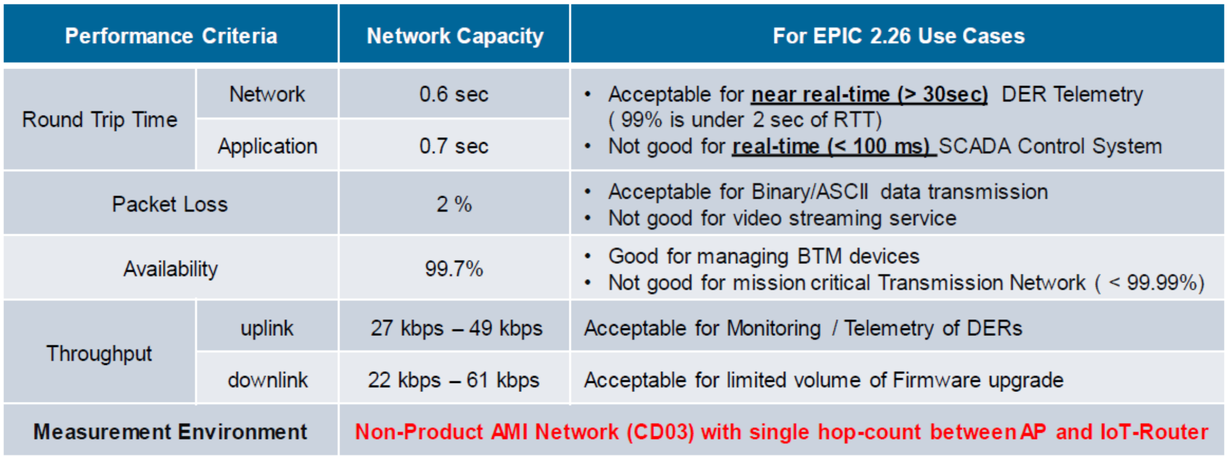
It is recommended that the infrastructure cybersecurity for the EPIC 2.26 solution be properly hardened by leveraging secure-boot functionality, device encryption and a strong password complexity policy. The cybersecurity for the systems between PG&E cloud and headend server was hardened.

4.5. Network Performance

Communication networks provide necessary infrastructure allowing PG&E to manage open architecture devices from a central location. In the smart grid, heterogeneous communication technologies and architectures are involved. Communication networks should meet specific requirements, i.e., bandwidth, reliability, and security, depending on smart grid applications. The complexity of use cases may lead to difficulties in choosing appropriate communications networks as many parameters and different requirements must be considered depending on applications and PG&E expectations.

Network performance was evaluated in the non-product (CD03) AMI environment with single-hop mesh connectivity between the AP and the IoT router. From a network latency perspective, the non-production AMI network can support data polling every 30 seconds. These results are summarized in Table 14.

Table 14: Network Performance Test Results in a Single-Hop Environment



Performance Criteria		Network Capacity	For EPIC 2.26 Use Cases
Round Trip Time	Network	0.6 sec	• Acceptable for near real-time (> 30sec) DER Telemetry (99% is under 2 sec of RTT) • Not good for real-time (< 100 ms) SCADA Control System
	Application	0.7 sec	
Packet Loss		2 %	• Acceptable for Binary/ASCII data transmission • Not good for video streaming service
Availability		99.7%	• Good for managing BTM devices • Not good for mission critical Transmission Network (< 99.99%)
Throughput	uplink	27 kbps – 49 kbps	Acceptable for Monitoring / Telemetry of DERs
	downlink	22 kbps – 61 kbps	Acceptable for limited volume of Firmware upgrade
Measurement Environment		Non-Product AMI Network (CD03) with single hop-count between AP and IoT-Router	

4.6. Recommendations from the Lab and Field Tests

The lab and field test results demonstrated the ability of using an IoT router to command and control various third-party end devices such as smart inverters, sensors, SCADA devices, RFID readers and DG controls over the AMI network using the IEEE 2030.5 protocol. General finding and recommendations are discussed first followed by use case specific findings and recommendations.

Client-Server Architecture

- To improve reliability, the Server should be deployed across multiple nodes for redundancy and to enable scaling by adding new processing nodes. While this can be easily implemented using the existing architecture, some development work such as the development of messaging queues will be required.
- In order to prepare both the EPIC 2.26 Server and Client for production deployment and ongoing maintenance, additional automated unit and regression testing should be developed to increase code coverage. This will require the development of test code to mock individual end devices and simulate AMI network performance since testing with real devices on a real AMI network may not be feasible.
- Load testing needs to be performed on both the EPIC 2.26 Server and Client to determine their capacities at different levels of activity of the various use cases.
- Currently, several Client functions such as frequency of connection with end devices are governed locally in the Client configuration. In a production environment, the ability of the Server to directly manage and control these Client functions will be necessary.
- The production system should have the capability to differentiate the AMI traffic from metering and those from non-metering use cases, as well as help optimize and coordinate the traffic to improve performance and prevent congestion.

Cybersecurity

- PG&E to ensure the production design of the IoT Router platform is properly hardened leveraging secure-boot functionality, device encryption and a strong password complexity policy. The cybersecurity deficiencies identified in the vendors report should be addressed.

Network Performance

- The field communication performance tests were only performed in a single-hop environment. The performance of the network in a production environment should be tested and compared with the performance tests in this report.

Use Case #2 – Solar Smart Inverter

- Both lab and field tests were conducted using two specific models (and firmware versions) of smart inverter. It is recommended that more testing be conducted with additional smart inverters to improve the Client support.
- The as-built user interface mimics the IEEE 2030.5 specification where DER Programs are set by start date, start time, and duration. It is expected that for a production version, a UI that supports calendar-based approach with repeating schedules would be required.

- Due to limitations in the smart inverters, end-to-end testing of smart inverter firmware updates were not performed. It is recommended that this testing be revisited after specific vendor's inverters allow such firmware updates to be performed.

Use Case #3 – Sensors

- The development and testing were focused on reporting all data from a remote sensor in real time. It is recommended that in a production deployment, Client modification be made such that data is recorded locally and only reported when a specific event is detected. This would significantly reduce the bandwidth consumed for transmitting data that is not essential.
- The current data retrieval is based on Server polling which is not ideal for real-time data transfer. If a real-time monitoring capability is required in production, it is recommended that the Client push data to the Server on a faster schedule over a short period of time.
- For a production rollout, it is recommended that the support for additional, specific sensor types be added.

Use Case #5 – Distribution Automation/SCADA Overhead and Underground Intelligent Electric Devices (IED)

- Lab testing revealed that offline devices were slow to respond and could affect message performance for other devices on a shared DNP3 Server channel. For a production environment, it is recommended that AMI network design be made to achieve a single hop and ensure 0.6 Seconds latency in AMI network.
- It is recommended that additional field testing be performed for all end device types including end devices in remote environments.

Use Case #6 – Radio Frequency Identification Tags (RFID tags) Over AMI Network

- Currently, material handlers conduct a visual cycle count of meter inventory and document their findings in the SAP inventory system on a weekly basis. It is recommended that in a production deployment, these processes be replaced with formalized API integrations with each data source.
- It is recommended that improvements be made to antenna coverage, data processing time, yard configuration, and tag size and reader performance at certain environmental conditions such as high temperature.
- In the development environment, much of the business logic was encapsulated in a runtime-editable script that is cumbersome for an end user to modify. It is recommended that the script be replaced with a user interface that is more easily updated by the end user.
- It is recommended that the Client data be augmented with Global Positioning System data if more real time and accurate locational information is required for mobile assets such as trucks.
- It is recommended that for mobile assets expected to travel outside the AMI network's range, a commercial cellular alternative be integrated with the EPIC 2.26 Client.

Use Case #7 – Direct Acquisition and Control Telemetry Solution

- It is recommended that the DER Programs be broken into DER Class (See Table of Acronyms) and AMI network be designed to support each class accordingly.

  Also, latency requirements are developed for each DER Class. For example, a DER class needing a faster response will have an AMI network collection equipment installed at the site to allow on hop communication to minimize the latency to less than 1 second. Some other DER classes not needing fast response will not have an AMI network collection installed at the site and can mesh into the existing network. In such cases, the latency is expected to be greater than 1 second.

4.7. Key Next Steps

Performing Network Tests in a Production Environment

As previously mentioned, the field tests were performed in the CD03 test environment with a single hop between the end device and the IoT router. The performance in a production environment should be tested for applicable cases. Latency, packet loss, throughput and reliability will need to be measured and compared with the use case requirements before scaling this solution further.

Production Demonstration for Use Case #6

Since Use Case #6 is non-reliability related and has potential for immediate cost savings, a demonstration should follow using number of yards to refine the to be process, develop lessons-learned, and understand how to use the data being generated for long term operational benefits. Specific changes to the end device performance, yard configuration, business logic software and SAP integration recommended from the lab and field tests should first be implemented.

Knowledge Transfer Plan

A primary benefit of the EPIC program is the technology and knowledge sharing that occurs both internally within PG&E and across the other investor-owned utilities, the CEC and the industry. To facilitate this knowledge, PG&E will share the results of this project in industry workshops and through public reports published on the PG&E website. Specifically, below are information-sharing forums where the results and lessons from this EPIC project were presented or are planned to be presented:
Information Sharing Forums Planned

- DistribuTECH 2019-2021
- EEI Conference 2019-2021
- Utility Benchmarking Meetings – Southern California Electric Company (SCE) and San Diego Gas & Electric Company (SDG&E) working group (2019-2021)

5. Value proposition

The purpose of EPIC funding is to support investments in TD&D projects that benefit the electricity customers of PG&E, SDG&E, and SCE. Project 2.26, *Customer and Distribution Automation Open Architecture Devices* has demonstrated the possibility and practicality of using the existing AMI infrastructure for monitoring and controlling various distribution assets including smart inverters, DERs, earth quake sensors, as well as telemetry.

5.1. Primary Principles

The primary principles of EPIC are to invest in technologies and approaches that provide benefits to electric ratepayers by promoting greater reliability, lower costs, and increased safety. This EPIC project contributes to these primary principles in the following ways:

- Greater reliability: This project demonstrated the ability of using the AMI (mesh) network for communicating with SCADA and other electric distribution IEDs. A mesh network is more reliable than a non-mesh network because when one node is inoperable, other nodes can still communicate with each other directly or through intermediate nodes. In addition, the PG&E's AMI network covers 99.5% of the PG&E electric service territory while the major telecom companies in California provide between 66% and 81% of 4G coverage. The use the AMI mesh network for electric communications with distribution IEDs (including SCADA) provides wider, more reliable system coverage which in turn will improve electric system reliability.
- Lower costs: This project identified various opportunities to reduce costs. These include the following:
    - Potential of reduced communication costs by using AMI for telemetry rather than the various communication technologies currently used;
    - Ability to identify and respond to events more quickly, thus reducing outage and restoration costs;
    - Ability to interconnect DERs as a low-cost solution; and
    - Reduced inventory costs by improved tracking and identification of assets in the field.

5.2. Secondary Principles

EPIC also has a set of complementary secondary principles. This EPIC project contributes to one of the secondary principles: efficient use of ratepayer funds.

- Efficient use of ratepayer funds: The use of the existing PG&E AMI mesh network for electric distribution system communications could reduce the need for the various third-party communications currently used. This would increase the use of an existing PG&E asset and reduce the communication costs currently paid to third party communications companies.

6. Accomplishments and Recommendations

The following summarize some of the key accomplishments of the project over its duration:

6.1. Key Accomplishments

This project achieved the following key accomplishments:

- Developed the solution architecture that defined the hardware, software, communications equipment, communication standards and protocols for secure control of various end devices using the AMI infrastructure including;
  - Successfully integrated IPv6 traffic through the AMI Network and into the PGE AWS. This was a first in handling IPv6 within PG&E
  - Successfully hardened Cybersecurity between systems from PG&E cloud to headend server
  - Successfully integrated data traffic between the AWS Cloud and distribution SCADA and SCADA -Master
- Developed the EPIC 2.26 Client and Server software and the IEEE 2030.5 interface that allows for maximum control of data flow over the AMI network
- Successfully demonstrated in laboratory and field tests, the ability to communicate with and control PG&E and third-party devices in five use cases. These use cases involved Smart Inverters, Distribution Automation, sensors, SCADA and other distribution IEDs, RFID equipment, and Control Telemetry
- Established two-way communications with smarter inverters using IEEE 2030.5 protocol and demonstrated the capability to schedule reactive power dispatch and real power curtailment, change control points, gather metering information and synchronize the smart inverter clock with the AMI network clock (Use case #2)
- Demonstrated the capability of the AMI network to communicate with 3 different distribution controllers – a capacitor bank controller, a line recloser controller and a subsurface switch controller. (Use case #5)
- Established two –way AMI communications with two different RFID readers and demonstrated the capability to read information for the RFID, observe the radio transmission power and radio state and monitor the RFID tag location (Use case #6)
- Established two-way AMI communication with DG controller using IEEE 2030.5 and DNP3 protocols and demonstrated end-to-end (SCADA system to DG controller) telemetry data collection and controls execution (Use case #7)

6.2. Key Recommendations

EPIC 2.26 was successful in demonstrating that PG&E's AMI network can be leveraged for these additional use cases and is suitable for connecting and transmitting data from customer and utility devices. The interface with the device in each use case was tested and demonstrated as working and operational.

The key to transitioning the EPIC 2.26 project from demonstration to production scale will be operational readiness, further definition of maintenance and operations work, and budget funding for each use case.

PG&E recommendation to the industry is that other utilities seeking to explore similar work will need to consider this prioritization. As while this EPIC 2.26 Project proved these use cases can be feasible, how the AMI network is used needs to be prioritized just like any other RF networks.

Customers and utilities can utilize its AMI network as an information highway to transfer data and information. The solutions developed in this Project can be benchmarked and expanded to other utilities.

7. Data Access

Data Access Upon request, PG&E will provide access to data collected that is consistent with the CPUC's data access requirements for EPIC data and results.

8. Intellectual Property

Because of the ground-breaking nature of the EPIC 2.26 Customer and Distribution Automation Open Architecture Devices Project, as well as the cost savings potentially achieved in leveraging the AMI network and providing a new solution for connecting new devices using open architecture standard protocols, a final patent application was filed with the US Patent Office. The “Application of Resource Meter System and Method” (Application Number 16143295) outlines the first of its kind solution using AMI network for monitoring, commanding, and controlling edge devices under EPIC 2.26.

PG&E looks forward to working with the other California utilities, and the industry at large, to realize the benefits of this approach. This intellectual property is owned and held by PG&E, and can be commercialized for the company’s commercial benefit, in accordance with all appropriate laws and regulations (including Decision D.13-11.025).

With this EPIC final report, which is required by the CPUC, PG&E and its subsidiaries do not undermine, waive or relinquish any ownership, title, exclusivity or any intellectual property or proprietary rights, of claims made by PG&E or its subsidiaries with respect to such AMI network connection method to utility and customer devices using open architecture standard protocols in the EPIC 2.26 Customer and Distribution Automation Open Architecture Devices Project.

9. Metrics

List of Proposed Metrics and Potential Areas of Measurement (as applicable to a specific project or investment area)	***Reference***
3. Economic benefits	
a. Maintain / Reduce operations and maintenance costs	Section 5.1(b)
b. Maintain / Reduce capital costs	Section 5.1(b)
5. Safety, Power Quality, and Reliability (Equipment, Electricity System)	
d. Public safety improvement and hazard exposure reduction	Section 5.1(c)
i. Increase in the number of nodes in the power system at monitoring points	Section 5.1(a)
7. Identification of barriers or issues resolved that prevented widespread deployment of technology or strategy	
j. Provide consumers with timely information and control options (PU Code § 8360)	Section 6.1

10. Conclusions

The PG&E AMI network covers 99.5% of the PG&E electric service territory while state telecom companies have up to 81% 4G coverage. This gives PG&E as well as third parties reach into PG&E customers and customer-connected devices that do not have cellular of other forms communication. Currently the AMI network is used exclusively for PG&E needs and applications. However, it may be possible to accommodate future non-AMI applications as well. It is estimated the AMI network is now operating at approximately 20% capacity. The AMI asset is a scaled resource and can grow to match the demand. This available network capacity along with its large system-wide footprint provide utilities with a cost-effective alternative to other vendor-provided communications currently used.

The EPIC 2.26, *Customer and Distribution Automation Open Architecture Devices* project successfully demonstrated the ability of a Client-Server architecture consisting on an IoT router to establish communication, monitoring, command and control of various third-party end devices such as smart inverters, sensors, SCADA devices, RFID readers and DG controls over the AMI network using the IEEE 2030.5 protocol. A cloud-based Client-Server architecture using the IEEE 2030.5 protocol, APIs for the command and control of various end devices and protocol adapters to communicate with a multitude of end devices were developed as a part of this project. Lab tests for five use cases and field tests for three use cases were also successfully completed. PG&E was able to successfully connect to, monitor, communicate with, and control these devices during the use case evaluations. This project demonstrated the ability to use PG&E's AMI mesh network as a communication medium for electric distribution equipment and devices. It is worth mentioning that this Client-Server solution can be adapted to operate over any available network (AMI, LTE, 5G, Wi-Fi) that a utility may have in their service territory. This solution will facilitate inter utility resource sharing, grid monitoring and DER management. This Client and Server solution will ease the interoperability, interconnection and regional infrastructure management.

The project demonstrated the ease of installing or interconnecting devices to the AMI network and could ultimately reduce equipment installation costs. It could also reduce operation costs, especially cellular telecommunications costs by reducing the need for vendor communication systems. The AMI mesh network has redundancy and is more reliable than current communication being used. This increased reliability will improve the ability to collect data from field devices, identify problems or incidents more quickly and improve response to events. This improved response time will reduce outage times and improve public safety.

Cybersecurity penetration tests were performed to identify potential risks and mitigation strategies at the product-level, as well as the site-level. These tests showed the need for properly hardened infrastructure leveraging secure-boot functionality, device encryption and a strong password complexity policy. The cybersecurity for the systems between PG&E cloud and headend server was hardened and resolved.

Network performance performed by PG&E also showed that the latency requirements of the use cases could be met in a single-hop environment. The latency requirements for DER telemetry and SCADA use cases can be met with a single hop by designing the AMI network and having a few endpoints transmit data directly a network node, as described further in the following:

- DER telemetry: Depending on the DER Class (see Table of Acronyms), various latency requirements can be determined and applied (e.g. slower latency for DER Class 2), and the AMI network design can be done accordingly.
- SCADA Use: SCADA over AMI solution can potentially be a complementary solution to SCADA in areas that other SCADA solutions are not available.

The AMI network has additional bandwidth available and can be used for other purposes beyond billing. The project demonstrated the ease of installing or interconnecting devices to the AMI network and could ultimately reduce equipment installation costs. Since the AMI network coverage is 99.5% of PG&E's service territory, it is seen as a reliable, lower cost network solution, specifically, network capital spending, maintenance operation spending, and especially telecommunications costs. The AMI mesh network has redundancy, and therefore may improve the ability to monitor field devices, identify problems or incidents more quickly and improve response time to events.