Pacific Gas and Electric Company

EPIC Final Report

Program	***Electric Program Investment Charge (EPIC)***
Project	***EPIC 3.03 – Distributed Energy Resource Management System (DERMS) and Advanced Distribution Management System (ADMS) Advanced Functionality***
Reference Name	*EPIC 3.03 - DER Headend System*
Department	*Grid Research Innovation & Development*
Project Sponsor	Quinn Nakayama
Project Business Lead	Omid Sarvian
Contact Info	EPIC_Info@pge.com
Date	April 10, 2023
Version Type	*Final*
Version	[Version 2]

Table of Contents

List of Tables

List of Figures

Table of Acronyms

PG&E	Pacific Gas & Electric
AB	Assembly Bill
API	Application Programming Interface
APN	Access Point Name
AVPN	AT&T VPN
BLR	Blue Lake Rancheria
BTM	Behind-the-Meter
CALSSA	California Solar and Storage Association
CEC	California Energy Commission

COT	Customer-Owned Telemetry
CPUC	California Public Utilities Commission
CPUC ED	CPUC Energy Division
CSIP	Common Smart Inverter Profile
CT	Current Transformer
DIDF	Distribution Investment Deferral Framework
DIH	Distribution Interconnection Handbook
DMS	Distribution Management System
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol 3
EGI	Electric Grid Interconnection
EMS	Energy Management System
FAN	Field Area Network
FAT	Factory Acceptance Testing
FSA	Function Set Assignment
GHG	Green House Gas
GIS	Geographic Information Systems
IAM	Identity and Access Management
ICA	Integrated Capacity Analysis
ICBP	Interconnection Best Practices
IGP	Integrated Grid Platform
IP	Internet Protocol
LAN	Local Area Network
LBE	Load-Balancing Edge
LFDI	Long Form Device Identifier
LGP	Limited Generation Profile
MPLS	Multiprotocol Label Switching
MUP	Mirror Usage Point
NEM	Net Energy Metering
NIST	National Institute of Standards and Technology
NWA	Non-Wires Alternative
ODN	Operational Data Network
OIR	Order Instituting Rulemaking
PCC	Point of Common Coupling
PCS	Power Control System
PKI	Public Key Infrastructure
PSPS	Public Safety Power Shutoff
PT	Potential Transformer
PTO	Permission to Operate
R21	Rule 21
RFP	Request for Proposal

RPS	Renewable Portfolio Standard
RSG	Remote Site Gateway
RSRQ	Referenced Signal Received Quality
RTU	Remote Terminal Unit
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDG&E	San Diego Gas and Electric
SFDI	Short Form Device Identifier
SIM	Subscriber Identity Module
SIOWG	Smart Inverter Operationalization Working Group
SOW	Statement of Work
SSL	Secure Socket Layer
TD&D	Technology Demonstration and Deployment
TLS	Transport Layer Security
UDN	User Data Network
VPN	Virtual Private Network

1 Executive Summary

This report summarizes the project objectives, technical results and lessons learned for EPIC Project 3.03 DER Headend System, also referred to as the EPIC 3.03 - Distributed Energy Resource Management System (DERMS) and Advanced Distribution Management System (ADMS), as listed in the EPIC Annual Report. The project was authorized June 2019 and concluded December 2022.

1.1 DER Headend Project Context

California is a leader in the growth of Distributed Energy Resources (DERs) including solar, battery energy storage, electric vehicles (EVs), and load controlled by demand response (DR) programs. This progress is driven by a confluence of technology advancements, consumer preferences, and complementary legislative and regulatory actions that have propelled solar, battery energy storage, and EV adoption within California.

PG&E's vision of the future electric grid is a secure, resilient, reliable, and affordable platform that enables continued gains for clean-energy technologies and California's economy in a way that provides maximum flexibility and value for customers. However, while DERs help achieve California's clean energy objectives, they can potentially create new challenges including capacity (thermal) constraints, power quality issues (inclusive of voltage violations), and adverse impacts on protection systems due to bidirectional power flow[1,2]. Furthermore, hosting capacity (e.g. available grid capacity to safely and reliably interconnect additional DERs) is decreasing, thus reducing the overall flexibility of the grid to handle more DERs without infrastructure improvements.

Significant grid modernization investments are required to operate in this new paradigm while achieving the state's ambitious clean energy goals. To address these issues, PG&E is developing an Integrated Grid Platform (IGP) that improves situational awareness, operational efficiency, and enhances cybersecurity to meet today's challenges while positioning PG&E to meet the demands of a dynamic energy future. This platform will provide the required tools and capabilities to maintain grid safety, reliability, and affordability through efficient grid management. It will develop foundational systems to enhance situational awareness, modeling, forecasting, and visibility, from which more advanced applications such as a Distributed Energy Resources Management System (DERMS) can be built to safely address both DER and non-DER related grid issues by coordinating, optimizing, and dispatching assets cost-efficiently.

A DERMS, combined with a system of new grid management tools including an Advanced Distribution Management System (ADMS), will enable the utility to leverage DERs for grid and local reliability benefits, realize value from DERs, and potential distribution investment deferral. Standardized, cost-efficient and reliable communications between DERs and PG&E are foundational to the rollout of a future DERMS and the overarching purpose of this project. Developing the default Common Smart Inverter Profile (CSIP) IEEE 2030.5 communications protocol[3] and standard will improve the cost effectiveness of communications and coordination between utilities and interconnected DER customers. The lower cost of communication systems will in turn lower barriers to the installation of more DERs and, when coupled with the future DERMS and ADMS systems, will enable customers to supply the grid with more renewable energy in a safe and efficient way.

1.2 DER Headend System Overview

Larger generators (1 Megawatt (MW) or greater) that interconnect to PG&E's distribution grid are required to provide telemetry (real-time power-related measurements) to PG&E's Distribution Control Center (DCC) in order to provide real-time visibility for consideration in grid operations per PG&E's Rule

[1] Emerging Issues and Challenges in Integrating Solar with the Distribution System: https://www.nrel.gov/docs/fy16osti/65331.pdf
[2] High-Penetration PV Integration Handbook for Distribution Engineers: https://www.nrel.gov/docs/fy16osti/63114.pdf
[3] Common Smart Inverter Profile, March 2018, Version 2.1.

21 (R21) tariff[4]. Prior to this project, PG&E installed either Mini Remote Terminal Units (Mini-RTUs) or Line Reclosers to fulfill the interconnection customer's telemetry requirement. PG&E installs, owns, and maintains these mini-RTUs and Line Reclosers which communicate over private communication lines using PG&E's SCADA network. The installation and cost of ownership charges resulted in a total cost of $50,000 - $150,000 for interconnecting generation customers. The cost of telemetry has been viewed as a barrier to adoption of DERs and there has been a desire across the industry to bring costs down significantly with a CPUC target of below $20,000 for utility-related costs.[5]

PG&E's EPIC 3.03 project set out to address the challenge of lowering telemetry costs for DER customers in a way that met the cost objectives, while also maintaining the reliability and integrity of PG&E's communications and operations systems and positioning the company to leverage DERs in new ways in the future. Toward this end, PG&E chose to deploy a production–ready CSIP-certified IEEE 2030.5 DER Headend Server (hereafter referred to as the "DER Headend Server") that would allow the marketplace of communications solutions to develop over time. The CSIP implementation of IEEE 2030.5 was chosen because it aligned with California's planned Smart Inverter Phase 2 Communications requirements[6] and because it supports PG&E cybersecurity's authentication requirements.

PG&E's DER Headend Server is one of the first of its kind deployed in the field for production use in the world. The system uses the CSIP implementation of the IEEE 2030.5 protocol over the public internet to communicate between the customer-owned devices or aggregation platforms and PG&E's DER Headend Server. Providing a Customer-Owned Telemetry (COT) solution was important to align with regulatory direction[7] and as a method to reduce costs. As a result of this project, PG&E now provides COT options, where customers can buy devices from one of multiple PG&E certified-interoperable vendors, with the goal of further reducing prices over time through vendor competition.

The COT solution is required to aggregate measurement data by DER type and transmit that data back to PG&E via a CSIP-certified IEEE 2030.5 device. For the first phase of the project, PG&E worked with vendors to develop a remote site gateway (RSG) to gather data from the site (generally from metering devices), translate that data from their native protocol (e.g. Modbus) to IEEE 2030.5, and then transmit that data over the public internet to PG&E (e.g. via a cell modem), as can be seen in Figure 1. RSGs are owned and maintained by the interconnecting customers and referred to as the COT option, where customers can buy RSGs from PG&E certified-interoperable vendors that have completed interoperability testing with PG&E systems. The goal of certifying multiple vendors is to promote competition for business to drive down prices further.

[4] Section J.5, PG&E Rule 21 Tariff

[5] Decision 19-03-013 Ordering Paragraph 9 issued April 5, 2019, would adopt proposal 1 after IOUs show the cost-effectiveness of telemetry and lower the threshold for telemetry to 250 kW or greater while instituting a cost-cap of $20,000 for estimated utility-related costs. This established the target price for low-cost telemetry.

[6] PG&E Electric Rule 21. (2018). HH.5.b.iv Smart Inverter Generating Facility Design and Operating Requirements, Communication Requirements.

[7] Resolution E-5038 Ordering Paragraph 2 required California IOUs to provide a customer-owned telemetry solution. PG&E designed the EPIC 3.03 solution with the discussions surrounding this ruling in mind, even though the final decision happened late in the timeline of the EPIC 3.03 project. This positioned PG&E well to be able to quickly comply with the ruling when it was enacted.

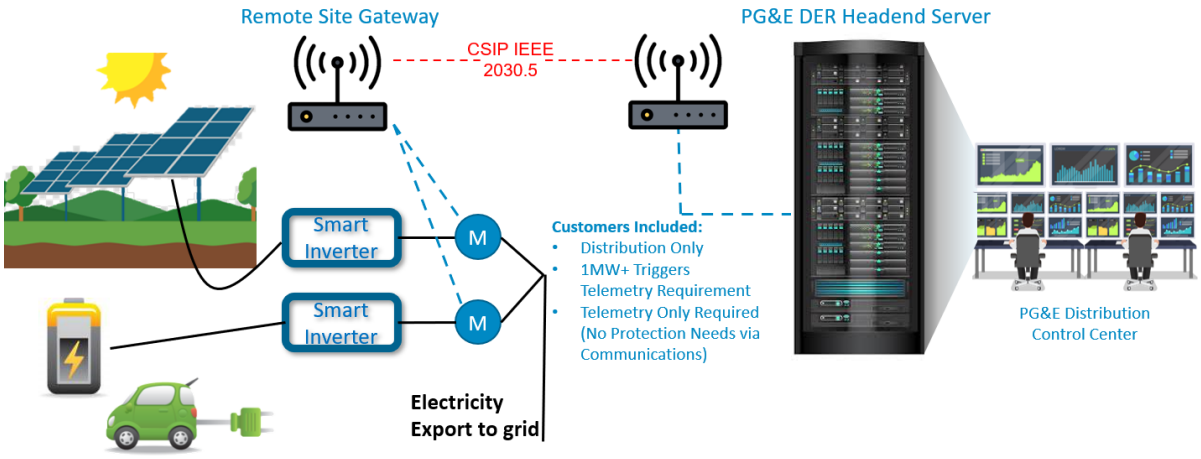


Figure 1: Simplified overview of the DER Headend System using a remote site gateway (RSG)

Following integration of the gateway solution, PG&E worked on enabling communications between the DER Headend and IEEE 2030.5 aggregators. As seen in Figure 2, the aggregator simply acts as a conduit between communications from the DER Headend Server and customer DERs. This can leverage existing communications between customer DERs and their developers and/or technology providers with the aggregator acting as the protocol translator to IEEE 2030.5 for the DER Headend server.

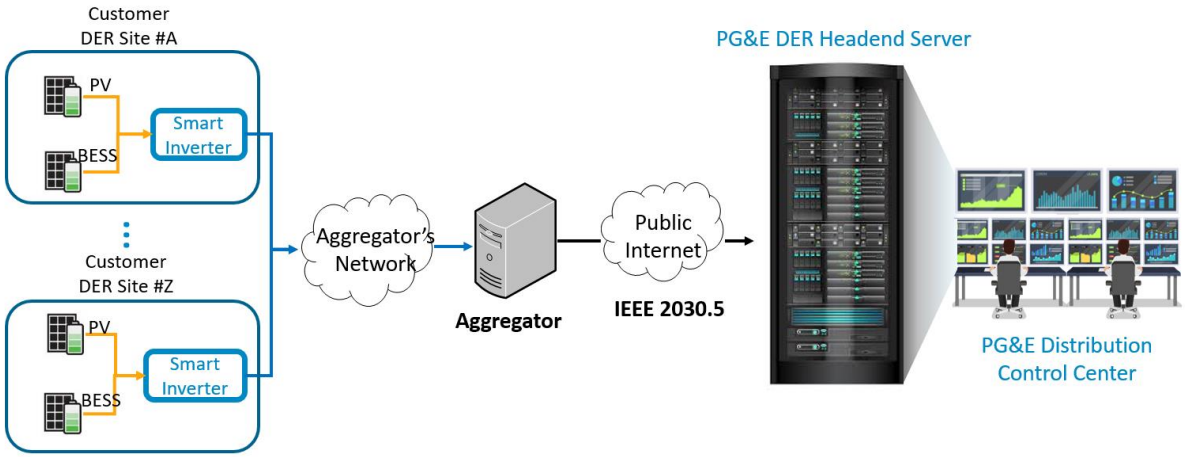


Figure 2: Simplified overview of the DER Headend System using an aggregator

In situations where there is no existing communication between the DER and the developer/technology provider then a potentially even lower cost gateway can be installed to communicate to the aggregator.

Beyond just telemetry, IEEE 2030.5 is seen as a foundational protocol for implementing more future-oriented DER management functions. DER management includes controlling DERs to avoid creating issues for the distribution grid or enable them to provide additional services to the grid. The EPIC 3.03 project tested a variety of control functions for DERs to evaluate off-the-shelf capabilities via IEEE 2030.5.

PG&E and the project partners overcame significant challenges in creating a pioneering IEEE 2030.5 production-ready ecosystem from a relatively new and untested protocol. Interoperability, cybersecurity, and cost-efficiency challenges were addressed through the progression of the project. The EPIC 3.03 project successfully developed a vendor-agnostic, cybersecure, and cost-efficient platform for customer-owned telemetry solutions, that provides immediate value to large interconnecting DER customers. While additional effort is required in advancing CSIP, IEEE 2030.5, and the vendor landscape, the foundational ecosystem that the EPIC 3.03 project created provides a launchpad for continuous development as the interactions between utilities and DERs continue to become more complex and more important.

1.3 Key Objectives & Accomplishments

The following summarizes the EPIC 3.03 – DER Headend project's key objectives and related accomplishments:

Objective 1: Build a cybersecure CSIP-certified IEEE 2030.5 DER Headend Server that is interoperable with customer-owned CSIP-certified gateways to fulfill the telemetry requirements of distribution interconnected DERs (1MW or greater).
Accomplishments:

- Worked with PG&E's existing supervisory control and data acquisition (SCADA) vendor to build a production IEEE 2030.5 server that is CSIP-certified to act as the DER Headend Server.
- Iteratively updated DER Headend Server to be interoperable with two separate remote site gateway vendors.
- Created a cybersecure architecture to allow PG&E to connect to third-party devices securely

Objective 2: Certify at least two CSIP-certified gateway vendors for interoperability with the DER Headend Server to provide a vendor-agnostic solution and customer options for purchase.
Accomplishments:

- Conducted an RFP to select two vendors to build CSIP-certified remote site gateways that are interoperable with the new DER Headend Server.
- Conducted extensive testing and development to resolve interoperability issues between the gateways and the DER Headend Server.
- Upon successful completion of interoperability testing, PG&E certified as interoperable two remote site gateway vendors and made them available for PG&E distribution interconnection customers.

Objective 3: Assess three CSIP-certified aggregator vendors' interoperability with the DER head-end server.
Accomplishments:

- Two different methods of an aggregator deployment were certified interoperable:
    1. Aggregator server installed within the existing communications network of a DER developer using licensed software of an aggregator vendor. This allowed that DER developer to use their existing network connection to their DERs to collect the metering data from the field and then provide that data to the utility via the IEEE 2030.5 aggregator connection.

2. Aggregator vendor deployed their own aggregator such that any interconnection customer could utilize it to fulfill their telemetry requirement. The aggregator vendor would have the DER customer install a gateway device (does not need to be an IEEE 2030.5 gateway device) at their site that communicates to their IEEE 2030.5 aggregator cloud server which then forwards that data using IEEE 2030.5 to PG&E's DER Headend Server.

- Of the three vendors providing cloud deployed aggregators, two have completed all testing on the IEEE 2030.5 QA Server and are certified-interoperable with the PG&E DER Headend Server. The third vendor is still in the process of testing on the QA Server.

Objective 4: Reduce the cost of telemetry to a target of below $20,000 for utility related costs.
Accomplishments:

- Reduced costs to where both utility and customer costs combined are projected to be under $20,000
- Reduced the scope of cybersecurity requirements for customers and the associated liability.
- Worked with vendors to reduce the cost of their remote site gateway systems.
- Worked with Public Key Infrastructure (PKI) organization to create a more affordable pricing structure for PKI certificates and implement a scalable model for future growth.
- Reduced the scope and cost of system requirements for customers, including:
    - Reassessing site Point of Common Coupling (PCC) metering requirements.
    - Right-sizing cybersecurity requirements to the nature of the risk by reducing the risk profile of these devices as connected to PG&E's network.

Objective 5: Integrate customer owned telemetry into the existing systems and processes for the Interconnection, Business Applications, and Operations teams.
Accomplishments:

- Updated interconnection customer portals, interconnection applications, and internal procedures to add customer-owned telemetry options to the interconnection process
- Created data connections among multiple backend and frontend software systems to integrate the data and make telemetry available to end users in the Distribution Control Center (DCC).
- Provided training and change management initiatives to ensure stakeholders could adopt new processes and access data appropriately
- Provided customers with guidance and updated documentation via the PG&E website and the Distribution Interconnection Handbook

Objective 6: Share learnings of the system with industry and stakeholders to strengthen standardization of IEEE 2030.5.
Accomplishments:

- Shared midterm learnings about challenges with interoperability with internal and external stakeholders, IOUs, and the CPUC.
- Presentation of the project at DistribuTech, EPRI conferences and seminars, Smart Inverter Working Group, CPUC, CEC EPIC Symposium, SunSpec and more.

Objective 7: Test control capabilities of the system.
Accomplishments:

- Tested control capabilities of the system using a lab smart inverter, a production gateway, and the test version of the DER Headend Server.

Objective 8: Assess whether this system can be used for remote grid applications.
Accomplishments:

- Reviewed the monitoring and control requirements of remote grids and because of the unique characteristics of a remote grid, PG&E determined that the CSIP-certified remote site gateways and the IEEE 2030.5 protocol were not the best suited option for this application.

Objective 9: Use learnings for integrating IEEE 2030.5 communications into the future DER Management System (DERMS) and Advanced Distribution Management System (ADMS).
Accomplishments:

- The EPIC project established an IEEE 2030.5 DER Headend server and multiple 2030.5 gateways and aggregators that are known to successfully communicate with each other. The certified-interoperable remote site gateways are being used as a baseline when testing the IEEE 2030.5 server in PG&E's new ADMS/DERMS vendor platform. This is important because it is known that CSIP Certification does not guarantee successful communication between servers and clients.
- The ADMS and DERMS projects are implementing IEEE 2030.5 using the lessons learned from EPIC 3.03 around cybersecurity and interoperability to create an architecture that securely integrates 3rd party devices and is tested to be interoperable between the EPIC 3.03 validated remote site gateways and the ADMS / DERMS CSIP certified servers. Using tested and certified-interoperable clients expedites testing and development of this future DER Headend System which will ultimately replace the system deployed within the EPIC 3.03 project.

Objective 10: Develop a process for new gateway or aggregator vendors to become PG&E certified-interoperable vendors.
Accomplishments:

- PG&E developed a process to assess new gateway or aggregator vendors at PG&E's ATS laboratory.

1.4 Key Takeaways

The following findings are the key takeaways and lessons learned from this project:

1. **The current CSIP-certification does not provide plug and play interoperability.** CSIP-certified products from different vendors are not interoperable out of the box. This requires that each gateway/aggregator integration needs troubleshooting and additional testing and adjustments to ensure interoperability with the PG&E DER Headend Server.

2. **Smart Inverter vendors prefer to communicate with utilities through an aggregator or gateway versus direct-to-inverter integration.** Through the smart inverter manufacturer survey, it was determined that direct-to-inverter integration was the least preferred option for integrating

with utilities. It was also determined, through the CEC inverter list[8], that over 99% of smart inverter vendors used a gateway or aggregator to receive their CSIP-certification. This not only validates the importance of the gateway/aggregator role for smart inverter communications, but it also reduces the risk of already installed smart inverters needing to be replaced or updated to conform with changes in communication protocols. In addition, it highlights that for larger sites with multiple inverters it is more efficient to have an energy management system or centralized data concentrator to connect to a gateway/aggregator especially when data and control by the distribution utility would only ever be required at a system level (per gen type) rather than at an individual inverter level.

3. **Further development and maturity of CSIP and the IEEE 2030.5 standard is important for server and client interoperability and control implementation.** Removing ambiguity and strengthening aspects around interoperability will help reduce the additional expense and time commitment from individual utilities and vendors needing to ensure interoperability and functionality of systems. In addition, complex control functions need to be clearly implemented for both direct and aggregator communications.

4. **PG&E can communicate with third-party devices over the public internet without additional cybersecurity risks.** By treating these devices and connections as zero-trust, PG&E network architects were able to devise a solution that limits PG&E's operational networks from exposure to potential bad-actors. This reduces the cost for telemetry from interconnecting DERs because private communications channels are typically higher cost.

5. **End-devices add another layer of interoperability complexity.** The interoperability between gateways and end-devices cannot be taken for granted. End-devices (e.g. meters, smart inverters) use protocols like Modbus to communicate but may map their data in various ways. This requires gateways/aggregators to continuously develop custom data maps to properly translate telemetry and control functions into IEEE 2030.5 until end-device vendors standardize their interfaces.

6. **CSIP needs to build out a process for updating the standard and being flexible in the face of real-world constraints and demands.** The CSIP standard needs to be flexible when it comes to adapting to new requirements as users gain more field experience such as developments with cybersecurity.

7. **DER controls require further testing.** Limited initial testing during EPIC 3.03 was unsuccessful in demonstrating out-of-the-box control capability across the stack. DER controls contain multiple complexities from setting schedules, to curves, to disaggregation among multiple DERs, to proper translation and functionality at the end-device. With the added interoperability challenges between the DER headend, DER aggregator/gateway, and DER end-device, control implementation will require further piloting before being ready for use at scale.

8. **Customer-Owned Telemetry shifts the maintenance burden from the utility to the customer.** Utility-owned communication equipment for telemetry was expensive up front for customers, but also did not require the customer to maintain or provide communications for the device in perpetuity. It is still unclear how well customers will maintain their equipment over the 10-20+

[8] https://www.energy.ca.gov/sites/default/files/2021-10/Grid_Support_Inverter_List_Simplified_Data_ADA.xlsx

year lifespan of the DER, and if they will experience challenges with vendor support over that time period.

1.5 Recommendations

The following recommendations are applicable both industry-wide and to PG&E specifically:

- Continue development of CSIP and IEEE 2030.5 standards and refinements in interoperability between CSIP-certified systems.
- Continue testing of control capabilities using the DER Headend System and control-enabled connected DERs.
- Continue development of aggregator integrations to lower the cost of these systems further for PG&E interconnection customers.
- Continue discussion of cybersecurity requirements for CSIP especially at a national standards level through IEEE, SunSpec[9] or another standards group.
- Consider deployment of the IEEE 2030.5 DER Headend in the cloud vs on premise for added flexibility and cybersecurity.

1.6 Conclusion

The EPIC 3.03 DER Headend System project successfully deployed, tested, and configured a CSIP-certified IEEE 2030.5 server that is interoperable with two vendors' RSG devices and three aggregators. It demonstrated that a utility can communicate with customer-owned devices over the public internet in a cybersecure way. In deploying and testing the DER Headend system PG&E has effectively lowered the cost for PG&E generation interconnection customers to fulfill their telemetry requirements for a cost of less than $20,000 over a ten-year period (vs $50,000-$150,000 previously) with costs likely to further decrease as the certified interoperable vendors mature their product offerings.

The success of this project does not diminish the work remaining to make CSIP-certified devices plug-and-play interoperable. Remaining still is the work to ensure the control functions can work when the need for that functionality arises for example through a Distribution Investment Deferral Framework (DIDF)[10] project or an interconnection customer requiring a granular limited generation profile for their DER.

This project has laid the foundation for the future of DERMS at PG&E. As more DERs are interconnected to the grid, it becomes important to be able to coordinate these resources through the DERMS. Establishing a low-cost connection to the DERs is the first step to unlocking that greater potential.

[9] SunSpec Alliance. (n.d.). Retrieved from https://sunspec.org/

[10] Pacific Gas & Electric Company. (n.d.). PG&E Distribution Investment Deferral Framework Fall 2022 RFO. Retrieved from https://www.pge.com/en_US/for-our-business-partners/energy-supply/electric-rfo/wholesale-electric-power-procurement/fall-2022-didf-rfo.page?WT.mc_id=Vanity_rfo-fall2022didf&ctx=large-business

2 Introduction

This report documents the EPIC Project 3.03 DER Headend System 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 several 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*[11], which established the Electric Program Investment Charge (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*[12], 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."[13]

The decision also required the EPIC Program Administrators[14] to submit Triennial Investment Plans to cover three-year funding cycles for 2012-2014, 2015-2017, and 2018-2020. On November 1, 2012, in A.12-11-003, PG&E filed its first triennial Electric Program Investment Charge (EPIC) Application with the CPUC, requesting $49,328,000 including funding for 26 Technology Demonstration and Deployment 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. On May 1, 2014, PG&E filed its second triennial investment plan for the period of 2015-2017 in the EPIC 2 Application (A.14-05-003). CPUC approved this plan in D.15-04-020 on April 15, 2015, including $51,080,200 for 31 TD&D projects.[15] On April 28, 2017, in A.17-04-028, PG&E filed its third triennial EPIC Application at the CPUC, requesting authorization for its for 43 Technology Demonstration and Deployment Projects. CPUC approved this plan through D.18-10-052 on October 25, 2018, and D.20-02-003 on February 10, 2020, and authorized $49,771,845 for the 43 TD&D projects.

Pursuant to PG&E's approved 2018-2020 EPIC triennial plan, PG&E initiated, planned and implemented the following project: EPIC 3.03 – DER Headend System. Through the annual reporting process, PG&E has kept CPUC staff and stakeholder informed on the progress of the project. The following is PG&E's final report on this project.

[11] http://docs.cpuc.ca.gov/PublishedDocs/WORD_PDF/FINAL_DECISION/156050.PDF
[12] http://docs.cpuc.ca.gov/PublishedDocs/WORD_PDF/FINAL_DECISION/167664.PDF
[13] Decision 12-05-037 pg. 37
[14] Pacific Gas & Electric (PG&E), San Diego Gas & Electric (SDG&E), Southern California Edison (SCE), and the California Energy Commission (CEC)
15 In the EPIC 2 Plan Application (A.14-05-003), PG&E originally proposed 30 projects. Per CPUC D.15-04-020 to include an assessment of the use and impact of EV energy flow capabilities, Project 2.03 was split into two projects, resulting in a total of 31 projects.

2.1 Project Motivation

California is a leader in the growth of DERs driven by a confluence of technology advancements, consumer preferences, and complementary legislative and regulatory actions. California's Renewable Portfolio Standard (RPS) and SB-100 (60% renewable by 2030, and 100% zero-carbon by 2045[16]), net energy metering (NEM) policies, and federal tax subsidies have propelled EV and solar adoption within the PG&E territory. As of December 2022, over 11,000 solar installations are added each month to PG&E's grid totaling more than 682,000 sites to date, over 47,000 behind-the-meter (BTM) energy storage interconnections, and there are already more than 477,000 EV registrations with more anticipated with Executive Order N-79-20 mandating the sale of zero-emission vehicles by 2035[17]. To further support this growth in renewables, California State Assembly Bills (AB) 2514[18] and AB 2868[19] are requiring large investments in energy storage technology to help create a more flexible grid to enable less traditional forms of generation.

However, while DERs help achieve California's clean energy objectives, they can potentially create new challenges including capacity (thermal) constraints, power quality issues, inclusive of voltage violations, and adverse impacts on protection systems due to bidirectional power flow. Furthermore, hosting capacity is decreasing, thus reducing the overall flexibility of the grid to handle more DERs without infrastructure improvements.

Systems such as DERMS are needed to not only manage the additional complexity created by DER growth, but to leverage DERs for grid and local reliability benefits, realize value from DERs, and potential distribution investment deferral. Significant grid modernization investments are required to operate in this new paradigm while achieving the state's ambitious clean energy goals. PG&E's vision of the future electric grid is a secure, resilient, reliable, and affordable platform that enables continued gains for clean energy technologies and California's economy in a way that provides maximum flexibility and value for customers. This will require the coordination of new and existing tools and infrastructure including advanced applications such as DERMS.

[16] Senate Bill No. 100 (SB-100): https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB100

[17] California Executive Order N-79-20, Governor Gavin Newsom. https://www.gov.ca.gov/wp-content/uploads/2020/09/9.23.20-EO-N-79-20-Climate.pdf?emrc=9f8f26

[18] AB 2514 was designed to encourage California to procure by 2020 and incorporate by 2024 energy storage into the electricity grid to support the integration of greater amounts of renewable energy into the electric grid, defer the need for new fossil-fueled power plants and transmission and distribution infrastructure, and reduce dependence on fossil fuel generation to meet peak loads. http://www.energy.ca.gov/assessments/ab2514_energy_storage.html.

[19] The California Public Utilities Commission (CPUC) has issued an order requiring that PG&E, SCE, and SDG&E propose programs and investments for up to 500 megawatts (MW) of distributed energy storage systems, distributed equally among the three utilities, above and beyond the 1,325 MW target for energy storage already required pursuant to AB 2514. http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M184/K630/184630306.PDF.

The EPIC 3.03 project builds upon the learnings of the previous EPIC 2.02 DERMS project[20]. In EPIC 2.02, PG&E evaluated more future oriented DERMS functionality, but in order to do so, relied on a standalone proof of concept system with customized integrations and non-standard implementations that were not able to be put into production at scale. EPIC 3.03 built upon those learnings to focus on a production-ready system to meet the existing needs and near-term demands of DER systems, while creating a foundation for future DERMS growth. To enable a future DERMS deployment, a standard for communication with DERs from the utility DERMS is needed. This DER Headend System project builds that foundational capability so that future DERs can communicate with the utility in low-cost, reliable, and predictable ways.

This project aimed to 1) advance the adoption of the Common Smart Inverter Profile (CSIP) and the IEEE 2030.5 protocol standard and contribute to its enhancement, 2) meet customer requests and regulatory mandates to lower the cost of telemetry using a customer-owned telemetry system, and 3) act as a foundational step to leveraging large volumes of DERs for monitoring and controlling DERs using a DERMS and ADMS.

2.2 Industry Trends

Over the last decade there has been expansive proliferation of DERs on the grid. This includes over half a million solar interconnections, a growing number of battery electric storage systems, and rapid acceleration of electric vehicles onto PG&E's service territory. The industry is moving from DERs being just passive devices on the grid towards active participation by these DERs to provide additional services. Examples include:

- DERs as distribution investment deferral framework (DIDF) projects also known as non-wires alternative (NWA) projects. DIDF/NWA projects aim to avoid or defer physical upgrades to the grid, like avoiding upgrading the capacity of a line with greater ampacity conductors with DERs that can offset load or generation in a given section of the grid.
- Leveraging bi-directional EVs to reduce the evening peak load on the grid or provide other grid services.
- Using Integrated Capacity Analysis (ICA) to set Limited Generation Profiles (LGP) on DERs to allow for greater export of generation from DERs.
- Setting up microgrids to power customers/communities during wider grid outages.
- Integration of DERs into the CAISO market
- Leveraging DERs for grid services like resource adequacy, assisting with grid switching operations and voltage support, and other use cases which are being discussed in the CPUC High DER Order Instituting Rulemaking's (OIR) Smart Inverter Operationalization Working Group (SIOWG).

One thing remains certain with the development of these different DER use cases: more communication and data collection will allow the use of these resources to be optimized. This is why the development of the CSIP and IEEE 2030.5 standards is so important to the future of these use cases. If utilities can cost-effectively and securely communicate with DERs, it will provide the greatest benefit to customers and

[20] EPIC 2.02, Distributed Energy Management System Final Report. https://www.pge.com/pge_global/common/pdfs/about-pge/environment/what-we-are-doing/electric-program-investment-charge/PGE-EPIC-2.02.pdf

DER owners. EPIC 3.03's development of an CSIP Certified IEEE 2030.5 server is foundational to the development of a DERMS to organize and direct all these DERs in coordination with the ADMS.

PG&E being at the forefront of much of the DER adoption has brought a lot of attention to the development of the DER Headend System under EPIC 3.03 from the utility industry worldwide. EPRI in collaboration with other utilities developed their "Distributed Energy Resources Utility Gateway Requirements: First Edition"[21] which outlines the hardware, operating system, firmware, security, environmental, functional, and cybersecurity requirements they determined were necessary for gateways. These requirements compare very similarly to PG&E's early stage of this project. Through comfort with the system, network architecture and results of penetration testing, PG&E was able to reduce the cybersecurity and hardware security requirements and make them guidelines. Through PG&E's efforts as part of EPIC 3.03, the rest of the industry may also make the same conclusions. PG&E is involved in the development of standards, including IEEE 1547.3 and CSIP, to help share what our experts have learned through the development of this process to be of benefit to the rest of the industry.

3 Project Summary

The DER Headend System project was focused on developing a production-level cybersecure vendor agnostic CSIP-certified IEEE 2030.5 DER Headend Server with interoperability to at least two vendor gateways with an overall utility-related cost of $20,000. The project was expanded to include interoperability with three aggregators as well. A process was put into place to test interoperability between the DER Headend Server and new gateway or aggregator vendors applying to be included as a PG&E certified-interoperable vendor. This was all done as a first foundational step for deploying a full scale DERMS and ADMS to manage larger volumes of DERs on the grid using the standardized CSIP IEEE 2030.5 protocol stack, enabling further penetration of DERs onto the grid and additional DER capabilities.

3.1 Project Objectives

The DER Headend System was developed to:

- Further the adoption of CSIP and the IEEE 2030.5 protocol standard.
- Meet customer requests and regulatory mandates to lower the cost of telemetry using a customer-owned telemetry system.
- Act as a foundational step to leveraging large volumes of DERs for monitoring and control using a DERMS and ADMS.

3.1.1 Further the Adoption of CSIP and the IEEE 2030.5 Protocol Standard

By creating the first production ecosystem using CSIP and IEEE 2030.5 in California, this project was able to move a relatively new technology from a vision to an actual production implementation that will continue to grow as more customers and vendors adopt the technology. The pain points that were faced through project implementation will help improve CSIP and IEEE 2030.5 and interoperability of devices, aggregators, and servers using these requirements.

[21] Distributed Energy Resources Utility Gateway Requirements: First Edition, EPRI. July 29, 2022. https://www.epri.com/research/products/000000003002025100

3.1.2 Meeting Customer Expectations and Regulatory Mandates to Lower the cost of Telemetry and Provide a Customer Owned Telemetry Option

By deploying a system that utilizes the public internet and third-party installed and maintained devices, the DER Headend System reduces the cost of telemetry for customers who choose the Customer-Owned Telemetry option. The only other option for interconnection customers would be to use PG&E owned devices communicating over private networks to PG&E's network and grid management systems. With increased volume, vendors will be able to lower their prices further through economies of scale. Using aggregators is expected to lower costs further by leveraging existing connections to the DERs and developer systems and porting that data using IEEE 2030.5 to the PG&E DER Headend Server.

3.1.3 Act as a Foundational Step to Leveraging Large Volumes of DERs for Monitoring and Control using a DERMS and ADMS

Through this project, PG&E was able to establish foundational technology to securely connect to third-party devices and aggregators for monitoring and control while reducing customer costs and creating a potential pathway for future integrations with aggregations of smaller DERs at scale to help support the grid through increased visibility and potential grid services.

3.2 Project Activities

To accomplish the objectives for the EPIC 3.03 – DER Headend System project was implemented in phases:

- Phase 1a, development and deployment of the DER Headend Server.
- Phase 1b, interoperability testing of two vendor RSGs was performed, and Customer-Owned Telemetry was deployed into production.
- Phase 1c, tested and deployed Customer-Owned Telemetry using PG&E certified-interoperable aggregators.
- Phase 2, focused on testing connect/disconnect functionality and demonstrated limited advanced control functions in a lab setting

The scope to make it production ready reflects the expectation that the deployed demonstration systems were pushed to production upon successful completion of each demonstration phase. Hence the design and architecture of the demonstration project were designed to be robust to meet production requirements.

Phase 1a – Deploy the DER Headend Server
In Scope for Phase 1a:

- Deployed the DER Headend Server to communicate with a demonstration RSG device installed at customer site for telemetry. The overall deployment included:
  - Utility side DER Headend Servers that received CSIP-certification and are compliant with SunSpec CSIP 2.1 requirements.
  - Network architecture and infrastructure needs using appropriate cybersecurity safeguards.
  - DER Headend Servers installed at PG&E data centers behind firewalls and edge devices according to designed network architecture.
  - Demonstrated RSG device from DER Headend Server vendor installed at a customer site to test communication to the DER Headend Server.
  - Telecommunication infrastructure to communicate with the field gateway.

Phase 1b – Move DER Headend System into Production with Two Certified-Interoperable RSG Vendors

In Scope for Phase 1b:

- Performed interoperability testing and troubleshooting between two RSG vendors compliant with SunSpec CSIP 2.1 requirements.
- Tested on-site DER communications at demonstration sites using the RSGs from the two RSG vendors.
- Developed and demonstrated the end-to-end operational processes required for taking the Customer-Owned Telemetry solution to production. For example, one of the processes developed was for registering the device for telemetry during interconnection.
- Enabled DER Headend Server, ED-PI, GIS, and DMS integration to display DER telemetry data to Distribution Operations.
- Developed and tested the distribution control center (DCC) operator screens in DMS (via ED-Pi link) to meet operator DER monitoring requirements for real-time streaming data and historical trends for the Customer-Owned Telemetry sites greater than 1MW.
- Enabled DER Headend Server, ED-PI, GIS, and DMS integration to display DER telemetry data to Distribution Operations.
- Developed the documentation of operational processes and training required to deploy the DER telemetry use case in production (with existing infrastructure (DMS, ED-PI, and SCADA).
- Documented the plan to scale the demonstration project system components and integration for in-production needs. The Customer-Owned Telemetry solution is expected to add ~30-40 DER telemetry sites per year.
- Conducted training sessions for DCC Operators, Electric Grid Interconnection (EGI) managers, IT Project Managers, and SCADA Specialists to use and deploy the systems.
- Detailed telemetry requirements for 3rd party DERs including field device specifications posted to the Distribution Interconnection Handbook[22].
- Updated YourProjects, PG&E's interconnection online application portal, for interconnection customers to choose Customer-Owned Telemetry option.

[22] TD-2306P-01 – Customer-Owned Telemetry Procedure, June 13, 2022. https://www.pge.com/includes/docs/pdfs/shared/customerservice/nonpgeutility/electrictransmission/handbook/TD-2306P-01.pdf

- Updated relevant Rule 21 PG&E interconnection webpages[23,24,25,26,27,28,29] to advertise information on the Customer-Owned Telemetry option.

Phase 1c – Approve three Aggregators for Interoperability with DER Headend Server and Move to Production
In Scope for Phase 1c:

- Reached out to Smart Inverter manufacturers with large quantities of deployed Smart Inverters on PG&E's grid to join the aggregator demonstration. Worked with one interested manufacturer to demonstrate an aggregator for their systems.
- Performed interoperability testing and troubleshooting between three aggregator vendors compliant with SunSpec CSIP 2.1 requirements.
- Tested on-site DER communications at demonstration sites using the aggregators.
- Worked with the two RSG vendors and other interested IEEE 2030.5 aggregator vendors to deploy and test their aggregators with the DER Headend Server.
- Offered IEEE 2030.5 aggregator to PG&E interconnection customers as a customer-owned telemetry option.

Phase 2 – Test Connect/Disconnect and Advanced Controls using the DER Headend System
In Scope for Phase 2:

- Tested connect/disconnect and advanced controls including scheduled controls with lab smart inverter through RSG device.
- Tested limited set of control functions and effectiveness of communications and response from inverter:
    - Tested the connect/disconnect, powering the smart inverter down and commanding it to power up.
    - Tested scheduled connect/disconnect, scheduling the smart inverter to power down and commanding it to power up.
    - Tested fixed power control.
    - Tested scheduled fixed power control.

[23] Expanded Net Energy Metering (NEM2EXP) webpage, https://www.pge.com/en_US/for-our-business-partners/interconnection-renewables/net-energy-metering/expanded-nem.page?ctx=large-business
[24] Net Energy Metering Aggregation (NEM2A) webpage, https://www.pge.com/en_US/for-our-business-partners/interconnection-renewables/net-energy-metering/nem-aggregation.page?ctx=large-business
[25] Virtual Net Energy Metering (NEMV) webpage, https://www.pge.com/en_US/for-our-business-partners/interconnection-renewables/net-energy-metering/virtual-nem.page?ctx=large-business
[26] Net Energy Metering for Fuel Cells (NEMFC) webpage, https://www.pge.com/en_US/for-our-business-partners/interconnection-renewables/net-energy-metering/nem-for-fuel-cell-generators.page?ctx=large-business
[27] Net Energy Metering Multiple Tariff (NEMMT) webpage, https://www.pge.com/en_US/for-our-business-partners/interconnection-renewables/net-energy-metering/nem-multiple-tariff.page?ctx=large-business
[28] Non-Export Interconnection webpage, https://www.pge.com/en_US/for-our-business-partners/interconnection-renewables/larger-self-generation-programs/non-export/non-export.page
[29] Energy Storage webpage, https://www.pge.com/en_US/for-our-business-partners/interconnection-renewables/export-power/distributed-generation-handbook/net-energy-metering/energy-storage/energy-storage.page

- Tested VoltWatt curve.
- Tested loss of communications before, after, and during a scheduled control.
- Tested multiple control operations

3.3 Project Timeline and Key Milestones

3.3.1 Tasks and Milestones

Phase 1a – Deployment of DER Headend System – Start June 2019

1. Detailed scope and charter created and approved - October 2019
2. Demonstration location selection finalized – Aug 2019
3. High level solution design completed – Nov 2019
4. Statement of work (SOW) finalized for DER Headend Server and demonstration RSG Contract Executed – Nov 2019
5. Required 3rd party contracts executed for the secure communication network and the cybersecurity infrastructure – Dec 2019
6. Factory Acceptance Test (FAT) completed for Phase 1 functionalities – Nov 2020
7. Site Acceptance Test (SAT) at demonstration site – April 2021

Phase 1b – Move DER Headend System into Production with Two Certified-Interoperable RSG Vendors – Start Oct 2020

1. Statement of work (SOW) finalized for two vendor RSGs and contracts executed – Oct 2020
2. Systems Integration between EGI's data system and DMS – July 2021
3. Internal and external Documentation and Training delivered – June 2022
4. First demonstration site using certified-interoperable vendor RSG device commissioned – April 2022

Phase 1c – Approve three Aggregators for Interoperability with DER Headend Server and Move to Production– Start July 2021

1. Gain commitment from one DER developer to develop aggregator interoperability with PG&E's DER Headend System – November 2021
2. Completion of testing and commissioning of first aggregator connection and demonstration site to DER Headend Server – July 2022

Phase 2 – Control Testing:

1. Test connect/disconnect using the DER Headend System (Reference section 4.9 for more detail) – Start May 2022
2. Test advanced controls using the DER Headend System (Reference section 4.9 for more detail)– Start September 2022

4 Project Activities, Results, and Findings

4.1 Project Initiation and Background

The EPIC 3.03 project was an outgrowth of both the prior EPIC 2.02 DERMS project and known challenges with the existing method of telemetry for large DER customers. In EPIC 2.02, PG&E implemented an IEEE 2030.5 system with two aggregators, however it was not able to be scaled for

multiple reasons including that it was created using an earlier version of IEEE 2030.5 and CSIP, it relied on multiple PG&E-specific customizations, and the servers were decommissioned after the proof-of-concept project as PG&E used the learnings from this project to launch the ADMS program and focused design and build efforts on their newly chosen ADMS vendor. At the same time, there was growing concern from DER customers and the CPUC regarding the costs of required telemetry systems for PG&E DER customers 1MW and greater. It was recognized that this communication link between DERs and the utility needed to be addressed as a foundational aspect of not only telemetry but any DERMS system in the future.

PG&E evaluated potential options for acquiring this type of information (Table 1) more cost-effectively via paths like Distributed Network Protocol 3 (DNP3), the AMI network, or line sensors, and selected IEEE 2030.5 as likely the best path to both reduce costs and align with the ongoing concerted push toward using IEEE 2030.5 as the default protocol for smart inverter communications in California. Therefore, the EPIC 3.03 project sought to address the challenges of cost regarding DER telemetry requirements, while at the same time providing a path to implement a production-ready IEEE 2030.5 system that could be the foundation for future smart inverter and DER interactions.

Table 1: Comparison of various telemetry options.

Telemetry Solution Options	Operational Requirements	Customer		Future Oriented	Readiness
		Cost	Responsibility		
SCADA Recloser (Existing Solution)	• **Net Load Only** (No Masked Generation Information) • Provides Added Utility Disconnect and Protection Capabilities	• **High**: ~$160k • Utility Owned	• **None**	• **Cannot Enable Future** Oriented Requirements	• **Existing**
SCADA Mini-RTU (Existing Solution)	• **Meets Operational Requirements**	• **High**: ~$70k • Utility Comms • Customer Metering	• **Aggregate** Input Devices for Mini-RTU • **Maintain** Customer Input Devices	• **Enables Most Future** Oriented Requirements • **Lacks Aggregator Support** • **Cybersecurity Constraints** Limit Future Use	• **Existing**
AMI Metering	• **Net Load Only** (No Masked Generation Information) • **Slow Data Sampling** Rates • **Slow Data Retrieval** Rates	• **Cost**: TBD • Utility Owned	• **None**	• **Cannot Enable Future** Oriented Requirements	• **Development Needed** to Operationalize Existing Data **but Still Cannot Enable Future** Requirements
Proposed 2030.5 Solution (Includes Smart Inverters)	• **Meets Operational Requirements**	• **Low**: Targeted <$20k • Customer Owned	• **Aggregate** Input Devices • **Maintain** Devices o Comms o Hardware o Firmware o Software o Security	• **Enables Future** Oriented Requirements • **IEEE 2030.5** Expected to be Mandated	• **Development Needed** to Enable Platform

4.1.1 Regulatory

The background for telemetry becoming a requirement with a drive towards low-cost telemetry has been elaborated within Advice Letter 6350-E-B and within CPUC Resolution E-5038. Briefly on April 5, 2019, D. 19-03-013, "Decision Adopting Proposals from March 15, 2018 Working Group One Report" was issued:

> "The IOUs believe that increased use of real-time telemetry is necessary for grid visibility. This grid visibility provides necessary information to grid operators who make decisions that support the safe and reliable operation of the electrical grid with the continued proliferation of DERs."

CPUC Resolution E-5038 and ALs 6350-E, 6350-E-A, & 6350-E-B

Within the timeframe of the EPIC 3.03 project, the CPUC issued Resolution E-5038 on August 20, 2021. The resolution called out new requirements from the IOUs regarding telemetry within Ordering Paragraphs 2 and 3.

Ordering Paragraph 2:

Ordering paragraph two of this resolution required PG&E to,

> "Implement specific technical requirements for telemetering of distribution-connected systems 1 MW or greater and less than 10 MW. The adopted technical specifications for these systems are as follows: 1) facilities can report measurements in 15-minute increments using customer-owned, nonrevenue-grade metering and a data aggregation device comparable to the serial device server that SCE has historically required, 2) customers can choose to connect the reporting device to the utility Energy Management System via cellular modem or dedicated internet connection, and 3) measurements do not have to be made from revenue grade equipment. The Utilities shall submit Tier 1 Advice Letters to implement these requirements no later than 45 days from the issuance of this Resolution."

PG&E submitted AL 6350-E on October 4, 2021, where the implementation plan of the customer-owned telemetry system was outlined as required by this ordering paragraph.

The initial implementation plan outlined the use of a customer-owned gateway device from a PG&E certified-interoperable gateway vendor that is interoperable with PG&E's CSIP-certified IEEE 2030.5 system, that the customer is responsible for maintaining the internet connection between the device and PG&E using a public static IP address, and that non-revenue grade metering is acceptable for the telemetry requirement.

Additionally in this AL, PG&E suggested an alternative reporting rate on the order of seconds instead of the 15-minute increment outlined in the ordering paragraph. The AL provided five reasons for more frequent near real-time data.

The implementation plan laid out in AL 6350-E was protested by the California Solar and Storage Association (CALSSA) on October 25, 2021. CALSSA's interpretation of the ordering paragraph, which the CPUC agreed with, was that the customer-owned telemetry option be available to interconnection customers by October 4, 2021. In order to comply with this interpretation of the ordering paragraph, PG&E submitted supplemental AL 6350-E-A on November 15, 2021, that required all projects requesting to use customer-owned telemetry be assessed for conditional-PTO. If the project received conditional-PTO, then they were able to wait on the sidelines until the customer-owned telemetry was widely available to interconnection customers. If the project was not able to receive conditional-PTO, then PG&E would accommodate them as a demonstration site. PG&E interpreted the timeline for offering the customer-owned option as those projects that had signed their interconnection agreements after the October 4, 2021 date.

Ordering Paragraph 3:

In AL 6350-E-B, PG&E addressed additional topics around items 1 and 4 of OP3. OP 3 states:
Pacific Gas and Electric Company, San Diego Gas & Electric Company, and Southern California Edison Company may request, via Tier 3 Advice Letters, a modification to the telemetry rules to require an IEEE

2030.5-based solution, with or without an accompanying request to reduce the telemetry threshold from 1 MW to 250 kW at a future date. Such a request must

1) **Report on the actual utility-related costs and non-utility-related costs incurred, over a period of at least 6 months, by systems providing IEEE 2030.5-based telemetry,**
2) discuss the specific operational needs that would be met via a reduced telemetry threshold at a level of detail beyond that available in the Working Group One Final Report filed on March 15,
3) quantify the benefit provided by meeting those needs,
4) **provide detail on any implementation differences between communications directly to the inverter versus an aggregator or gateway.**

[formatting added]

PG&E was not requesting a change to the "telemetry rules" but since the EPIC 3.03 project was going to deliver an IEEE 2030.5-based solution, it was important to respond to the relevant items 1 and 4 of this OP. This AL reiterates that PG&E is not requesting to lower the threshold of DERs requiring telemetry from 1 MW to 250 kW at this time. The AL only commented on the cost (item 1) and direct to inverter communication (item 4).

Item 1: Cost of Installation

Lowering the cost of telemetry for PG&E interconnection customers was a major goal of the EPIC 3.03 project. The goal for telemetry had always been less than $20,000 of utility-related costs. Through assessing the costs with the certified-interoperable RSG vendors and the configuring costs with PG&E IT, PG&E believed that it was under this threshold. As PG&E began demonstrating the first few customer-owned telemetry sites, it came up at a meeting PG&E EGI holds with interconnection stakeholders, known as the interconnection best practices (ICBP) meeting, that the demonstration site costs were still too high. The immediate challenge was how to bring costs down for a system that requires communication charges and potentially maintenance on project volumes that are very small. The Smart Inverter Working Group (SIWG) Working Group 1 final report defines utility related costs as costs for, "metering equipment (meters, circuit transformers (CT) and potential transformers (PT)), communications/telemetry equipment (Remote Terminal Unit (RTU) and a modem), and charges for labor, taxes, and maintenance." This definition is not time bound but PG&E used a ten-year timeframe to estimate the telemetry costs. PG&E also reviewed the requirements for the customer-owned telemetry solution and found opportunities to lower the system costs further. As mentioned in the site metering section 4.3.1 of this report, PG&E reviewed the telemetry requirements from Southern California Edison (SCE) and San Diego Gas & Electric (SDG&E) to see how their telemetry costs were lower. The other two IOUs did not require a PCC meter because there is sufficient visibility into the loads using other available data points i.e. the telemetry from an upstream SCADA device would suffice for grid operators. PG&E reviewed this with its DCC operations teams and agreed that PCC-level metering is not needed but with the caveat that those DERs requiring control would likely still need PCC-level metering.

PG&E's cost to configure the RSG devices onto the DER Headend Server is $4,000 based on estimates from PG&E's IT team. This figure is planned to be reviewed annually to ensure that it is raised or lowered based on actual costs over the year and will be published in the annual unit cost guide.

PG&E reviewed the remaining costs and cost structure with the two certified-interoperable vendors. The costs were to the best of PG&E's knowledge, in the range of $12,000 to $23,000 including PG&E configuration costs depending on what optional additions the customer decides to choose from the vendors.

PG&E also anticipates that the cost of fulfilling the telemetry requirement using an aggregator will be significantly less as the device costs are less because the site devices can be more generic. The aggregator connection can also leverage existing connections between the DERs' smart inverter(s) and the developer's data systems. The aggregator would just translate that information to IEEE 2030.5 protocol for PG&E's DER Headend System.

Item 4: Direct-to-Inverter Communications vs Gateway or Aggregator

As mentioned in the survey results section of this report, it is anticipated based on the survey results and review of the CEC list that greater than 99% of DERs will likely utilize a gateway or an aggregator connection if they need to integrate with PG&E's utility systems. The EPIC project team did not test any direct-to-inverter communications through this project but if a smart inverter manufacturer that desires direct-to-inverter communications would like to test their interoperability with PG&E's DER Headend Server, they are welcome to apply to become a certified-interoperable vendor that is capable of interoperating with PG&E's DER Headend Server.

On October 18, 2022, the CPUC made AL 6350-E-B effective as of October 4, 2021.

Smart Inverter Working Group and Smart Inverter Manufacturer Survey

In support of the request to assess what the impact of using a different cipher suite from CPUC Energy Division (ED) Staff (discussed further in section 4.4.3) was on the installed base of smart inverters, PG&E devised and conducted a survey[30] to ascertain the ability for the installed base of smart inverters to communicate with utility systems as installed and to determine the ability to update the smart inverters to update software or cybersecurity requirements. This would allow PG&E to also determine what the impact of changing the cipher suite would be. The survey was sent to members of the Smart Inverter Working Group and smart inverter vendors.

PG&E stated that it would not share individual or self-identifying answers or information outside of the IOUs or the CPUC and that the purpose of the survey would be to help guide PG&E's roadmap for communicating with DERs. While presenting the survey at the Smart Inverter Working Group, someone responded that their company would not want outsiders to know their product development plans and asked to answer the survey anonymously. As a result, question one, company name, and question two, email address, were made optional. It was possible to link answers from question to question to the respondent even if the respondent was anonymous. This helped track whether the respondent was answering a question because they were planning to develop or had developed the specific capability. While reviewing the results of the survey, it was determined that cross referencing the results of the survey with the vendors that are listed on the California Energy Commission's (CEC) smart inverter list as CSIP-certified would help provide more context into the responses. Through review of the CEC's list, PG&E learned that smart inverter vendors could be listed as CSIP-certified if they used a RSG device to

[30] Smart Inverter Utility Integration Survey (Preview) (office.com)

perform CSIP's certification test. The CEC list[31] distinguished between smart inverters that received certification using a gateway versus direct to inverter. Filtering between the two options, over 99% of smart inverter models, 759 models, leveraged the use of a gateway to attain their CSIP-certification. Only nine smart inverter models from four vendors received their CSIP-certification with direct to inverter communications. Of the nine models only one of the vendors responded to the survey and their least preferred option, according to their survey response, was to integrate with utility systems using direct to inverter communications. By review of the CEC list, it became apparent that the impact of the changes to the installed base of smart inverters was negligible, but the survey results provided interesting results that helped broaden PG&E's understanding for why these devices are more challenging to integrate with utility systems than simply building the capacity to communicate with the devices within PG&E's network.

Following the results of the survey and the analysis of the results coupled with review of the CEC's smart inverter list, PG&E presented the results to ED staff; namely, that the installed fleet of smart inverters would not be isolated from communicating to the grid because of the change in cipher suite requirement from the utility because they would either need to use a certified-interoperable gateway or aggregator to make that connection to the utility if the requirement to integrate with these DERs ever became of interest or a requirement. PG&E also reported that some of these smart inverters do not have a sort of network connection or capability for network connection based on the responses to the survey. More details on the survey results can be found in Appendix G: Smart Inverter Working Group and Smart Inverter Manufacturer Survey.

4.2 DER Headend

4.2.1 Vendor Selection

The EPIC project team evaluated multiple vendors and technologies to address communications with DERs. An IEEE 2030.5 DER headend was eventually chosen to best align with California's smart inverter phase 2 communication requirements, including California's push to implement IEEE 2030.5 as the default protocol for DER communication, supporting customer-owned equipment, and the ability for IEEE 2030.5 to support PG&E cybersecurity's authentication requirements.

PG&E narrowed potential vendors to PG&E's existing SCADA vendor and PG&E's planned ADMS/SCADA replacement vendor. While PG&E would have preferred to implement the IEEE 2030.5 headend with the planned ADMS and future SCADA platform vendor as part of EPIC 3.03, the decision was made to make a direct award contract for the CSIP-certified IEEE 2030.5 DER Headend Server and the Site Located Communication Gateway to PG&E's existing SCADA vendor for the reasons listed below.

- **Timeline:**
    1. **Regulatory:** PG&E had stated in Advice Letter 5595-E that it would deploy a demonstration project for customer-owned telemetry to be completed by the end of 2020.
    2. **Vendor Readiness:** The planned ADMS/SCADA vendor was unable to commit to implementing IEEE 2030.5 prior to the third quarter of 2020. Even then, the system

[31] https://www.energy.ca.gov/sites/default/files/2021-10/Grid_Support_Inverter_List_Simplified_Data_ADA.xlsx

would have been limited to basic monitoring capability and not certified. In contrast, the existing SCADA vendor had already started implementing IEEE 2030.5 capabilities and already received product certification from SunSpec for the field components of the product. Selecting the existing SCADA vendor was the more feasible solution to meet the given timeline and IEEE 2030.5 requirements.

- **Operational Complexity:** PG&E's existing SCADA vendor also benefited from being an installed and known system within the PG&E environment for end users and had application-level support infrastructure and expertise. This was a benefit to adoption, integration, and ease of deployment within the expedited timeline. Deployment of the new ADMS/SCADA solution within the existing platform would have been very complex both from a systems integration and operational perspective (i.e. change management).
- **Path to Production:** Tied in with the operational complexity, was the ability to create a path to production for the system after the EPIC project. There was added uncertainty given the early stage of the ADMS deployment at the time, being a very large project encompassing an extensive scope, budget, and timeline beyond the very limited scope of EPIC 3.03. The project team was able to create a clear path with the existing SCADA vendor and internal stakeholders to have a production system with the key owners/stakeholders aligned to fund development needed, contingent on a successful technology demonstration. The ability to scope what it meant to go to production and gain commitment for future production support by internal teams familiar with the system was an additional factor in moving forward with the existing SCADA vendor.

  However, because the existing SCADA vendor would be replaced as part of the ADMS project, it was understood that the existing SCADA vendor's system (including IEEE 2030.5) would be decommissioned once the new system was ready. Therefore, the EPIC project team has also been involved in the cut-over plans, design, testing, and development for the ADMS in parallel to the EPIC 3.03 system.
- **CSIP Certification**: PG&E required CSIP certification to participate in the demonstration because this was an essential part of complying with the planned California implementation of IEEE 2030.5. It was assumed that this would ensure a base level of functionality and ease interoperability among systems. There were only a limited number of vendors that had a plan to CSIP certify their headend server. The existing SCADA vendor was one of the few that had a plan within the timeframe PG&E required. The SCADA vendor achieved CSIP-certification of their system on March 16, 2021.

4.2.2 Internal Architecture

The PG&E IEEE 2030.5 DER Headend Server is installed in three environments. The first environment is in the cloud and hosted by the Server Vendor. The interoperability testing between the RSG vendors and the DER Headend Server was done in this environment. The IEEE 2030.5 clients make a TLS session directly with the DER Headend Server. The purpose for the cloud server is for the initial testing of updates and new IEEE 2030.5 clients. The Server Vendor has access to the cloud server so any bugs can be demonstrated and resolved directly with the vendor. The second environment is the Quality Assurance (QA) server inside the PG&E network. The QA server has its own public hostname, Virtual IP, and load balancer path in the PG&E network. After a server update or new client has been proven to work on the cloud server it is tested on the QA sever to verify that the SSL offloading done in the PG&E network does not impact functionality. The third environment is the production (PROD) servers inside

the PG&E network. This is the production environment that is used to collect Rule 21 required telemetry data form the field and send the data to the Historian.

The DER Headend Server needs to communicate with untrusted customer-owned DER client devices (RSG or aggregator) and still meet the low-cost goal of $20,000 or less in utility related costs for customer-owned telemetry. PG&E considered four communication methods: using the field area network (FAN), using the smart meter network, using the public internet protocol (IP), and PG&E cellular APN (Access Point Name) based private IP.

The EPIC project team initially chose the PG&E APN based cellular IP which is a PG&E owned private IP network (see Figure 3). This APN based private IP address and isolated communication path is more secure than public internet-based communication as it used the PG&E Private Static IP Network for Customer DERs using AT&T FirstNet with custom APN. This was the chosen route because this system was initially being scoped broadly to include customer-owned DERs, PG&E-owned DERs, and potentially even transmission interconnected energy resources. PG&E-owned RSG devices and RSG devices used for transmission interconnections would require the use of the private network. The FAN is not currently widely available enough within PG&E's service territory and the smart meter network was not ideal either because the real-time telemetry traffic would impede smart meter to billing data traffic.

PG&E uses the FirstNet[32] managed communications network as one of its preferred network connections. AT&T's FirstNet is a communications network with reserved bandwidth prioritized for emergency and critical services. FirstNet's mission is to, "deploy, operate, maintain, and improve the first high-speed, nationwide wireless broadband network dedicated to public safety."[33] This managed private network is directly connected with the "peering zone" where data traffic enters PG&E networks. This is a dedicated DER AT&T Virtual Private Network (AVPN) (multiprotocol label switching (MPLS)-based VPN) connection between AT&T and PG&E peering zone. While in the peering zone, the entering data traffic is authenticated and encrypted with IEEE 2030.5 using transport layer security (TLS) 1.2 and then the load-balancing edge (LBE) device (depicted as the "internet router" in Figure 3 and Figure 4) performs secure sockets layer (SSL) offloading to inspect decrypted ingress traffic before reaching the DER Headend Server. The peering zone and the managed private network are a more trusted network connection into PG&E and able to connect directly into the ODN-DMZ where the DER Headend Server was located. This also allows the DER Headend Servers' IP addresses and port numbers to be hidden from untrusted networks and devices. The DER Headend Servers only allow access to registered RSG devices using the provided LFDI/SFDI and pre-registered static IP addresses. The DER Headend Server then connected to the core ODN for SCADA control commands and the UDN for ED-Pi historian connection.

The advantages of this solution were that it provided a private IP network (more secure than public internet) which leverages the existing 'peering zone' to provide direct private communication paths with cellular network operations (i.e. AT&T). It also allowed PG&E to use the RSG devices for its DERs or for transmission interconnected energy resources.

The disadvantages of this route were the cost of the FirstNet modem needed, the FirstNet service, the size of the modem and additional IPSec VPN tunnel. Additionally, PG&E would not allow third-party use of this communications infrastructure. This meant there could be no vendor over-the-air updates to

[32] https://firstnet.gov/
[33] https://www.firstnet.com/

equipment for things like troubleshooting, cybersecurity updates, or firmware updates. Requiring a truck roll for these types of remote management for customer systems was a barrier to scaling efficiently. It also required that PG&E own and maintain the RSG device which would add to the cost.

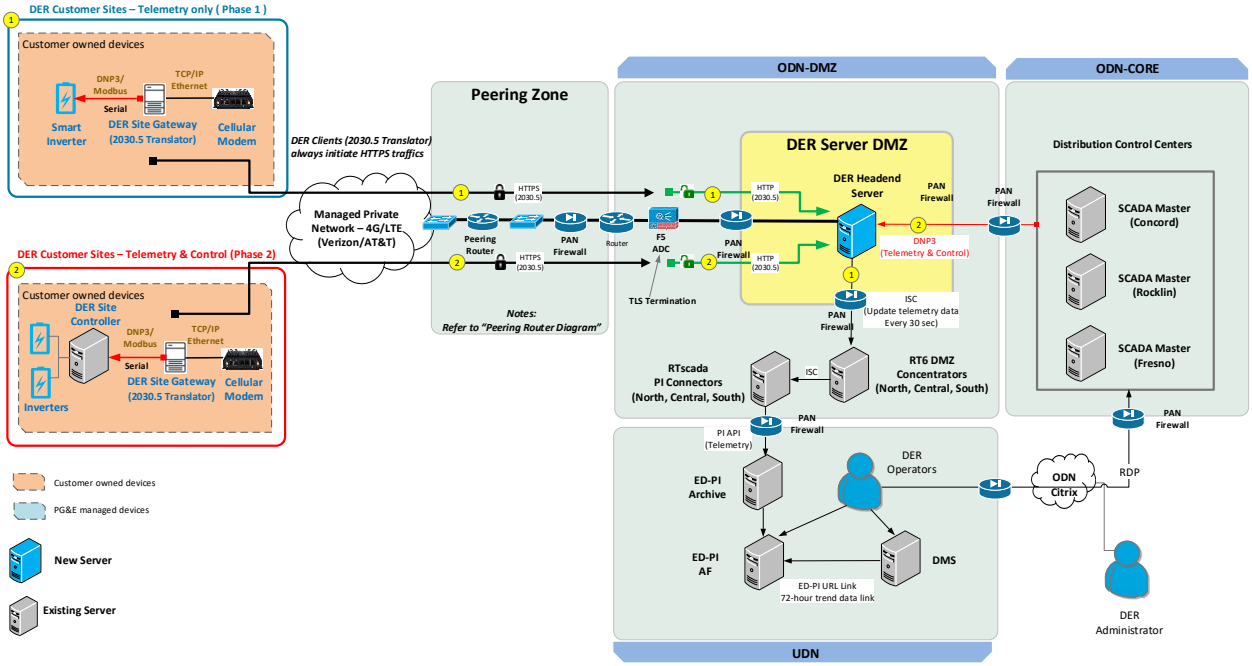


Figure 3: Initial EPIC 3.03 Network Architecture using FirstNet Private IP Network – High-Level Architecture.

There were several concerns that were major reasons to change the communication method to using the public internet, mainly:

- Monthly cellular network bills: Monthly cellular costs are high for FirstNet. Using the public internet and a standard cellular connection reduces the cost of the telecommunications costs for interconnecting customers.
- Cybersecurity concerns: Third party vendors cannot use the PG&E Private Network due to security risks.

In order to lower the cost of the system further and open up communications using less costly non-PG&E managed networks, the network architecture was updated to have data traffic coming from the public internet via the IEEE 2030.5 protocol into the PG&E UDN as can be seen in Figure 4. This meant that the devices could not be used for PG&E owned DERs or for transmission interconnected energy resources. It was decided that the benefit to DER interconnection customers was greater than the benefit this system would have provided PG&E or transmission level interconnections.

The final architecture has data traffic from the public internet arriving at the LBE device in the UDN which authenticates and encrypts the data into IEEE 2030.5 using TLS 1.2, inspects decrypted ingress traffic before the traffic enters the DER Headend Server, and hides the real DER Headend Server's IP addresses and port numbers from untrusted devices and networks. The LBE device also acts as a load balancer for the servers and the volume of data traffic coming into the DER Headend Servers. The UDN adds a layer of abstraction in an environment that is further removed from the ODN, which is beneficial because it is better for zero trust devices to communicate with that network than the more sensitive operational network.

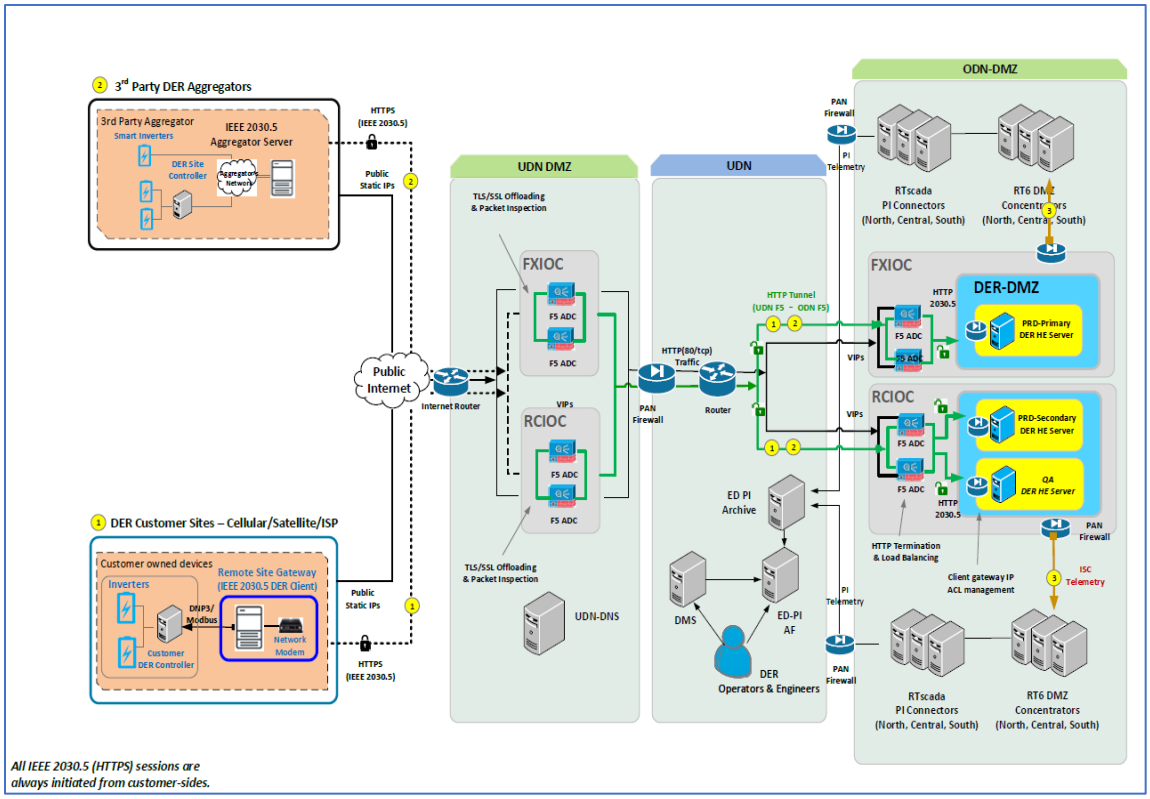


Figure 4: High-Level Network Architecture

The DER Headend Servers are located in the ODN where the SCADA servers reside. This is a closed loop network with very tight cybersecurity controls.

Once the information is received in the DER Headend Servers, the traffic is directed through a series of servers to the ED-Pi historian server in the UDN where the telemetry data is stored for use by PG&E DCC operators.

Control commands can be sent from the DCC to the DERs via the DCC SCADA system through the DER Headend Server, but this was not configured as there was not a use case available within the timeline of the EPIC 3.03 project (namely a DIDF project).

Discussed further in the section on RSGs, the RSG devices communicate to the end device i.e. the meter or energy management system (EMS) using DNP3 or SunSpec Modbus communication protocols and translate these communications to IEEE 2030.5 for HTTPS communication to the DER Headend Server over the public internet.

4.2.3 Deployment Timeline

The team considered deploying the DER Headend server at the operational data network (ODN)-demilitarized zone (DMZ) in the ODN Virtual Machine (VM) environment, but the ODN VM environment was not North American Electric Reliability Corporation (NERC)- critical infrastructure protection (CIP) compliant.

PG&E requested approval to install in the VM environment but learned that this environment was not ready for application for two reasons: first, the existing SCADA application had never been tested on a VM server and second, the SCADA team did not have a process in place to manage a VM system. PG&E decided not to pursue solutions that required significant additional resources or investment for a system that would ultimately be replaced.

The production DER Headend Servers, the primary and secondary, were installed within PG&E's data centers as discussed above. The high-level deployment timeline of the DER Headend System can be seen in Table 2.

Table 2: Deployment timeline.

Task Name	Completed
Headend Servers Installed	12/30/20
First Demonstration at Blue Lake Rancheria using FirstNet	1/25/21
System Integration	7/30/21
Interoperability Testing	5/13/22
Handoff to Production	6/8/22

4.3 DER Telemetry Devices: RSG and Aggregators

4.3.1 Site Metering Requirements

The value of telemetry for PG&E DCC Operators is being able to differentiate between load and generation on a given circuit. This helps them in forecasting load during switching events and bringing customers back online after an outage. Smart inverters are required to wait 15 seconds for the grid to come back online and stabilize before re-energizing[34] and DCC Operators have to account for that delay when switching and restoring a circuit after an outage. In order for the DCC operators to understand these dynamics it was important to determine what the gross load is versus generation to anticipate for this lag in generation coming back online. Initially it was interpreted that PCC level metering would need to be acquired from the DER sites to support the DCC operators' understanding of the gross load on the grid.

[34] (PG&E Rule 21 Section HH.1.a.ii)

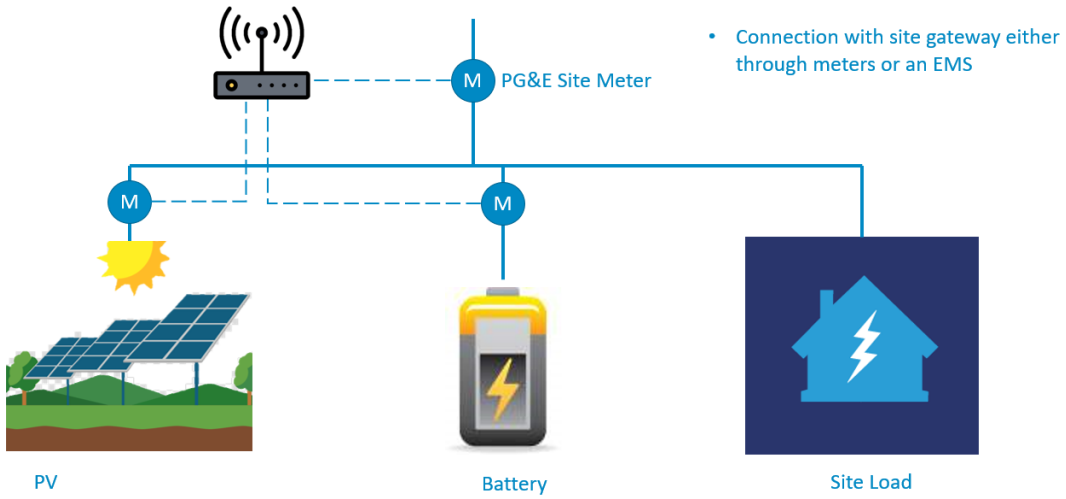


Figure 5: Site metering communication arrangement with PCC-level monitoring for a control site. Note also that each DER type (solar/battery) communicates with the RSG device separately.

For customers to provide PG&E the PCC-level metering data, the RSG device would have to acquire data from a PCC-level meter. This PCC-level meter either had to be either a Mark V meter, a dual-socket meter for a compatible customer owned meter, or a customer-owned meter added in-line with the PG&E revenue meter installed at the PCC. After realizing the options needed to support this, building out the internal and external processes for including PCC level meter data, testing it out at a demonstration site, and subsequently hearing from interconnection customers at the Electric Grid Interconnection (EGI) Interconnection Best Practices (ICBP) Forum that the cost of the customer-owned telemetry system was too high, the project team went back to the drawing board. The PG&E team surveyed the other IOUs to see how they were implementing their telemetry systems at the customer site. After discussing with each of the IOUs, neither SCE nor SDG&E were requiring PCC-level metering from their customer sites needing telemetry. Their reasoning was that they have sufficient data on the load on the circuit through SCADA devices installed upstream of the DER sites' PCC meter from SCADA enabled line reclosers or other measurement points. The telemetry information they get from the customer's DERs helps unmask the gross load enough to make grid operations decisions and the level of granularity the PCC meter provides does not enhance that enough to justify the extra expense. PG&E DCC Operations agreed with this approach with the caveat that DER sites needing control will still likely require measurements at the PCC. DERs requiring control often require export to be limited and modulated at the PCC, cognizant of the off-setting site load as well. This is consistent with discussions at the CPUC High DER OIR Smart Inverter Operationalization Working Group regarding smart inverter use cases.

4.3.2 RSG Device Vendor Selection

PG&E also decided that after building out requirements with the DER Headend vendor, the team would conduct a separate RFP to select gateway vendors through a competitive sourcing process. The procurement process was split into an initial RFP, a supplemental questionnaire for finalist vendors, and in-depth vendor interviews and demonstration of specific target use case scenarios. After the RFP was published, vendors were given the opportunity to send questions and PG&E published responses for all the vendors to see. Once response packages were received from the vendors, they were tallied in a spreadsheet so that the individual evaluators could score each vendor in the categories shown below

(Commercial, Technical, Cybersecurity, Pricing, and Responsibility). The team's evaluations were compiled into a total score for each vendor and the evaluators met to discuss the results and how to move forward.

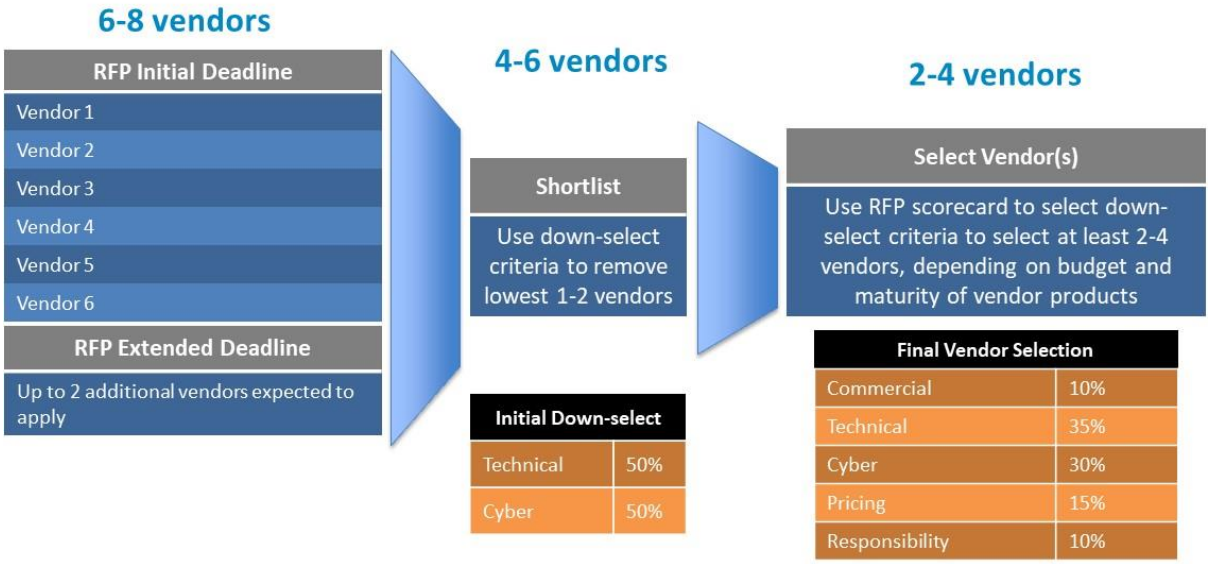


Figure 6: Vendor selection overview

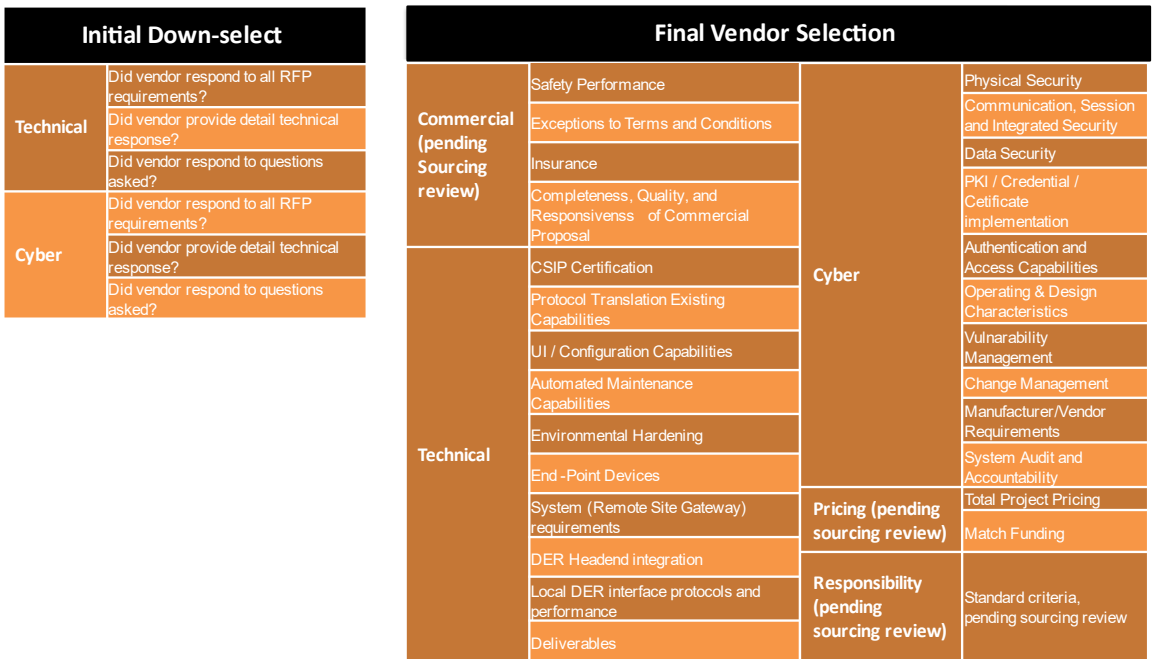


Figure 7: RSG RFP selection criteria and sub-criteria.

4.3.3 Remote Site Gateway Device Requirements

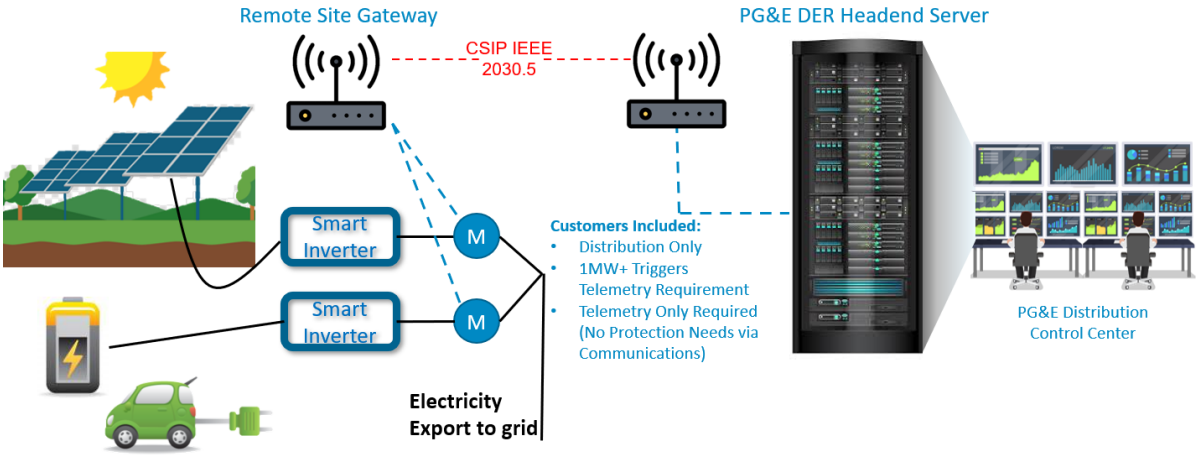


Figure 8: Simplified overview of the DER Headend System using a remote site gateway (RSG).

The RSG device communicates with all end-devices at the DER site and then provides telemetry data for each DER type (i.e. solar, battery storage, fuel cell etc.) at the DER site in IEEE 2030.5 protocol communication to the DER Headend Server.

The full list of requirements for the certified-interoperable RSG devices are stated in the Distribution Interconnection Handbook (DIH) under TD-2306P-01 Customer-Owned Telemetry Procedure and TD-2306P-01 Customer-Owned Telemetry Procedure Attachment 2. A copy of TD-2306P-01 and TD-2306P-01 Attachment 2 are provided in Appendix A. These requirements are based on lessons learned throughout the execution of the EPIC 3.03 project.

In brief, the requirements are split out in the following fashion with some of the key requirements highlighted (the full list can be seen in the linked documents on the DIH webpage):

- Required Data Points
    1. Per-phase and total watts (W)
    2. Per-phase and total volt-amperes-reactive (VAR)
    3. Per-phase voltage (V)
    4. Per-phase current (Amps)
- Functional Specifications
    1. Must be CSIP-certified for IEEE 2030.5 running the latest version of CSIP.
    2. CSIP version needs to be able to update.
    3. Proven interoperability with PG&E's DER Headend Servers.
    4. Must be able to provide LogEvents as described in TD-2306P-01 Customer-Owned Telemetry Procedure Attachment 2.
    5. Etc.
- Non-functional specifications –
    1. Embedded OS on RSG device.

    2. Min/Max operating temperature.
    3. Outdoor installation compatible.
    4. Required to initiate communications with DER Headend Server.
    5. Default posting rate of 30 seconds.
    6. Etc.
- Cybersecurity
    1. Terms of connection with PG&E network.
    2. Required cipher suite.
    3. Guidelines for practicing good cybersecurity hygiene.
    4. Cybersecurity event identification, assessment, and response.
    5. Etc.
- Maintenance Specifications
    1. Customer and RSG device vendor are responsible for maintaining good working telemetry.
    2. Customer and RSG device vendor are responsible for all updates and security patching.
    3. Timeframe for remediation of any issues.
    4. Ability to securely update RSG device remotely.
- Cellular Strength (discussed below)

Key lessons learned for the RSG devices over the course of the project include:

1. The original requirement was for the RSG devices to use a Private APN over a cellular network to connect to the PG&E ODN. The initial demonstration at Blue Lake Rancheria (BLR) was deployed this way. The Private APN does not allow an internet connection and PG&E does not allow dual-homing for a device connected to the PG&E ODN. With these communication limitations the RSG vendor did not have remote access to the device for troubleshooting. Another challenge with the Private APN is only PG&E can order the subscriber identity module (SIM) cards. This is an additional cost that PG&E would have had to pass to the customer and would have required an additional contract where the customer would have to pay PG&E for the monthly cellular usage charges. As discussed in the internal architecture section 4.2.2 of this document, due to these challenges the decision was made to implement a new network architecture that allows the RSG devices to connect to PG&E over the public internet.
2. The RSG device at BLR exhibited stability problems. Onsite power cycles of the RSG device were required to re-gain functionality and eventually the RSG device stopped communication even after power cycles. This highlighted the need for remote management of all RSG devices.
3. The requirement for the RSG devices to connect from a static IP was originally for two reasons: first, because the DER Headend Server used the source IP to identify the RSG device, and second, because an “allow list” was originally used at the load balancer on the internet facing edge of the PG&E network. The requirement for the allow list at the load balancer was removed by cybersecurity through the course of the project. A penetration test of the server was done where the attacker had full control of an RSG device with a registered certificate. This can be seen as a worst-case scenario. The penetration test did not result in any high level or critical findings. The static IP requirement is still in place because the DER Headend Server requires it for operation but in the future a different method of authentication will be used for allowing traffic between RSG devices and the DER Headend that allows dynamic IP addresses.

4. The original requirement was for the end device (energy producing or metering device) to connect to the RSG in a non-routable communication interface. This essentially means a serial interface. Serial interfaces are already becoming non-standard and at some point in the future could no longer be available on smart inverter and metering devices. As the security posture of the DER Headend System evolved to view the RSG as an untrusted device it was no longer required to have a non-routable end device.
5. An active area of discussion throughout the project was which certificate authority would be used for the SLL certificates. SunSpec certificates use Kyrio as the certificate authority and that is the only option for publicly available CSIP conformant certificates. PG&E decided early that it would not provide self-signed certificates to RSG vendors because it is far outside the scope of the utility's operations. The DER Headend Server is not currently using the CSIP specific fields in certificate so it is possible for a generic web certificate to be used but that would require either agreement on a certificate authority or support of multiple authorities. There was some concern with the cost of the SunSpec certificate . The final decision was to move forward with SunSpec certificates because it conforms with CSIP, allows future use of CSIP specific fields, and provides an industry standard for interoperable certificates.

Gateway Telecommunications Requirements

Cellular: To ensure the telecommunications connection between the RSG and the DER Headend Server is robust, PG&E provided guidelines for assessing the cellular connection at the installation site to ensure good connectivity. The cellular signal strength is measured using the Berkeley Varitronics Systems – Octopus Cellular Signal Meter Pro Kit[35]. PG&E uses this device to measure cellular connectivity because using a cell phone to do so gives false positive results for connectivity. The cellular signal strength metering device measures Referenced Signal Received Quality (RSRQ) values. Locations with RSRQ values measuring less than -14 dB should not be installed. Reference Table 3 for RSRQ values.

Table 3: RSRQ and RSRP values in highlighted green are sufficient for good connectivity.

If RSRQ (dB) is=	Then RSRP (dBm) must be:
≥ -9	≥ -105
-10	≥ -104
-11	≥ -103
-12	≥ -102
-13	≥ -91
-14	≥ -87
-15	NA - Do Not Install
-16	NA - Do Not Install
-17	NA - Do Not Install
-18	NA - Do Not Install
-19	NA - Do Not Install

Local Area Network Connection: Additionally, customers can connect their gateways to the internet through a local area network (LAN). To date no customers have chosen this option, but

[35] Berkeley Varitronics Systems – Octopus Cellular Signal Meter Pro Kit https://www.bvsystems.com/product/octopus-cellular-signal-meter-kit/

it is a way to reduce the cost of telecommunication services further by leveraging existing internet service at the site.

4.3.4 Aggregator Integration

An alternative to RSG devices installed at the customer sites and communicating directly with the DER Headend Server is the option to use an aggregator. As can be seen in Figure 9, an aggregator server directly communicates to the DER Headend Server using the IEEE 2030.5 protocol. The aggregator server can, meanwhile, collect data from several different DER sites using any preferred communication protocol and translate this to IEEE 2030.5 when forwarding the information to the DER Headend Server.

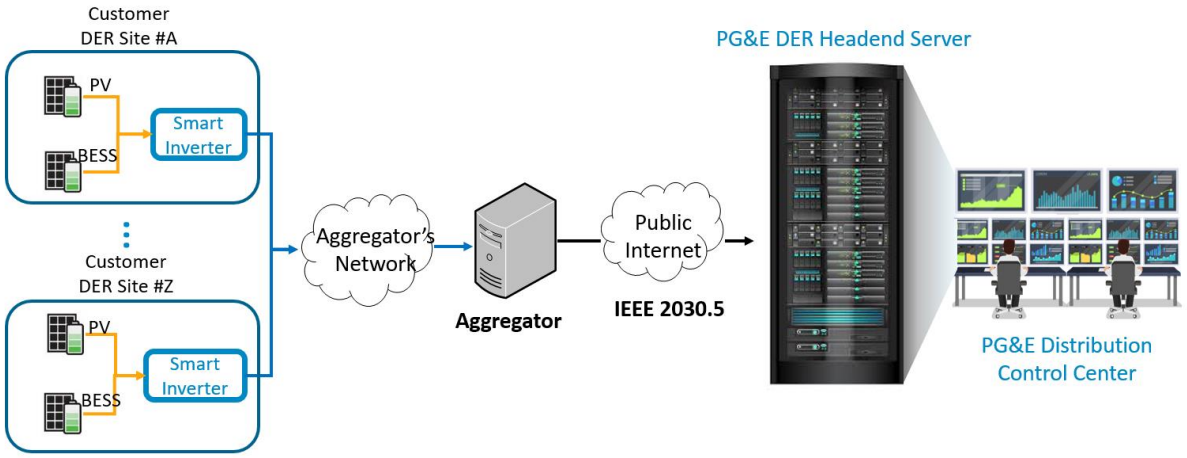


Figure 9: Simplified overview of the DER Headend System using an aggregator.

This method of integration has several potential advantages:

- **Ability to leverage existing communications links and data streams that DER developers have with their customers' DERs.** Many developers have existing communications with the DERs that they install for their customers. Using an RSG device would be a redundant data collection and transmittal to PG&E's DER Headend Server. The aggregator server would gather these DER sites' data and transmit it to the DER Headend Server leveraging that single connection and removing the redundancy. This can further reduce the cost for meeting telemetry requirements in two ways:
    - **Removes redundant telecommunications linkage for customers' DERs –** Instead of two telecommunications connections, one to PG&E and one to the DER developer or technology provider, there would only be one to the DER developer/technology provider removing the monthly fees to a cellular carrier.
    - **Lower cost gateway device –** Vendors claim that the gateways used with aggregators could be lower cost than those for RSG devices because they have fewer requirements and can use other types of communications protocols (e.g. Modbus or vendor specific protocols).
- **Reduces the number of nodes that connect to the PG&E network –** From a cybersecurity perspective, the aggregator connections reduce the size of the potential attack surface into PG&E's network. Fewer connections directly into PG&E from customer sites and instead one from an aggregator is preferable and adds an additional layer of abstraction.

PG&E has so far certified three aggregators as interoperable with the DER Headend Server. The aggregator server can be specifically operated by the DER developer either by licensing

aggregator software from an aggregator vendor or by developing their own IEEE 2030.5 aggregator server. The other option is for a DER customer to leverage an aggregator vendor that houses their own aggregator server. In either case, the aggregator server would have to be certified-interoperable with PG&E's DER Headend Server before it can be made available to PG&E interconnection customers.

Aggregator Testing

Aggregator interoperability testing with the first aggregator vendor was completed without any major issues because this testing was done after the interoperability testing of the RSGs were completed. The changes to the DER Headend Server to be accommodating of the varying communication methodologies used by the RSG devices proved effective when incorporating a new vendor. The only modification required on the aggregator side was to copy the response pattern that was developed for the RSG devices when the DER Headend Server restarts. This vendor worked with a DER developer and collected the metering data directly from their inverters and then did the mathematical aggregation to present multiple inverters as a single generation source.

After successfully testing the first aggregator vendor's software, the software was deployed in the DER developer's own network. A demonstration was performed where the DER developer had generators deployed in Chico, CA. The aggregator software was successful in communicating with the inverters in the field and providing the telemetry data to the DER Headend Server. Data reporting from this demonstration site was monitored over the course of one month. There were two communication outages caused by the aggregator that lasted over five minutes, and both of them occurred because the aggregator lost communications with the inverters. Communications were recovered after one hour on the first outage and a half-hour on the second. In both cases the recoveries were executed automatically.

Three additional aggregators were tested and have completed testing at the time of this report. These aggregators are from the same vendors previously tested but they are deployed on the cloud so any customer can utilize them. Because the IEEE 2030.5 interoperability testing was already completed with alternative products no interoperability issues were encountered with any of these aggregators.

One PG&E network issue was exposed during aggregator testing. Part of the cloud aggregator testing is to simulate 50 end devices and post the telemetry data for all end devices. The purpose of the test is to see how the DER Headend System reacts to high volumes of traffic from a single source. It was found that some of the requests were dropped before they could reach the DER Headend Server. While troubleshooting, the aggregator disabled concurrent requests and then all the requests made it to the DER Headend Server. The issue is still being investigated to determine where in the network the requests are being dropped. Both aggregators that completed testing incorporated a retry mechanism in the event the requests are dropped. Because this issue only happens at higher traffic volumes it does not have an impact at the moment, so the cloud aggregators are available for use by interested customers while the issue gets resolved.

4.4 Cybersecurity

4.4.1 Cybersecurity Assessment

PG&E and a contracted cybersecurity vendor assessed the cybersecurity of the system through each network architecture iteration. The following risks were identified through review of the network architecture that were mitigated in the following ways:

1. **Data injection into operational data network –** Risk mitigated through appropriate firewalls and application layer inspections. Enacted multi-level segmentation to contain any risk of lateral movement and limit impact to PG&E control system applications. Implemented identity and access management (IAM).
2. **Data termination points -** Several endpoint protection and monitoring systems including monitoring for security events.
3. **Implementation of IEEE 2030.5—**Application of NIST high risk controls[36].
4. **Denial of service, spoofing, and tampering –** Controlled through application of boundary protection devices.
5. **Expanded attack surfaces –** Limited the landing into specific isolated network zone. Disabled unnecessary protocols and ports.
6. **Multiple-third parties –** Thorough and detailed risk analysis of each vendor and the devices they provide.
7. **Untrusted networks –** Implemented zero-trust model.
8. **No utility control of physical site and network –** Implemented zero-trust model because PG&E has no control over the physical site, network, and device.
9. **Diverse and untraceable DER hardware –** Not approving any vendor device from a cybersecurity perspective, only focusing on functionality and compatibility. Also implemented zero-trust model.
10. **Non-repudiation risk** – PG&E assessed the risk of bad data being received from devices. PG&E implemented historical data algorithm on the operations side to be able to identify and react to anomalies. The non-repudiation risk is discussed further below.

Overall, the DER landscape and the understanding of all parties evolved significantly over time. Hence it was deemed appropriate to revisit the requirements.

After considering all the details, PG&E cybersecurity recommended:

- That all RSG devices and Aggregator connections must be considered “Zero Trust” devices and connections.
    - The fact that devices are not under the control of PG&E’s IT, along with the lack of visibility into configuration of the RSG devices and remote management required PG&E to consider customer-owned devices zero-trust. As a result, PG&E does not apply any cybersecurity requirements. PG&E instead recommends industry best practices as developed and published in the DIH guidance document[37]. The RSG

[36] National Institute of Standards and Technology. (2020, December 10). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[37] Pacific Gas & Electric Company. (n.d.). TD-2306P-01: Customer-Owned Telemetry Procedure, Section 6. Retrieved from

device originating IEEE 2030.5 communication leverages SSL and device certificates to establish legitimacy.

- Vendors must be required to be aligned with IEEE 1547.3 and be compliant with the requirements of CSIP and SunSpec.
    - Non-compliant devices are not allowed to connect to the PG&E network and are assessed before becoming certified-interoperable
- No additional "PG&E" managed penetration test is required for RSG devices and aggregator connections. More information on this is in the penetration testing section below.

Finally high-risk controls derived from the National Institute of Standards and Technology (NIST) framework[38] were applied to improve the security posture and address the issues found in design and development of the system. To verify and confirm the effectiveness of the controls, penetration testing was conducted.

4.4.2 Cybersecurity Penetration Testing

PG&E enlisted the services of a third-party cybersecurity vendor to perform a security assessment of PG&E's EPIC 3.03 Application Programming Interface (API). The API is a DER management interface that allows client devices (e.g. gateways and aggregators) to communicate with end devices that sit behind the API server. Communication between RSG devices and the DER Headend Server is performed according to the IEEE 2030.5 specification. The goal of the engagement was to review the EPIC 3.03 API for vulnerabilities that could affect PG&E's overall security posture in a negative way and provide guidance and strategic support to resolve any identified issues.

The cybersecurity vendor observed that the API was not sufficiently validating input data sent in commands to end devices. Invalid inputs can be sent to the API to unsafely modify end device settings. Although requests must be authorized with a valid TLS certificate, the API's security model should account for scenarios in which an authorized client device is controlled by a malicious actor or a valid client certificate is stolen. Any external data parsed by the API should be considered untrusted and validated for safety even if it's coming from an authorized source. This allows a malicious consumer of the API to modify end device settings in ways that could cause the device to function unsafely.

Through penetration testing, it was determined that the only issue that could not be mitigated would be the reliability of the data that PG&E is receiving from the field of customer-owned devices. This issue is called data non-repudiation. This risk was discussed with PG&E operations engineers to determine what kind of issue this would cause with managing the system. PG&E operations engineers commented that they utilize historic telemetry data from all available metering points on the grid (including DERs) to make grid decisions and switching operations and that while the data from the DER is useful for these decisions, it is not the only data point that goes into making switching decisions for the grid. As a result, PG&E operations engineers were comfortable managing the system with the non-repudiation risk.

https://www.pge.com/includes/docs/pdfs/shared/customerservice/nonpgeutility/electrictransmission/handbook/TD-2306P-01.pdf

[38] National Institute of Standards and Technology. (2020, December 10). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Overall, the DER Headend System demonstrated generally good security practices that bring the API in line with all of the IEEE 2030.5 specification's security requirements. The API enforces the specification's TLS cipher security requirements, and the certificate-based end device authorization model is implemented successfully.

Strengths of the design and cybersecurity controls applied were discovered and confirmed:

1. Strong Authorization Controls
    a. Throughout the course of the assessment, authorization controls were checked to ensure the API did not disclose other end devices' data to unauthorized users. The controls in place proved to be effective in preventing such information disclosure.
2. IEEE 2030.5 TLS Security Requirements Met
    a. The API requires the use of TLS 1.2 with a very strong cipher suite, which means the API is compliant with IEEE 2030.5's mandates on TLS security.
3. No Injection Vulnerabilities
    a. Testing did not identify any vulnerabilities that would allow an attacker to inject their own code or payload
    b. Firewall and application layer inspection to eliminate any inward attack vectors
    c. Multi-level segmentation to contain any risk of lateral movement and limit impact to PG&E control systems applications
    d. Implementation of identity and access management (IAM)
    e. Several endpoint protection and monitoring systems
    f. Security event monitoring
    g. Passive monitoring for OT protocol malfunctioning

In a parallel effort, the internal environment was penetration tested by the same cybersecurity vendor and the following strengths were confirmed:

1. **Directly Exploitable Issues Within the Internal Network Environment**
    No directly exploitable issues were identified within the internal network environment tested that would allow a compromise of the target system or data.
2. **Web Server Configuration**
    The web servers hosting the applications were found to be up to date and well configured. No vulnerabilities related to web server configuration were uncovered.

The favorable results of the penetration testing attested to the strength of the network architecture that was designed and the ability for PG&E to allow the connections of untrusted devices onto the network. As a result, PG&E determined that it did not need to penetration test new RSG devices and aggregators in the process of certifying them as interoperable with the DER Headend System. Over the course of the project and while demonstrating the RSG devices but prior to penetration test completion, PG&E was concerned with the liability and risk of these systems on the network. The demonstration sites were required to sign cybersecurity agreements to ensure cybersecurity requirements were being implemented by customers at their DER sites. Some demonstration partners balked at the breadth of the agreement's liability provisions. Following the completion of the penetration testing, PG&E determined the risk was low enough to remove the cybersecurity agreement and many of the provisions

and requirements within the agreement. The site cybersecurity requirements became recommendations, and the liability provisions were reduced significantly[39].

4.4.3 Cipher Suite

As discussed in the regulatory section of this report, the cipher suite that PG&E had chosen based on what would work with PG&E's network firewalls and edge devices required the RSG device vendors to use a compatible cipher suite. This cipher suite (TLS_ECDHEECDSA-AES128-GCM-SHA256 (oxc02d) GCM (GCM cipher)) was different from the one that was suggested in CSIP 2.1 for gateway devices (TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (CCM cipher))[40].

At a mid-point presentation of the EPIC 3.03 project's challenges and progress, the issue arose that PG&E was not using the CSIP preferred CCM cipher. Through discussion there was concern that choosing a different cipher suite would leave thousands of smart inverters that have been deployed out in the field without the ability to communicate back to the utility's data systems. Under the requirements for Rule 21 section Hh.5.b.iv[41], which became applicable September 8, 2017, the default communication protocol for smart inverters is IEEE 2030.5 as defined in version 1.0 of the *Common California IOU Rule 21 Implementation Guide for Smart Inverters*[42] published August 31, 2016, and there was fear that this amounted to hundreds of thousands of smart inverters that fell under these conditions. It is important to emphasize that these devices, many of them for residential interconnections, did not have a use case requiring communications with PG&E in the near future.
There was a request from the CPUC Energy Division to assess whether there were other solutions to be able to communicate with these devices without using the LBE device and, additionally, to perform a survey (section 4.1.1) to assess what the extent of the impact of choosing this cipher was on that installed base of smart inverters.

It was also determined, following analysis of the CEC inverter list[43], that over 99% of the smart inverters used a gateway or an aggregator to meet their CSIP-certification. This means that if utility integration of the installed base of CSIP-certified smart inverters was needed, the gateway installed at the site would either use the compatible cipher suite or that the DER would use an aggregator to integrate with the utility. As elaborated in the regulatory section 4.1.1, the smart inverter vendors that were surveyed said that aggregator and then gateway were their preferred approaches to integrating with the utility network with the least preferred being direct-to-inverter integration.

Cipher suite related survey results:

[39] TD-2306P-01: Customer-Owned Telemetry Procedure, Section 6. https://www.pge.com/includes/docs/pdfs/shared/customerservice/nonpgeutility/electrictransmission/handbook/TD-2306P-01.pdf
[40] CSIP Version 2.1 (2018) section 5.2.1.1
[41] Pacific Gas and Electric Company. (2018, June 30). Electric Rule No. 21 Generating Facility Interconnections. San Francisco, CA.
[42] Common Smart Inverter Profile Working Group. (2018, March). Common Smart Inverter Profile: IEEE 2030.5 Implementation Guide for Smart Inverters Version 1.0
[43] California Energy Commission. (n.d.). Grid_Support_Inverter_List_Simplified_Data_ADA. Retrieved from https://www.energy.ca.gov/sites/default/files/2021-10/Grid_Support_Inverter_List_Simplified_Data_ADA.xlsx

13. Can your Smart Inverter be updated remotely to use alternative cipher suites? e.g. using ECDHE-ECDSA-AES128-GCM-SHA256 (oxc02d) (GCM) cipher suite
    a. Yes
    b. No
    c. Other

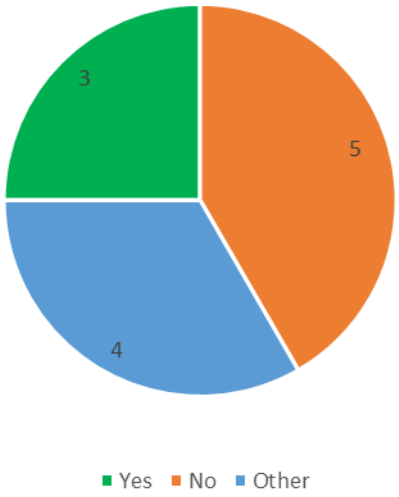


Figure 10: Are you able to update your smart inverters to the new cipher suite.

As noted earlier, there was confusion about whether the question was related to the smart inverter alone or the gateway. This contributed to mixed results in the responses. Those respondents using a gateway or aggregator said that they were able to update the cipher suite because they would just update the gateway or aggregator to accommodate the new cipher suite. Those that interpreted the question with their ability to update the smart inverter said that they would not be able to update the cipher on the smart inverter and that, in one case, the computer system on the smart inverter would not be capable of handling that level of computer processing.

14. How would you characterize the level of impact (in terms of cost, complexity, and time) of requiring the use of the GCM cipher in order to integrate with a utility headend system?
    d. Minimal impact (e.g. straightforward, over-the-air update)
    e. Moderate impact
    f. Large impact (e.g. extensive reprogramming of inverters and physical visit to site for manual update of inverters)
15. Please comment on your above choice.

Analysis: The responses for the level of impact for changing the cipher suite for an installed smart inverter again depended on the interpretation of the question by the respondent. If they interpreted the question as being able to update a gateway or aggregator, they responded that the cipher suite update would cause a minimal impact or moderate impact.

> "We use cloud integration for Smart Inverters" … "if GCM needs adjustment, it can be done in the cloud setting files easily,"

One respondent said that they would be concerned that the update would invalidate their CSIP-certification and would require retesting and certification.

> "We use a vendor's certified gateway. This question applies to the gateway. An important question is if this update can be made without invalidating previous integration testing + certification for users of the gateway."

If they interpreted the question with regard to the smart inverter needing to be updated, there was more anxiety about having to update a cipher suite with moderate to large impact being chosen. This is where some vendors commented that they would have to visit sites with installed smart inverters and put into place engineering resources with truck rolls to update the devices.

> "This would involve engineering resources, time and also require an update to expensive and time-consuming certifications. Firmware updates may also require site visits. So the response of "yes" to [question] 12 means that it could be done (even if it required a firmware update), but the impact depends."

4.4.4 Public Static IP vs Dynamic IP

The current design of the system is based on dynamic IP addressing. While this may seem counterintuitive, in this specific case static IPs represented a lessor cybersecurity risk to the IOUs. The network architecture and design leveraged the use of static IPs primarily as a cybersecurity risk mitigation measure. Static IPs are not without their downsides, the use of static IPs can expose an IOU to future attacks via reconnaissance missions (via the DER). The alternative would be to use dynamic IPs, which was believed to pose a greater cybersecurity risk. PG&E has the capability to isolate their internal networks and systems by adding to the 'allow list' the DER's known static IP. This allowed PG&E greater control over access by only allowing known entities to access the systems. If a dynamic IP was used, PG&E would need to allow all IPs access to the edge devices and network entry points, which would greatly increasee the cybersecurity exposure.

The challenge associated with dynamic IPs includes the expanded attack surface and attack vectors but has the advantage of requiring that bad actors determine what a dynamic and changing IP address is instead of a static one. For this instance of the DER Headend Server, the compensating controls required to mitigate the increased exposure would have resulted in delays to the implementation of the DER Headend System, and add significant costs and complexities (people, process, technology). Adding the compensating controls would, in itself, be an additional risk given the additional processes and tools to keep the updated controls managed and monitored.

The current design of the new DERMS and its DER Headend, that will replace the DER Headend System deployed in EPIC 3.03, is based on dynamic IP addressing. This is to accommodate a better cybersecurity posture for the DER gateway devices and customer infrastructure. It will do so by having the internet facing edge device use IP based geolocation for the source IP and block access to IPs from regions outside the country. Additional network devices will validate the DER client's identity using device certifications (PEM) which would be pre-registered (out-of-band) and will block access to unregistered devices even if a bad actor modifies the source IP address or performs re-routing.

There was discussion throughout the project that due to a limited number of static IP addresses available within IPv4 that PG&E should consider using IPv6. IEEE 2030.5 specifies DNS-based methods for service discovery, resource discovery, and hostname to IP address resolution. A service is defined as an application instance uniquely identified by {host, port, protocol}, where protocol in this case is IEEE 2030.5 plus its underlying transport bindings (e.g., HTTP(S)/TCP/IP). DNS-based Service Discovery (DNS-SD) (IETF RFC 6763) is a conventional use of existing DNS name syntax and message and record formats to discover instances of a given service within a given domain. The current DER Remote Site Gateway and DER Headend Server support IPv6 addresses but PG&E's network does not allow the use of IPv6 address routings at the time of this writing. In order for PG&E to allow IPv6 IP addresses, it would need to engage in a much broader effort to redesign the network architecture to allow for that. Since the new DERMS system that is replacing this version of the DER Headend will allow dynamic IP addresses, the limited number of static IP addresses will no longer be a pressing issue.

4.4.5 Cybersecurity Key Conclusions and Recommendations

Cybersecurity was a central element and a key challenge for this project. The DER Headend System requires connection of customer-owned untrusted devices into a controlled utility environment. PG&E's understanding and assessment of this connection was developed through various network re-architectures and stress tests of the system. As a result of this work, PG&E was able to successfully use this system over the public internet allowing for this to be a low-cost system for customers to use.

Key conclusions and recommendations:
The number of stakeholders for implementing this system, including RSG/aggregator/server vendors, customers, developers, and the utility, makes standardization important. Continued work on standardization will only help enhance interoperability among systems. For this reason it is best for PG&E's cybersecurity and monitoring jurisdiction to ensure conformance through leveraging these standards and requiring conformance with them. Requirements like 'compliance with 1547.3' or 'compliance with IEEE 2030.5' help PG&E and the industry ensure a robust, interoperable environment for DER communications.

The industry should leverage entities like EPRI and the various national labs to drive standardization of communication and cybersecurity protocols and requirements. Additionally, working groups through the CPUC and other regulatory bodies are valuable forums for industry collaboration.

As part of the development of this system for customer use, PG&E has uploaded its expectation for cybersecurity best practices in the customer-owned telemetry procedures document posted on the DIH website.[44]

The EPIC 3.03 project allowed PG&E to demonstrate that a low-cost customer-owned system communicating over the public internet is possible through mitigation of various attack vectors. The learnings from the development of this system will go to enhance the future rollout of the DERMS DER Headend.

[44] TD-2306P-01: Customer-Owned Telemetry Procedure, Section 6.
https://www.pge.com/includes/docs/pdfs/shared/customerservice/nonpgeutility/electrictransmission/handbook/TD-2306P-01.pdf

4.5 Interoperability

4.5.1 Description of Test Setup

PG&E performed functional acceptance testing between RSG devices from each vendor and the DER Headend Servers. The main objective of the testing was to ensure that the DER Headend Server and vendor RSG devices operated properly under various conditions. This was done prior to promoting the system and RSG vendor offerings to production in the field.

As seen in Figure 11, the Vendor #1 RSG device communicates with the IEEE 2030.5 testing server over a cellular connection on the internet using HTTPS. The IEEE 2030.5 testing server is accessed through a Windows Remote Desktop connection. The Vendor #1 RSG device has 2 ethernet ports. Port 1 is connected directly to the testing laptop for device management. Port 2 is connected to the testing network where the TCP Modbus end devices are. The meter communicates with the Vendor #1 RSG device by TCP over the testing network. USB serial adapters are used on the testing laptop to create Serial Modbus end devices that the Vendor #1 RSG device can communicate with. The testing laptop is used to simulate TCP and serial Modbus end devices.

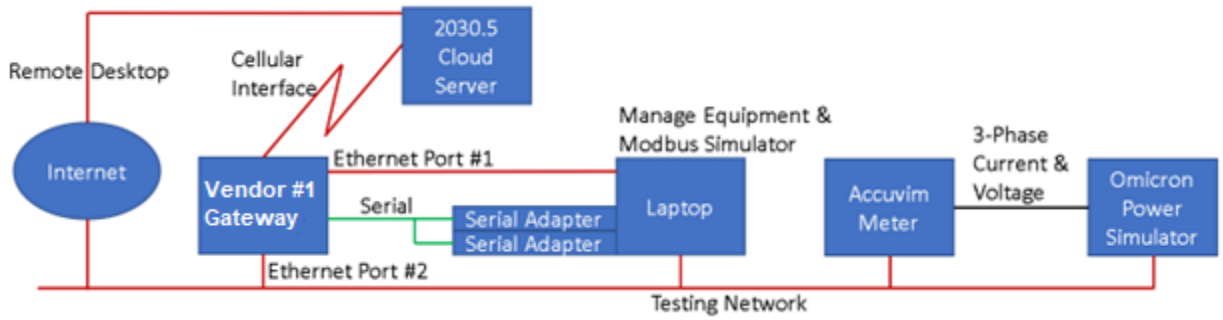


Figure 11: Vendor #1 device communication setup.

Figure 12 shows, Vendor #2 RSG device communicates with the IEEE 2030.5 testing server over a cellular connection on the internet using HTTPS. The IEEE 2030.5 testing server is accessed thought a Windows Remote Desktop connection. The Vendor #2 RSG device has 2 ethernet ports. Port 2 is connected to the cellular modem. Port 1 is connected to the testing network where the TCP Modbus end devices are. Device management of the Vendor #2 RSG device is done over the testing network. USB serial adapters are used on the testing laptop to create Serial Modbus end devices that the Vendor #2 RSG device can communicate with. The meter is connected to the Vendor #2 RSG device using a serial connection. The testing laptop is used to simulate TCP and serial Modbus end devices.

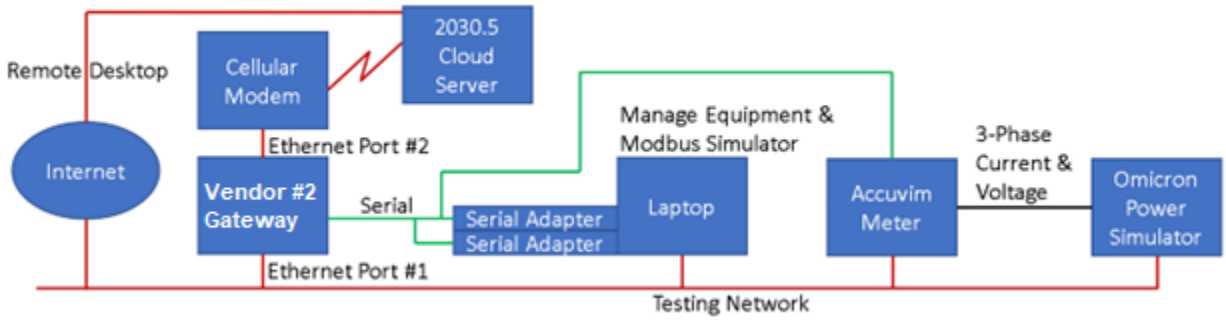


Figure 12: Vendor #2 device communication setup.

4.5.2 Key Findings

CSIP certification is an important step towards interoperability, but it does not guarantee that servers and clients will be able to communicate with each other. The CSIP system is based off a stack of technologies (Figure 13) that need to be interpreted in a consistent way by the industry to ensure interoperability between CSIP certified devices.

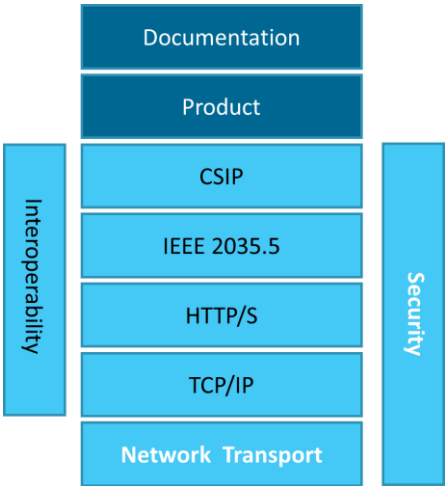


Figure 13: Stack of technologies layered under CSIP.

The following communication/protocol issues between server and clients were found after the server and clients received their CSIP certification.

1. Implementation of TCP was different between the server and one vendor client. While not directly an IEEE 2030.5 issue, since IEEE 2030.5 is built on top of TCP, it impacted the ability to maintain communication between the RSG client and the DER Headend Server.
    - The server implementation assumed that there would be only one active TCP session from a single source IP. This is a common communication method in SCADA. After it was discovered that one of the clients will initial multiple TCP sessions simultaneously the server changed its implementation to accommodate this.
2. An RSG client requested the location to post Mirror Usage Point (MUP) with a single data point, and then later added the rest of the data. This is valid in IEEE 2030.5 but not tested in the CSIP-certification and was initially not supported by the DER Headend Server as they did not envision the use of this method. The RSG client in CSIP-certification adds all data when requesting the MUP location.
    - The server was modified to allow adding additional MUP data points to an already existing location.
3. An RSG client signaled an error and would restart because it was not given a FunctionSetAssignment (FSA) (used for control). Since this is telemetry only testing (no control), an FSA was not given, but the RSG client should still function even without an FSA.
    - The RSG client was modified to signal a warning instead of an error when no FSA is given. This allowed the RSG to proceed with registration and MUP posting when no FSA is given.
4. The installed DER Headend Server destroys existing locations for MUP data after a restart and the RSG clients need to request new locations. Agreement was required on the error code signaled if an RSG client posts to the wrong MUP location so that the RSG client can request a new MUP location.

- The server provides a 404 response when posting to a non-existent location and the clients are instructed to re-register when receiving 404 responses to MUP posts. Additionally, the location names at the server are created deterministically so there is no risk of a client posting to a location that was created for a different client.

5. The DER Headend Server uses the IP address and certificate to identify RSG devices. One RSG client vendor creates multiple IEEE 2030.5 clients, each with their own certificate to support multiple energy devices communicating on a single RSG. The DER Headend Server is unable to differentiate between the energy devices in this configuration.
    - The server was modified so the clients are tracked by socket instead of source IP. When a TCP session ends the socket is destroyed. When a new session starts the TLS handshake provides the client certificate and that is used again with the socket to track the traffic associated with the client. Additionally, it was required to disable TLS caching at the load balancer to ensure the client certificate was provided with each new session.

4.5.3 Test Results

Table 4: Test Case Results Summary

#	Test Case	Objective	Vendor #1 Result	Vendor #2 Result
1.01	DERMS Headend and client configured to communicate with each other	Confirm proper communication is established between the DER Headend Server and RSG client after configuring the DER Headend Server, RSG client, and any intermediary cybersecurity devices to communicate with each other.	PASS	PASS
1.02	Client communicates telemetry and log events to the headend	Confirm all required telemetry points from BLR are communicated and refreshed in near real-time (< 30 seconds) from the RSG client to the DER Headend Server with correct scaling, units, and Modbus-2030.5 translation.	PASS	PASS
1.03	Change decimal points and units of measure for incoming telemetry data	Confirm the DER Headend Server can modify the decimal point scaling and vary unit of measure. For example, change scaling and units from Volts to kVolts.	PASS	PASS
1.04	DER Headend Server and RSG client will resume proper operation after loss of power/comms to one or more devices	Confirm DER Headend Server and RSG device will provide the appropriate alarms and can recover from power being removed and returned to the DER Headend Server, RSG device, and DER simulator.	PASS	PASS
1.05	Security related log events are properly communicated	Confirm security related log events are properly communicated including any physical security or tampering alarms available.	NOT TESTED	NOT TESTED

1.06	Update DER Headend Server and RSG client time	Confirm that the RSG device will update its internal clock based on the time from the DER Headend Server.	FAIL	PASS
1.07	Change posting frequency	Update posting frequency from the DER Headend Server to increase (2 seconds) and decrease (2 minutes) posting rate from the standard	PASS	PASS
1.08	Update site information by adding and removing a meter	Confirm that the DER Headend Server and RSG device can be reconfigured to allow for the addition or removal of onsite metering points (e.g. new PV installation).	PASS	PASS
1.09	Update registration information at the DER Headend Server	Update DER site information within the DER Headend Server including: Display Name, Feeder, Certificate information, PIN, IP Address.	PASS	PASS
1.10	Use template for adding new clients to DER Headend Server	Confirm DER Headend Server has a method to use templates to ease the configuration of new DER sites into the DER Headend Server	PASS	PASS
1.11	Use template for configuring RSG client	Confirm RSG device has a method to use templates to ease the configuration of new RSG client devices	PASS	PASS
1.12	Update registration information in the RSG client	Update registration information within the RSG client including: Certificate Information, PIN, IP Address	PASS	PASS
1.13	Update firmware on RSG client remotely	Remotely manage the RSG device to update RSG device firmware/software.	PASS	PASS
1.14	Revert to previous firmware on RSG client	Remotely manage the RSG device to revert RSG device firmware/software to a previous version.	PASS	PASS
1.15	Receive multiple serial and IP inputs	Connect the RSG device to multiple serial and IP input connections to verify data can be received and transmitted from various onsite devices.	PASS	PASS
1.16	User Access Management	RSG devices will provide a means of authenticating users connecting to the RSG device	PASS	PASS
1.17	Access Control List Updates	Update the Access Control List to allow and block RSG devices from communicating with the DER Headend Server.	PASS	PASS

Table 5: Identified Issue Summary

Priority	Closed / Fixed	In Development	In Research	Deferred	TOTAL
Critical					
High					
Medium		2			**2**
Low	4		1	2	**7**
TOTAL	**4**	**2**	**1**	**2**	**9**

Table 6: Identified Issue Descriptions

Device	Priority	Description	Comments
Server	Low (Research)	In Vendor #2 TC 1.01 it is observed that the status field in the Comm Monitor does not accurately report the status of the Self Device. It shows Fail when the server is operating properly.	Low because not happening in production DER Headend Servers and didn't affect operation of system.
Server	Med (In Dev)	In Vendor #2 TC 1.04 it is observed that device communication status remains normal during a 6-minute communication outage.	Medium because it impacts ability to determine communication status. Server Vendor working on solution.
Server	Med (In Dev)	In Vendor #2 TC 1.08 it is observed that the end devices under an aggregator show a communication status of Failed when they are Normal.	Medium because it impacts ability to determine communication status. Server Vendor working on solution.
Vendor #1	N/A	In TC 1.05 the RSG device has an input suitable for an enclosure sensor, but this is not tested because we are not implementing PG&E custom LogEvents. (Not a defect)	Because we are not implementing the custom LogEvents in the DER Headend Server this is not a significant issue.
Vendor #1	Low (Deferred)	TC 1.06 showed the RSG will not post telemetry data when its time is mismatched from the server.	Low because the RSG is connected to the internet via a cellular connection its highly reliable to have an accurate time that matches the DER Headend Server. Ideally the RSG will take its time from the DER Headend Server but failing to post if the time is mismatched achieves the business objective of accurate timestamps on posted data. Vendor #1 informed of issue. Note – Vendor #1 resolved this issue with a software update after the project period had completed and the RSG device was in production.
Vendor #1	Low (Closed)	In TC 1.07 the minimum posting was 15 seconds, even though set to 2 seconds.	Low because the business requirement is 30 seconds, and at this time no need to go down below 15 seconds. This is greater than the 2 seconds test rate but ability to change

			the posting rate was demonstrated. Closed issue since no need to address this for telemetry.
Vendor #1	Low (Closed)	Note that TC 1.15 shows the RSG only allows 3 2030.5 clients. This is aligned with our requirement for all generation of the same type to be reported as a single DER.	Greater than 3 metering points at a site would require modifications to the RSG software, but should be able to handle majority of telemetry systems. Closed, will use a different vendor or will have to update code if need more than 3 clients at a site.
Vendor #2	Low (Closed)	In TC 1.05 the RSG hardware does not have an input suitable for an enclosure sensor.	Low, because we are not implementing PG&E custom LogEvents in the DER Headend Server the alarm for open enclosure cannot be implemented so this is not a significant issue. Vendor #2 has indicated they will not support the enclosure sensor alarm, PG&E agreed to this implementation.
Vendor #2	Low (Closed)	When reusing a configuration file, it is mandatory to change all MRIDs. This is demonstrated to work in TC1.12.	PG&E made Vendor #2 aware of this to consider when reusing configuration files. Closed, not a defect, but an implementation step.
Vendor #2	Low (Deferred)	When there are multiple serial devices in a single RS485 channel the devices are read in a round robin. When one device is not communicating then the timeout and retry for that point will execute before the next point will be read. This will create communication delays with the working device.	Low, this is something Vendor #2 needs to be aware of in implementation. When there are multiple devices in a single RS485 channel the communication timeout and retries should be adjusted so one down device does not impact the communications of the working devices.

4.5.4 Future of Interoperability Standard

There has been a lot of interest from utilities across the country and internationally with the implementation of this project. There is a push to standardize communications between DERs and utility systems as the grid becomes a more dynamic environment. PG&E has shared insights learned from this project with the industry and utilities through one-on-one meetings and through presentations at

conferences and regulatory forums. PG&E has also shared with SunSpec interoperability issues found during the implementation of the DER Headend System. Critically, SunSpec is looking to improve CSIP's interoperability through their "Non-Stop Interop" testing sessions.[45]

As interoperability improves, deployment of DER Headend Systems will improve. Additionally, implementation of DERMS software within the utility will include IEEE 2030.5 communications, further establishing IEEE 2030.5 as the communication pathway of choice into utility networks.

4.6 Demonstration Sites

To test the DER Headend, demonstration gateway, vendor RSG devices, and aggregators, PG&E needed interconnection customers with demonstration sites that met certain criteria:

1. PG&E DCC Operations Engineering needed to approve the demonstration site for conditional permission to operate (PTO)(conditional-PTO). This allowed flexibility for the project team in the event of delays or issues in deploying the telemetry system without impacting the DER customer's ability to operate and produce power from the DER. Interconnection customers not granted conditional-PTO for telemetry would be unable to produce power until their telemetry requirement is met.
2. Conditional-PTO or PTO would need to occur during the EPIC project's timeline.
3. Interconnection customer would have to agree to the terms of the demonstration agreement and the cybersecurity agreement to be involved in the demonstration.
4. Initially, the number of demonstration sites were limited based on resource availability so as not to overwhelm the EPIC team's bandwidth during commissioning of the RSG devices onto the DER Headend System and any issues that could potentially arise therefrom.

If a demonstration site and interconnection customer met the above criteria, they were added as a demonstration site for the project.

4.6.1 Blue Lake Rancheria – First Demonstration Site

Blue Lake Rancheria (BLR) is located in Humboldt County in the northern part of PG&E's service territory and the state of California. BLR's site "houses tribal government offices, EV charging, a convenience store and gas station, a hotel, restaurants, and casino, and energy, telecommunications, and water systems — including a low-carbon microgrid"[46]. These resources and the microgrid capability designated BLR as an American Red Cross emergency evacuation site. The microgrid includes 420kW AC of solar, 1,150kW/1950kWh battery energy storage system (BESS), and 1MW backup diesel generator. The BESS had been increased to 1,150kw/1950kWh from 500kW/950kWh in 2019 triggering the Rule 21 telemetry requirement for the site. The project team determined that BLR would make a great site to demonstrate the DER Headend System.

BLR was selected to be the first demonstration site for EPIC 3.03 project because PG&E has a long-standing relationship with Blue Lake Rancheria, the Schatz Energy Research Center at Cal Poly Humboldt, and Idaho National Laboratory. PG&E had worked with this team of collaborating organizations to support their development of the BLR microgrid. BLR had also been very enthusiastic and supportive of new endeavors with PG&E.

[45] https://sunspec.org/wp-content/uploads/2020/12/2020-Non-Stop-Interop-1.pdf
[46] https://schatzcenter.org/blrmicrogrid/

With the Server Vendor building the DER Headend System the team decided it would expedite the schedule if the Server Vendor also provided the gateway. The demonstration Server Vendor RSG device used a FirstNet connection to PG&E which was required for the initial network architecture. The FirstNet modem has the advantage of getting prioritized communications as opposed to a standard cellular data connection. As the public internet option was developed and became available, there was no longer a need for the FirstNet modem. The demonstration gateway that was originally installed at BLR was overbuilt for the requirements and would not be supported by the vendor long term.

The initial demonstration RSG device was the proof of concept to show that the DER Headend Server could work but the RSG device needed to be replaced with a production device. It was decided that it would be replaced with an aggregator service and BLR would again be at the cutting edge for the development of this system. See the section 4.3.4**Error! Reference source not found.** for more information. BLR has since successfully implemented a production aggregator telemetry system using an aggregator vendor at the site.

4.6.2 Gateway Vendor Sites

In July 2021, the EPIC 3.03 team began assessing projects in the interconnection queue as possible demonstration sites to test out RSG devices from the two vendors in the field. Projects that were chosen for inclusion in the customer-owned telemetry demonstration had to be slated for completion within the EPIC project's timeframe and had received or would receive approval from PG&E DCC Operations Engineering for Conditional-PTO status. The EPIC project team had initially wanted to limit this to five or so projects in order to not overload resources for troubleshooting and configuration work. Due to an internal lapse in communication, additional projects were offered COT in their study report. The EPIC team decided to include these sites in the demonstration and the total number of sites went up to eleven.

These pilot sites were required to sign a pilot agreement and a cybersecurity agreement in order to move forward with customer-owned telemetry during the pilot period. One customer was responsible for seven of the eleven pilot projects and this customer had issues with the indemnification and liability language in the cybersecurity agreement that are discussed further in section 4.8.2.2 of this report. The other four pilot sites signed were able to move forward after signing their agreements.

During the vetting process for pilot sites, the CPUC issued Resolution E-5038 on August 20, 2021. Ordering paragraph two of this resolution required PG&E to, "implement specific technical requirements for telemetering of distribution-connected systems 1 MW or greater and less than 10 MW. The adopted technical specifications for these systems are as follows: 1) facilities can report measurements in 15-minute increments using customer-owned, nonrevenue-grade metering and a data aggregation device comparable to the serial device server that SCE has historically required, 2) customers can choose to connect the reporting device to the utility Energy Management System via cellular modem or dedicated internet connection, and 3) measurements do not have to be made from revenue grade equipment. The Utilities shall submit Tier 1 Advice Letters to implement these requirements no later than 45 days from the issuance of this Resolution."

Following this announcement, PG&E was required to offer the customer-owned telemetry option back dated to October 4, 2021. Since the DER Headend System was still being demonstrated and was not ready for production, for DER interconnection projects that requested the use of customer-owned telemetry, PG&E set the following guidelines:

1. Projects should be reviewed for conditional-PTO without telemetry. Projects that are able to conditionally PTO for lack of telemetry should remain that way until the DER Headend System is in production.
2. If a project cannot receive conditional-PTO, the project would be included in the EPIC project's pilot.

This issue did not arise during the course of the project and the EPIC project was close enough to transition to production that it never became an issue.

On April 11, 2022, the first site that was ready installed a Vendor #2 gateway device at the site and received its SCADA release letter, followed by its PTO letter from PG&E. This site installed over 1MW of fuel cell generation at their site and required telemetry. There were challenges with getting the site operational. The PCC monitoring requirement was still in effect when the RSG was installed. The PCC meter is owned by PG&E so coordination with the PG&E meter team was required so the local Modbus communication interface could be tested at the site. The RSG has 2 serial ports, and the wrong port was set to RS485 which is required for the meter to communicate. This was discovered and corrected so the RS485 ports was used. The PG&E meter was configured and tested at PG&E's ATS lab before being deployed to the site so there were no issues with meter configuration. Another challenge that arose was a missing DNS configuration at the RSG. Without the DNS configuration the RSG was not able to resolve the provided host name. This was discovered by using the IP instead of hostname as a debugging step. After the issue was discovered the RSG configuration was updated, and it worked as expected. The configuration mistakes were minor and easily resolved. These types of issues are expected on a first installation and in total the installation was considered a success.

Following that, on May 2, 2022 the second pilot site using a Vendor #1 deployed RSG device received its SCADA release letter and PTO. The RSG at this site was collecting telemetry data from a site energy data acquisition system. The provider of the data acquisition system did not implement Vendor #1's requirements correctly and Vendor #1 had to make changes to the Modbus polling on their side to accommodate the data acquisition system's Modbus configuration. There was no opportunity to test with the data acquisition system being used in the field ahead of time so this was not an issue that could have been avoided but a resolution was accomplished via software update in the field. The site had two RSGs deployed, and one of the two units had a hardware issue which compromised its cellular communication. This unit was replaced, and an investigation was started with the RSG hardware vendor. These types of issues are expected on a first installation and in total the installation was considered a success.

The DER Headend System was finally moved into production on June 29, 2022. As of the writing of this report, seven customers are using RSG devices and two are using aggregators to fulfill their telemetry requirement to PG&E.

4.7 Performance

4.7.1 Data

The following data points are required for generator telemetry. All generators of a single type (i.e. PV, BESS, etc.) are to be aggregated and represented with a single set of values.

Table 7: Required data points from DER types.

Telemetry	Uom Type	Phase Code	Accumulation Behavior	Unit and Precision	Note
Current A	5	128	12	1 A	Always Positive
Current B	5	64	12	1 A	Always Positive
Current C	5	32	12	1 A	Always Positive
Voltage AN	29	129	12	0.1 V	Use for Wye
Voltage BN	29	65	12	0.1 V	Use for Wye
Voltage CN	29	33	12	0.1 V	Use for Wye
Voltage AB	29	132	12	0.1 V	Use for Delta
Voltage BC	29	66	12	0.1 V	Use for Delta
Voltage CA	29	40	12	0.1 V	Use for Delta
Active Power Total	38	224	12	1 W	Negative = Export to Grid
Active Power A	38	128	12	1 W	Negative = Export to Grid
Active Power B	38	64	12	1 W	Negative = Export to Grid
Active Power C	38	32	12	1 W	Negative = Export to Grid
Reactive Power Total	63	224	12	1 VAR	Negative = Capacitive Load
Reactive Power A	63	128	12	1 VAR	Negative = Capacitive Load
Reactive Power B	63	64	12	1 VAR	Negative = Capacitive Load
Reactive Power C	63	32	12	1 VAR	Negative = Capacitive Load

NOTE: Any Types not listed including CommodityType, DataQualifierType, FlowDirectionType, and KindType should be left blank or set to the default value of 0.

The data posting rate specified is 30 seconds. Interoperability Test 1.02 in Table 4 showed that the RSGs were able to meet the specification.

4.7.2 Health Monitoring

During interoperability testing it was observed that the communication health monitor that comes with the DER Headend Server was not tracking the device communications properly. There are two communication rates that are specified at the server. The "Polling Rate" is how often the IEEE 2030.5 client checks for updates from the DER Headend Server. The "Posting Rate" is how often the IEEE 2030.5 client sends data to the DER Headend Server. The polling rate is set to once per day and the posting rate is set to every 30 seconds. The DER Headend Server uses a multiplier on the polling rate to determine when the IEEE 2030.5 client has lost communication. Because the polling rate is once per day, this is too long an interval. Additionally, the communication status of devices that report through an aggregator are not having their communication health status tracked. Only the aggregator is tracked because that is the device responsible for communications. The DER Headend Server was released to production with these defects and resolutions to these defects are currently being worked on.

An alternative communication health tracking system was developed for use until the built-in system functions properly. All of the data is stored in ED-PI with timestamps. Once a day at 7 AM a python script checks ED-PI for all devices using the IEEE 2030.5 data templates. The timestamp for the last reported value is checked and if the timestamp is over one hour old it is marked as failed communications. An e-mail report is sent which lists all devices with failed and good communications.

Three circuit breakers from each region are also reported on to validate if there are any communication issues with ED-PI itself. From the email report, follow up action is taken to investigate the RSG device's failed communication.

4.7.3 Performance

PG&E set a communication reliability requirement of 98% connectivity for the vendors and their RSG devices. Each vendor met this requirement and meets the performance goals for the RSG devices. Through testing, bugs with the PG&E and vendor equipment were found and bugs with PG&E equipment did not count against vendor RSG device performance. The performance of the system improved as bugs that were discovered were rectified.

RSG device performance is determined by evaluating the percentage of time the device is reliably posting telemetry data. Figure 14 is a plot of the time interval between data posts which should be every 30 seconds. Spikes in the plot show a period of time where telemetry data was not being posted by the RSG device. The date range for Figure 14 is the evaluation period after the DER Headend Server was operating in the production environment but before the ownership of the server was handed off from the EPIC team to the final production system owners. The data was collected from the ED-Pi historian which records all the data from the DER Headend Server. The gap between May 17, 2022 and May 19, 2022 is from the recorded data not being collected. These gaps were not due to a communication outage.

Two large spikes are seen with Vendor 1. The first spike is due to a software bug where if the data buffer between the Modbus and IEEE 2030.5 interface gets full and it is unable to purge itself. The buffer overflow started with a DNS failure at the PG&E network edge. Critical systems were rebooted and the hostname to the DER Headend Server was not automatically restarted with the systems. This root cause of the problem was resolved. Vendor 2 did not have a communication outage during this same time because Vendor 2 only resolved the hostname once and then caches the IP for further use. Vendor 2 will only perform the DNS lookup again if the cached IP does not provide the expected HTTP request response codes. Vendor 1 was able to determine the root cause of the buffer purge failure and resolve the issue. The second large spike seen with Vendor 1 is due to an issue with the PG&E historian. The DER Headend Server was checked, and it was verified that the RSG device from Vendor 1 was still posting data as expected. This gap is not seen by Vendor 2 because the two pilot locations were in different areas of the service territory which utilize different instances of the historian.

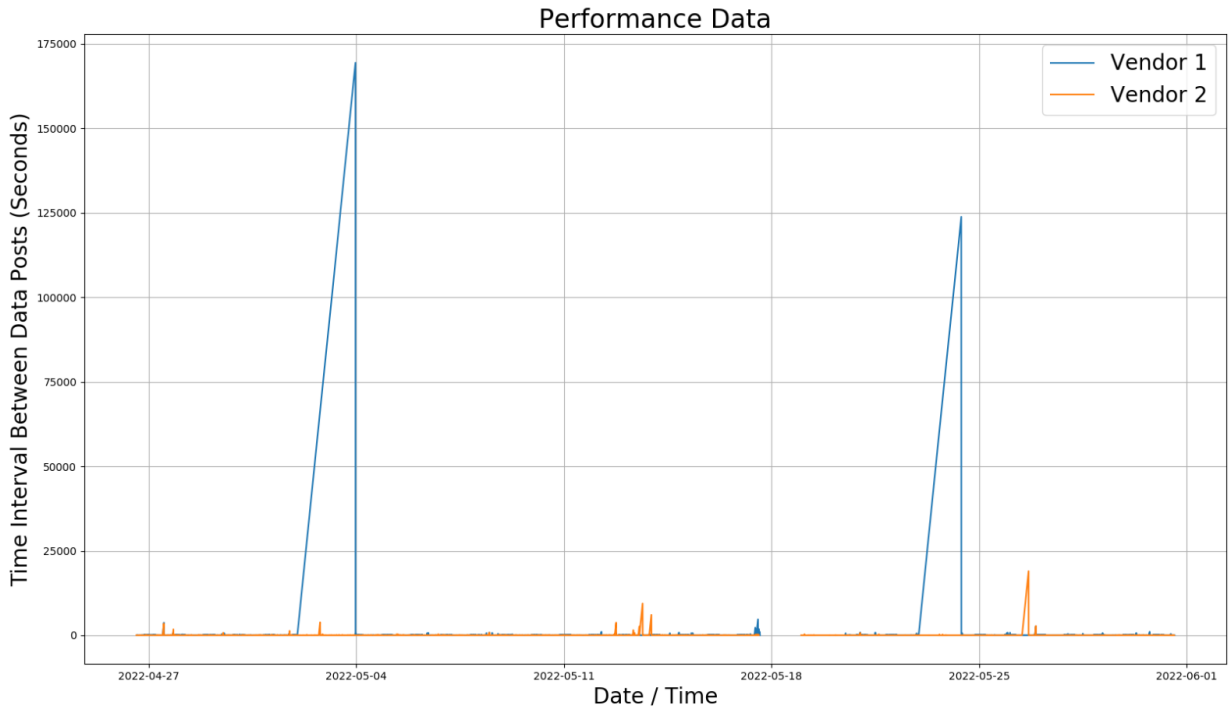


Figure 14: Performance Data.

Figure 15 displays the same data as Figure 14 but with a zoomed in y-axis so more detail can be seen. On May 17, 2022 multiple spikes can be seen with Vendor 1. When Vendor 1 investigated, their logs show that were posting data to the PG&E sever but getting a 0 response. On the 18th (data was not collected from the historian over this time) the RSG device from Vendor 1 had a Trusted Platform Module (TPM) lockout. The RSG device had to be restarted remotely to regain communication and the intermittent 0 responses stopped. Since then, Vendor 1 has resolved the root cause of the TPM lockout, and there have been no more known occurrences of 0 responses. On May 26, 2022 a spike can be seen with Vendor 2. This communication outage was caused by a server restart. The gateway did not regain communication until its daily DCAP forced a re-registration. After this observation period Vendor 2 released a RSG device firmware upgrade that detects server restarts and automatically re-registers instead of waiting for the daily DCAP. Much of the smaller spikes are due to cellular communication issues.

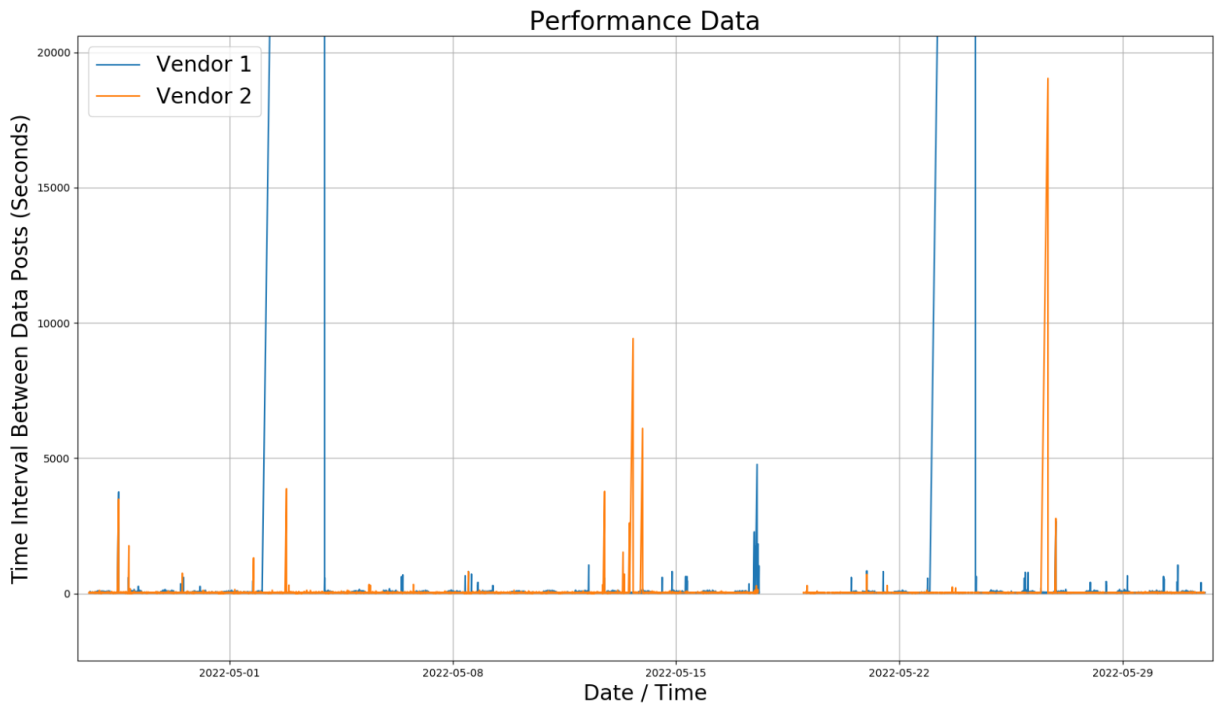


Figure 15: Performance Data

When evaluating the performance of Vendors 1 and 2 the two largest outages for Vendor 1 are removed from the data and the one largest outage for Vendor 2 is removed from the data. This is done because the outages were a combination of being caused by PG&E and the root causes being known and addressed. Vendor 1 had a communication reliability of 98.3% and Vendor 2 has a communication reliability of 98.5%. Both vendors met the reliability target of 98%.

4.8 Production Readiness

4.8.1 Systems integration

The production DER Headend System needed to be well integrated into PG&E's existing systems and processes to be easily accessible, configurable, and actionable by the operational end users. This required modifications to multiple platforms within PG&E's operational systems.

Consultation among the internal operational stakeholders affected by the new system resulted in requiring modification to five major internal PG&E systems and the interfaces between:

1. Electric Grid Interconnection System of Record and Customer Portal (SAP): The system of record for all data related to generation customers and the interface to populate data via the external facing customer portal.
2. Geographic Information Systems (GIS): The system of record for mapping the as-built PG&E and customer related data and information.
3. Distribution Management System (DMS): The interface used by Operations with the as-switched PG&E system and customer information used to operate the grid in real-time.

4. DER Headend Server: The new system created by the EPIC 3.03 project to communicate with customer-owned IEEE 2030.5 telemetry devices
5. Electric Distribution Data Historian (ED-PI): The historian for time-series data collected from PG&E distribution field devices.

A sixth system, Supervisory Control and Data Acquisition (SCADA), was originally planned to be modified to enable the control aspects of the DER Headend System, but because control of DERs via IEEE 2030.5 from the DCC was not fully realized within the timeline of this project, there were no modifications required in SCADA. The control aspects of IEEE 2030.5 are planned to be further studied and implemented as PG&E transitions to a new ADMS/DERMS system in the future. However, PG&E did build in the foundation for controllable objects within the framework of the modifications to the other systems to be ready when this functionality is available, as described below.

Figure 16 provides an overview of the initially planned systems affected by the EPIC 3.03 project and how they are integrated with each other.

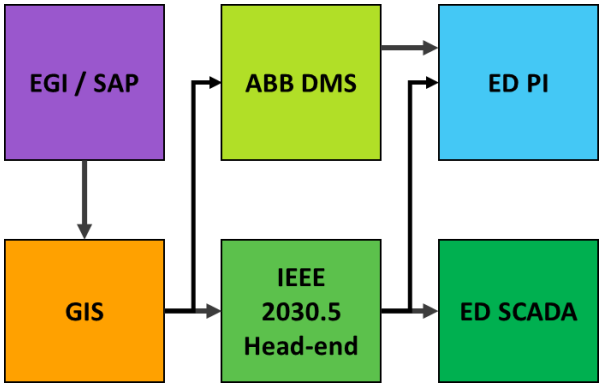


Figure 16: Planned System Integrations

SAP modifications included changes to the customer portal to specify the type of telemetry requested, as well as three new attributes added to generation projects to indicate the communication type (i.e. IEEE 2030.5 gateway, IEEE 2030.5 aggregator, mini-RTU, or SCADA), whether the system was controllable, and what program allowed it to be controllable (e.g. community microgrid).

There is an existing interface between SAP and GIS to automatically update GIS with generation information to display data on system maps and have the generator information easily accessible by engineers and other stakeholders. This interface was modified to additionally transfer the three new generator attributes available in SAP.

Within GIS, these new attributes needed to be displayed within the existing interface for each generator. This indicated to a user whether a generator had telemetry, control, the type of telemetry, and type of control program, if applicable. For sites with control, symbology was added to indicate that the site was available for control in SCADA (Figure 17). In addition, a query was created for users to be able to identify all generators with telemetry on any feeder of interest.

Figure 17: Primary and Secondary-connected Generators with Control Symbology (SCADA Lightning Bolt) in GIS

The interface between GIS and DMS also needed to be modified to account for the new generator attributes from GIS. In addition, added logic was required to create the appropriate symbology in DMS based on the type of generator and the type of telemetry or control function available at the generator. For example, a site with controllable resources had a SCADA symbol to visually indicate that an Operator could control it if needed. Whereas a site with just telemetry showed a "π" symbol to indicate that just historical trending was available via PI. All the historic telemetry data from the generator resources with telemetry via IEEE 2030.5 could also be easily displayed via a right-click interface (Figure 18) similar to other SCADA data Operators have access to.

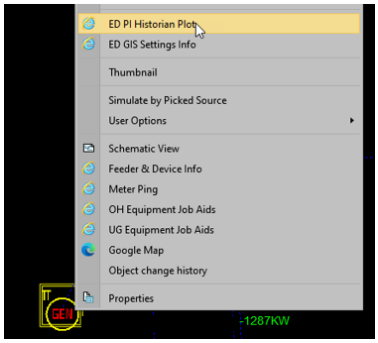


Figure 18: Functionality to access PI Historian data for a 2030.5 device via DMS

The trending of historic data required an interface with ED-PI to ensure that the data was properly linked between DMS and ED-PI. Within ED-PI, new templates were created to ease in the commissioning of new DER sites. Because data at the gross generator level by fuel type was new, this required a modification to the general hierarchical structure in ED-PI to provide operators and engineers better information about potential masked load by generator type and a method to calculate overall masked load at a site (Figure 19).

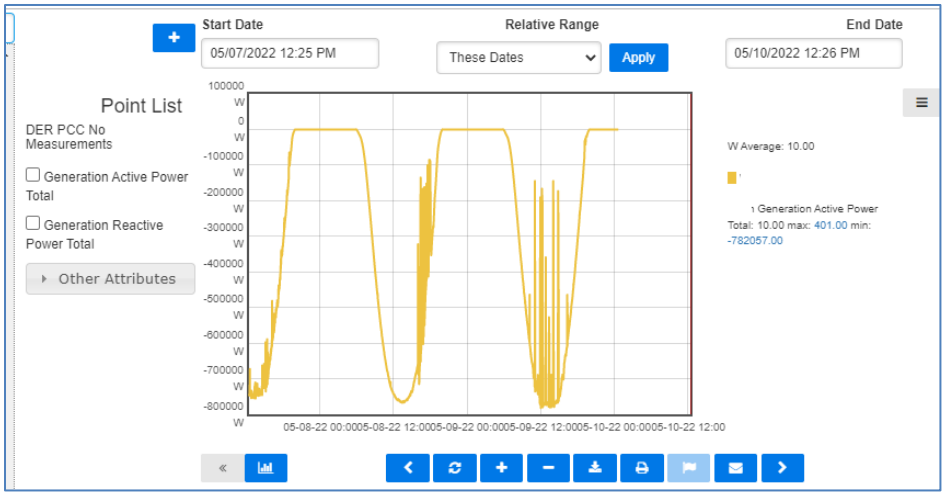


Figure 19: PI data for an IEEE 2030.5 site with solar generation

4.8.2 Process Development and Customer Engagement

In order to make the DER Headend System production-ready and make it widely available to the interconnection customers that were required to install it, PG&E worked with stakeholders within the organization to make sure they were ready for the impacts of this offering to their operations. This included working with internal teams to determine their current processes for installing MiniRTUs at customer sites, what customer facing information needs to be updated, what legal requirements there might be, what updates to internal data systems will be required, and how to collect funds from the customer for the performance of the work. With the updated processes, PG&E was able to support customers using their customer-owned RSG devices from interconnection application to installation and commissioning.

4.8.2.1 Customer onboarding process

Figure 20: High-level overview of COT onboarding steps.

The Electric Grid Interconnection (EGI) department within PG&E accepts applications for interconnection of DERs and were one of the key PG&E departments that would be impacted by this new system. EGI had existing processes for setting up MiniRTUs at customers' sites, which included engaging the IT project management team and billing customers appropriately for the installation of these devices at the DER sites. The EPIC project team worked closely with EGI to develop the new customer intake process as outlined in Figure 20. The first touchpoint for an interconnection customer is to apply through an interconnection application or online through the new YourProjects application portal. The modification to the interconnection application and YourProjects application portal required

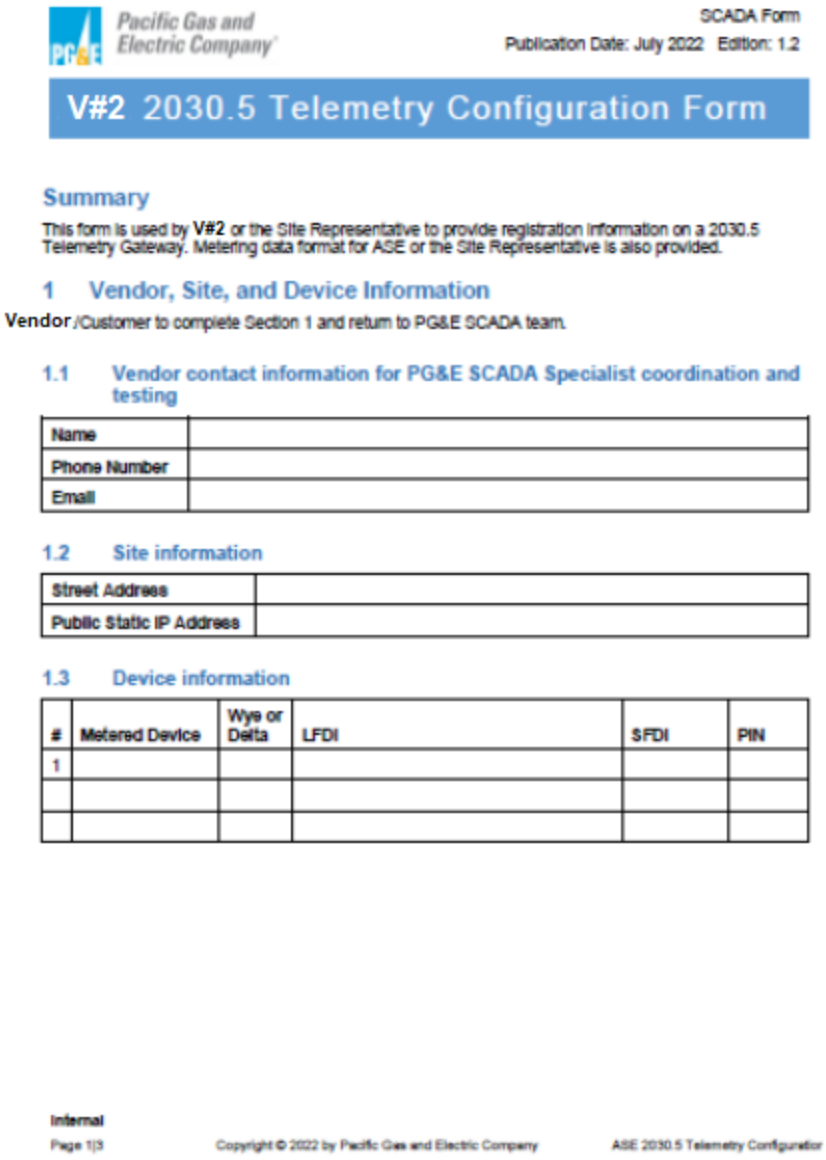
the submission of advice letter 6454-E[47] requesting approval. If the customer is applying for a 1MW project or greater under the appropriate tariffs, a question pops up for them to choose what type of telemetry they are requesting with MiniRTU, IEEE 2030.5 – Gateway, and IEEE 2030.5 – Aggregator as available options. PG&E decided to keep the MiniRTU as an available option to allow customers to choose something they are already familiar with and to be in compliance with CPUC Resolution E-5038 which requires the option of customer-owned telemetry but not the requirement for customer-owned telemetry. Some customers may take comfort in the idea that PG&E will own and maintain the MiniRTU systems, which PG&E anticipates will fade as the lower cost and familiarity with the customer-owned telemetry system increases with time.

The interconnection customer's application is then studied by the distribution planning department. The distribution planning department then determines if the standard telemetry is appropriate or if the customer requires protection using a line recloser. In order to keep costs down, PG&E is not currently requiring customers that need to install a line recloser to install additional telemetry for their generation. This may be something that PG&E reconsiders as grid needs arise or through customer requests.

For projects not requiring a line recloser and choosing the IEEE 2030.5 option, EGI will then bill the customer $4,000 for the cost of configuring the customer-owned telemetry device onto PG&E servers. This is a current estimate that will go through the annual unit cost reassessment process. Once the money is received, the customer chooses a telemetry vendor (either aggregator or gateway) and the interconnection agreement is signed, EGI then passes the project to the IT project manager to ensure the technical installation is performed correctly, answering customer questions, and arranging the configuration of the customer device onto PG&E's DER Headend Server. This is done through an internal request portal that IT project management uses to track requests. This portal was updated as part of the EPIC project to enable the new customer-owned telemetry option.

The IT project manager connects with the customer and ensures they understand the required scope of the interconnection and requirements of the system. The assigned IT project manager then requests the customer fill out an intake form to map out the data points of the DER from the meters communicating with the gateway or aggregator. An example can be seen in Figure 21: Example Customer-Owned Telemetry intake form (page 1). The intake form is specific for each certified-interoperable gateway/aggregator vendor and requests certified-interoperable vendor contact information, site location, public static IP address, device information including what the device is measuring, whether it is wye or delta connected, the Long Form Device Identifier (LFDI)/Short Form Device Identifier (SFDI), the pin, and designates the required data points. The customer and/or certified-interoperable vendor fills out the intake form and returns it to PG&E. The IT project manager then coordinates the configuration of the device(s) with a PG&E SCADA specialist. Once the SCADA specialist has successfully configured the device onto the PG&E server it will send a SCADA release letter to EGI which will follow up with a Permission to Operate letter for the customer.

[47] ELEC_6454-E.pdf (pge.com)



Pacific Gas and Electric Company

SCADA Form
Publication Date: July 2022 Edition: 1.2

V#2 2030.5 Telemetry Configuration Form

Summary

This form is used by **V#2** or the Site Representative to provide registration information on a 2030.5 Telemetry Gateway. Metering data format for ASE or the Site Representative is also provided.

1 Vendor, Site, and Device Information

Vendor/Customer to complete Section 1 and return to PG&E SCADA team.

1.1 Vendor contact information for PG&E SCADA Specialist coordination and testing

Name	
Phone Number	
Email	

1.2 Site information

Street Address	
Public Static IP Address	

1.3 Device information

#	Metered Device	Wye or Delta	LFDI	SFDI	PIN
1					

Internal

Page 1|3 Copyright © 2022 by Pacific Gas and Electric Company ASE 2030.5 Telemetry Configurator

Figure 21: Example Customer-Owned Telemetry intake form (page 1).

Pacific Gas and Electric Company

SCADA Form
Publication Date: July 2022 Edition: 1.2

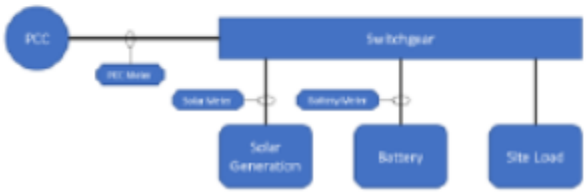
2 Vendor #2 /Customer Information

This section is provided for V#2 /Customer information.

2.1 Connection to PG&E server

Host Name	dermsprd.pge.com
Port	443
Device Capability URL	/dcap

2.2 Device Information Example

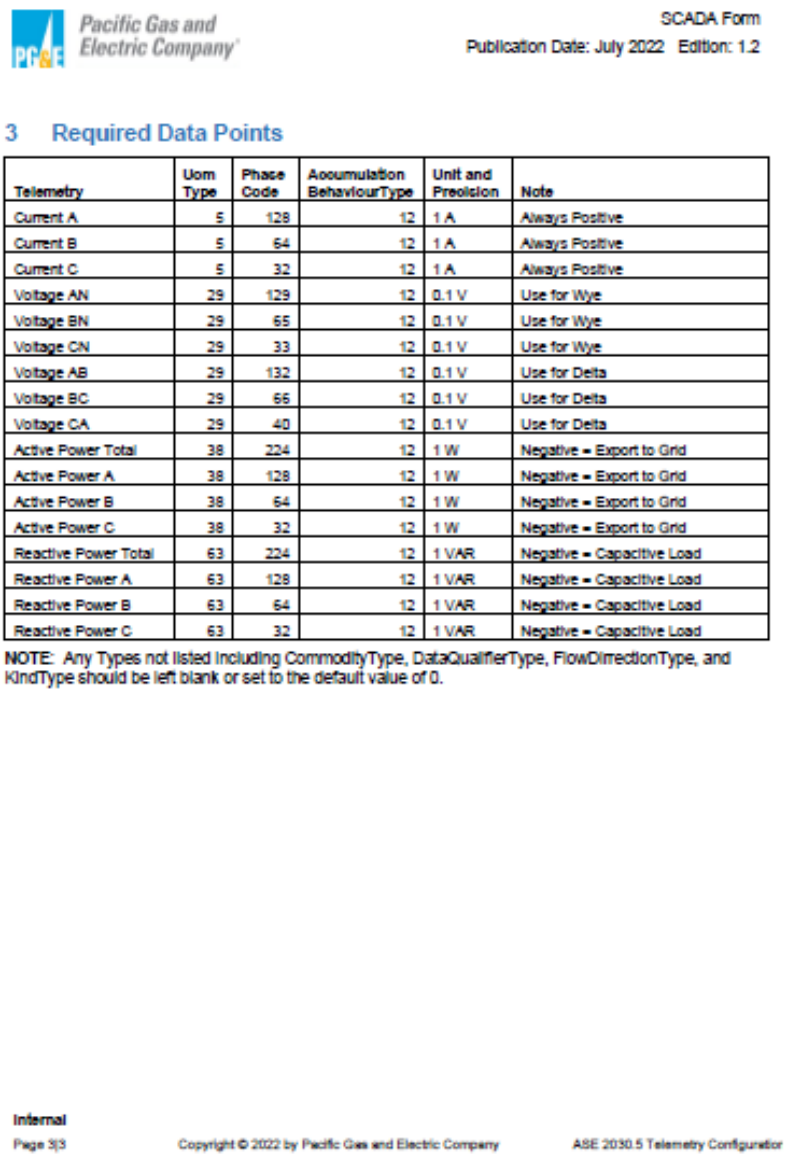


#	Metered Device	Wye or Delta	LFDI	SFDI	PIN
1	Aggregator	N/A	37625a519a07fbdf1396790864e04be1bfde812a	66577358261	192521
2	PCC	Wye	703e84691946469463056a9bea51cf0a4ebaea0c	36625753676	192521
3	Solar	Wye	d825f2269971a22b4b6a11f582d7e7a012c2e36e	47222089300	192521
4	Battery	Wye	929a9a0c17e5c52c4502f464f5c2d5e035fe1ebb	27075373564	192521

Internal

Page 2|3 Copyright © 2022 by Pacific Gas and Electric Company ASE 2030.5 Telemetry Configurator

Figure 22: Example Customer-Owned Telemetry intake form (page 2).



Pacific Gas and Electric Company

SCADA Form
Publication Date: July 2022 Edition: 1.2

3 Required Data Points

Telemetry	Uom Type	Phase Code	Accumulation BehaviourType	Unit and Precision	Note
Current A	5	128	12	1 A	Always Positive
Current B	5	64	12	1 A	Always Positive
Current C	5	32	12	1 A	Always Positive
Voltage AN	29	129	12	0.1 V	Use for Wye
Voltage BN	29	65	12	0.1 V	Use for Wye
Voltage CN	29	33	12	0.1 V	Use for Wye
Voltage AB	29	132	12	0.1 V	Use for Delta
Voltage BC	29	66	12	0.1 V	Use for Delta
Voltage CA	29	40	12	0.1 V	Use for Delta
Active Power Total	38	224	12	1 W	Negative = Export to Grid
Active Power A	38	128	12	1 W	Negative = Export to Grid
Active Power B	38	64	12	1 W	Negative = Export to Grid
Active Power C	38	32	12	1 W	Negative = Export to Grid
Reactive Power Total	63	224	12	1 VAR	Negative = Capacitive Load
Reactive Power A	63	128	12	1 VAR	Negative = Capacitive Load
Reactive Power B	63	64	12	1 VAR	Negative = Capacitive Load
Reactive Power C	63	32	12	1 VAR	Negative = Capacitive Load

NOTE: Any Types not listed including CommodityType, DataQualifierType, FlowDirectionType, and KindType should be left blank or set to the default value of 0.

Internal

Page 3|3 Copyright © 2022 by Pacific Gas and Electric Company ASE 2030.5 Telemetry Configurator

Figure 23: Example Customer-Owned Telemetry intake form (page 3).

4.8.2.2 Customer Legal Requirements

For pilot sites, PG&E required that a pilot agreement and cybersecurity agreement be signed. The pilot agreement's purpose was to designate the work that was being done as pilot and not part of the usual process of performing work with PG&E. The cybersecurity agreement required that customers meet certain cybersecurity best practices and included language on how detected cybersecurity issues would be resolved amongst the parties involved. As discussed in the pilot sites section 4.6.1 of this report, this caused some issue with one customer and work was done to resolve any issues with the cybersecurity agreement so that they could be comfortable with the system and the risks involved.

Through the cybersecurity evaluation of this system, PG&E determined that the risk level was sufficiently low to warrant paring down the cybersecurity agreement substantially and changing the requirements of the agreement into suggested best practices and adding those best practices to the PG&E DIH website[48].

Of course, the pilot agreement would not be needed once this EPIC 3.03 system was moved into production and all the requirements of the system would be posted to the DIH website which the interconnection agreement requires adherence to.

4.9 Control Testing

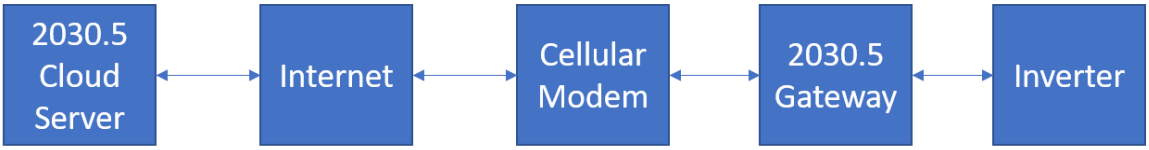


Figure 24: IEEE 2030.5 control testing setup.

Controls were tested with the IEEE 2030.5 DER Headend Cloud Server used for interoperability testing (see Figure 24 for control testing setup). Control testing was very limited in scope and included only the tests listed below. In order to operationalize controls with the DER Headend System, PG&E would need to perform extensive controls testing against the test setup and then in QA and then again in production. Initially, there was a desire to use control with an interconnected DER but no DER needing control was interconnected during the project timeline.

The RSG device was configured to interface with a smart inverter by the RSG device vendor. The smart inverter and RSG device communicated SunSpec Modbus over TCP/IP. The RSG device polls the DER Headend Cloud Server every 30 seconds for new DERControl or changes to DefaultDERControl. Subscription/Notification is not used. The following control scenarios were tested, and observations of the control operation are provided.

Table 8: Control test objective and corresponding results.

#	Objective	Results
1	Confirm the gateway polls and acts on changes from the server within the defined 30 second interval.	**Passed** – Confirmed the gateway picked up the changes and acted on them within the 30 second interval.
2	Confirm the gateway and smart inverter properly respond to a connect/disconnect control via opModConnect changes to the DefaultDERControl function.	**Passed** – Confirmed the gateway picked up the changes to the DefaultDERControl and the smart invert output changed accordingly to both the connect and disconnect functions. For the reconnect function, the smart inverter observed a 5-minute grid monitoring time before power output started.

[48] Utility Procedure: TD-2306P-01 Customer Owned Telemetry Procedure, Section 6. https://www.pge.com/includes/docs/pdfs/shared/customerservice/nonpgeutility/electrictransmission/handbook/TD-2306P-01.pdf

3	Confirm the gateway and smart inverter properly respond to a fixed watt (max watt for solar) control via OpModFixedW changes to the DefaultDERControl function.	**Failed** - Control is a percentage value and smart inverter name plate is 33.3kW. However, when sent a command to set the output at 10% (3.3kW), the output was set to 5kW. The issue found was that the smart inverter firmware stated incorrectly that the smart inverter output was 50kW instead of the actual 33.3kW. Therefore, while the communications and command worked appropriately, settings within the inverter caused the output to be incorrect.
4	Confirm the gateway and smart inverter properly respond to a volt/watt curve change to the DefaultDERControl function.	**Failed** – The gateway received the curve points, but they were not applied to the smart inverter. It is suspected that there could be an error in the Modbus mapping, but this issue was not debugged to confirm based on timing issues.
5	Confirm the gateway and smart inverter properly respond to a single scheduled control change, and after completion of the schedule the smart inverter returns to the DefaultDERControl.	**Passed** – OpModFixedW (mapped to maxW in the smart inverter) and OpModConnect were both able to be scheduled separately with a start time and duration.
6	Confirm the gateway and smart inverter properly respond to multiple scheduled control changes, and after completion of the schedule the smart inverter returns to the DefaultDERControl.	**Failed** - Only one control schedule is able to be executed at a time. The UI of the server had no way to implement multiple schedules, and therefore is unable to implement a changing constraint profile or multiple scheduled controls.

The following tests explore how the RSG device responds to losing communication with the server. Loss in communication is achieved by disconnecting the RSG device from the cellular modem. Further discussion is required to determine the desired action for each of these scenarios.

#	Objective	Results
1	Loss of communication occurs after scheduled control starts.	**Unknown Outcome** - Control persists until the scheduled duration elapses. The RSG device then reverts back to the DefaultDERControl.
2	Loss of communication occurs after the RSG device retrieves the schedule but before the start time.	**Failed** - Scheduled was not followed.
3	Momentary loss of communication occurs after the RSG device retrieves the schedule but before the start time and is reestablished before the scheduled control event ends.	**Unknown Outcome** – After communication is resumed and the RSG device communicates with the DER Headend Cloud Server, the schedule3d control starts until the originally scheduled control event ends.

The following tests explore how the smart inverter responds to losing communication with the RSG device. Loss of communication is achieved by disconnecting the smart inverter from the RSG device.

#	Objective	Results
1	opModFixedW is set to 10 in the DefaultDERControl. opModFixedW command is removed from the DefaultDERControl after communication to the smart inverter is lost.	**Failed** - After communication between the RSG device and smart inverter resumes, the smart inverter continues to output 10% indicating output control is still active. It is suspected that opModFixedW is not continually commanded to the smart inverter, more testing needed.
2	opModFixedW is set to 20 in DefaultDERControl. opModFixedW command is set to 100 in DefaultDERControl after communication to the smart inverter is lost.	**Passed** - After communication between the RSG device and smart inverter is resumed the smart inverter increases its output to utilize all available DC power.

3	opModFixedW is set to 10 in the DefaultDERControl. Communication to the smart inverter is lost.	**Unknown Outcome** – The smart inverter continues to operate at 10% output. DC and AC power to the smart inverter are each cycled, and the smart inverter continues to output at 10%. Further discussion required to standardize the expected behavior from the smart inverter when it loses communications.

4.9.1 Control Lessons Learned

From PG&E's limited control testing on this project, the lessons learned include:

- DERs that require control where specific power levels are set will need to demonstrate this ability during commissioning. This is important because IEEE 2030.5 uses percentages instead of absolute values for 'Fixed Watt' commands. If the nameplate information registered in the energy device and IEEE 2030.5 server do not match, the Fixed Watt setpoint will not produce the expected power level.
- All possible loss of communication scenarios need to be characterized and the expected response from the RSG device or aggregator and the energy device need to be specified. Energy device here being a smart inverter or an EMS. This effort should be made with industry partners because of the limitations in energy devices to retain settings and revert to defaults.
- Interoperability between RSG devices or aggregators and different energy devices is not guaranteed. All required control functions need to be tested during site commissioning.
- Performing more advanced scheduling requires additional testing beyond CSIP certification. For example the ability to implement a limited generation profile on the EPIC 3.03 DER Headend Server is not possible since only one scheduled start time and duration can be entered into the existing vendor user interface. Enhancements would be required to further validate this functionality.

4.9.2 Continuing and Future Work to Develop Control Capabilities

PG&E will continue to study and test control capabilities for the purposes of eventually rolling out the function into production within PG&E's new DERMS and ADMS. The challenges faced achieving the basic telemetry function limited PG&E's ability to have adequate resources and time to implement and test control capabilities to the desired extent within the schedule and budget of EPIC 3.03. Furthermore, because the EPIC 3.03 DER Headend server is planned to be replaced by the upcoming DERMS and ADMS in the near-term, further effort is being put into the future product development rather than the legacy system.

As shown through the control testing, there is still significant further testing required to have full confidence in the control capabilities via smart inverters and IEEE 2030.5. To mitigate the issues seen from smart inverter firmware creating improper dispatches, to the inability to set a volt/watt curve, PG&E recommends that commissioning testing be required for any control field systems until certifications like CSIP and Power Control Systems (PCS) have had more field experience and can mature as needed.

Also as seen from the deficiencies of the EPIC 3.03 CSIP-certified server, certain capabilities like implementing a limited generation profile, as discussed in Issue 9 of the Smart Inverter Working Group

report[49], are currently not possible without modifications to user interfaces. Furthermore, with the inability to do recurring schedules via IEEE 2030.5 and limitations on the number of events that can be scheduled, it is more prudent to use the soon to be released updated UL 1741 PCS certification for implementing limited generation profiles at this time.

PG&E will continue to be involved in the maturation of both the CSIP and IEEE 2030.5 standards as more experience is gained in DER control. PG&E is investing in its enterprise DERMS platform to enable control capabilities via IEEE 2030.5 as an important tool to address the increased complexity of the grid, and the ability to fully utilize existing grid resources to enable the growth of DERs, and to better serve customers.

4.10 Suitability of DER Headend for Remote Grid Use Case

To take advantage of the low-cost communication pathway back to PG&E the project team assessed whether the DER Headend System and certified-interoperable RSG devices could be used for PG&E's remote grid systems. The remote grid program establishes remote standalone power systems (i.e. off grid systems) for customers or small communities that are far removed from the main distribution grid, and which would otherwise require long distribution lines installed in high-fire threat areas. These standalone power systems require monitoring and control from PG&E's Distribution Control Center operators and dispatchers to determine system health and perform Public Safety Power Shutoffs (PSPS) in the event the risk is still considered high given environmental conditions around the remote grid equipment.

The project team assessed what data points would be required by the remote grid systems. A remote grid system consists of a Solar PV system, a battery storage system, and a fossil fuel backup (typically apropane generator) in order to meet the same power quality requirements as the main grid. While the solar PV system and battery storage system data points are the same as those of grid connected DERs, the fossil fuel backup generation was different as was the monitoring of the breaker status and configuration of the larger remote grid system. For example, an important data point for the backup systems is the amount of fuel remaining. Fuel could be in the form diesel or propane and the measurement of each would be very different and would require some sort of translation to make sense for a DCC operator. This fuel quantity translation would be different for each fuel storage thus requiring customization. Since remote grid systems are standalone, they require communications back to PG&E to alert for issues at the site like overheating or equipment failures, data points that PG&E does not monitor in for a typical 3rd party DER site.

Additionally, since PG&E would have to own and maintain this RSG device, a separate program would need to be developed to support IEEE 2030.5 devices that are PG&E owned. This would have required significant effort to develop and set up within the company with limited value to PG&E and customers.

It was determined that since these systems required more customization than a typical grid connected solar PV or battery storage smart inverter-based resource and that setting up a program to manage PG&E owned devices offered little if any benefits, it would make more sense to use a more purpose built monitoring and control solution with the agility to customize for each remote grid site. This might be something that CSIP or IEEE 2030.5 would want to explore in the future as an enhancement if there is

[49] https://www.cpuc.ca.gov/industries-and-topics/electrical-energy/infrastructure/rule-21-interconnection/limited-generation-profiles

sufficient interest on behalf of vendors developing monitoring and control systems for remote grid systems.

4.11 Macro Project Execution Challenges

- Interoperability: As discussed in more detail in section 4.5, the project faced unexpected interoperability challenges because CSIP-certified devices were not interoperable off-the-shelf with CSIP-certified servers. This was one of the driving challenges throughout the project. PG&E had to work with server and device vendors to troubleshoot interoperability and enable the devices to communicate properly with the DER Headend Server. This is an indication of a protocol and certification process that is still in its early stage of development.
- Cybersecurity Delays: Integration of third-party customer-owned devices to secure operational systems was as anticipated a central challenge of this project due to the nascency of the protocols and standards. There was lack of consensus from the industry and in a lot of ways, this project was the head of the spear in developing this integration. This created delays both in collaboration and coordination as well as when strategies shifted as more information became available such as when penetration testing was completed, and the smart inverter market survey and analysis was completed.
- Turnover of cybersecurity experts: The large demand for cybersecurity professionals in a multitude of industries led to substantial turnover of cybersecurity leads and experts working on the project.
- Lack of familiarity with emergent communication protocols and standards by key support vendors: PG&E's initial cybersecurity penetration test vendor was not able to successfully test the vulnerabilities of the system because they lacked the familiarity with the IEEE 2030.5 protocol and CSIP requirements. PG&E was able to find a penetration test vendor that was able to perform the tests, but this caused a significant delay in assessing the system and moving forward with decisions that hinged on the outcome of the penetration test.
- COVID-19 pandemic: COVID-19 impacts were wide and often hard to anticipate. In addition to the general work disruption that everyone faced during the pandemic, there were some specific challenges for this project.
    - PG&E's first pilot site, Blue Lake Rancheria (BLR) was a safety site for the community and emergency responders sheltered at the site in the early part of the pandemic. Each spike in COVID cases also triggered emergency responses that restricted the project team from completing the work at BLR. Additionally, while transitioning BLR from the pilot RSG that was installed to a production supported device, a 6.4 magnitude earthquake struck the region, challenging the transition from pilot to production for that site.
    - Gateway device manufacturers were experiencing delays due to global supply chain issues, indirectly caused by the COVID-19 pandemic, with computer chip availability particularly hindered.

5 Value Proposition

The purpose of EPIC funding is to support investments in technology demonstration and deployment projects that benefit the electricity customers of PG&E, San Diego Gas and Electric (SDG&E), and Southern California Edison (SCE). The EPIC 3.03 – DER Headend System project has demonstrated:

1. The deployment of a low-cost telemetry solution using interconnection customer owned RSG devices. This solution reduces the cost of fulfilling telemetry requirements for DERs 1 MW or greater in size from $50,000-150,000 using a MiniRTU to less than $20,000 using an RSG device from one of PG&E's certified interoperable vendors. With an estimated $90,000 per customer saved and 25 customers interconnecting, this amounts to an annual savings to our customers of $2.25 million. PG&E expects that this cost will decrease with the further deployment of aggregator connectivity to PG&E's DER Headend Server. With increases in the number of interconnections above 1 MW expected, the increased volume will be another driver for lowering the cost of telemetry connections to DER sites.
2. As interconnection related costs decrease with the low-cost customer-owned telemetry system being deployed on the DER Headend Server the penetration of DERs is expected to increase.
3. The development of the DER Headend System is foundational for the deployment of IEEE 2030.5 communications on PG&E's network. This will allow the future DERMS/ADMS systems to enable even greater penetration of DERs on the distribution grid. These systems will allow DERs to export more power and provide more grid services to the distribution grid because all grid and interconnected DERs will be managed for constraints more granularly.
4. The EPIC 3.03 project positively contributed to better standardization of CSIP and IEEE 2030.5 through this deployment enabling other utilities in California, the country and around the world as well as their customers to benefit from the work accomplished. It also highlighted gaps in the communications standards to the standards bodies to rectify benefiting the industry at large.

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:
    - The DER Headend System lowers the cost of the telemetry requirement for interconnection. This enables more DERs to interconnect onto the grid due to better economics. More DERs can help meet resource adequacy needs during times of high load.
    - The DER Headend System is foundational to the future implementation of a DERMS/ADMS where DERs outputs can be optimized to meet or account for grid constraints safely thus increasing system reliability.
    - Awareness of DER outputs on the distribution grid can help enablement of microgrids in order to de-energize powerlines running through high fire threat locations during periods of high fire risk while maintaining service to the maximum number of customers or critical facilities.
- Lower costs:
    - Costs for implementing telemetry at DER customer sites are reduced by using the DER Headend System versus the MiniRTU option. Less than $20,000 would be expected for

the DER Headend System and approximately $50,000-$150,000 would be required for the MiniRTU or PG&E recloser.

  - Costs will likely lower further with time, volume, and the use of aggregators.

- Enhanced environmental sustainability:
  - The DER Headend System and future DERMS/ADMS will allow greater penetration of DERs onto the distribution grid.
  - Better and lower cost monitoring and control capabilities for DERs will allow DERs to interconnect greater amounts of generation safely while taking into account more granular grid constraints.

5.2 Secondary Principles

EPIC also has a set of complementary secondary principles. This EPIC project contributes to the following three secondary principles: societal benefits, greenhouse gas (GHG) emissions reduction, low-emission vehicles, transmission, and efficient use of ratepayer funds.

- Societal benefits:
  - Lowering the cost of the telemetry requirement for interconnecting DERs will lower the cost to interconnect enabling more DERs to interconnect or interconnect with more generation.
- Greenhouse gas (GHG) emissions reduction:
  - Lowering the cost of the telemetry requirement for interconnecting DERs will lower the cost to interconnect, enabling more DERs to interconnect or interconnect with more generation. More DERs will contribute to better grid reliability, more locally sourced generation, and reduced costs to serve customers
- Electric Vehicles:
  - Demonstrating communications using IEEE 2030.5 with DERs is the first step to working on and demonstrating communications between Electric Vehicles (EVs) and the utility for the same monitoring and control capabilities turning an EV from a consumer of electricity to an energy storage device with the same benefits e.g. resources adequacy, storing renewable energy for peak shaving, etc.
- Transmission:
  - Increasing the penetration of DERs onto the grid using the DER Headend System and the future DERMS/ADMS will reduce the need for new transmission projects.
  - Increasing the penetration of DERs will also reduce congestion on transmission lines as well as provide grid support when transmission lines are out of service.
- Efficient use of ratepayer funds:

- As with many clean energy initiatives and foundational energy policies, California is the leader in implementation of the IEEE 2030.5 and CSIP standards. This project represents a huge leap forward in enabling these communications standards in the field and will help shape implementation not just for California ratepayers but utilities around the globe.

5.3 Accomplishments and Recommendations

5.3.1 Key Accomplishments

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

- Installed a cybersecure CSIP-certified IEEE 2030.5 DER Headend System within PG&E that is interoperable with two customer-owned gateway vendors over the public internet.
- Successfully deployed RSG devices from both vendors at a handful of pilot sites.
- Tested and certified-interoperable three CSIP-certified aggregator vendors with the DER Headend System for use by PG&E customers.
- Integrated the new telemetry option into PG&E's business and IT systems.
    - Updated the interconnection application forms and portal, YourProjects, to offer customer-owned telemetry as an option.
    - Update to customer data systems (SAP) to add fields for the new customer data points coming in for customer-owned telemetry.
    - Systems integration between internal data systems (SAP, GIS, and DMS).
    - Procedures for configuring customer-owned telemetry RSG devices on the DER Headend System and linking the telemetry data into ED-Pi. ED-Pi is the system PG&E uses to view telemetry from field devices and now DERs with customer-owned telemetry RSG devices.
    - Developed a process for bringing new vendors and aggregators onboard to ensure interoperability between their offerings and PG&E's DER Headend System and making them a certified interoperable vendor[50] following successful testing.
- Progressed the state of the industry by testing out interoperability of CSIP-certified IEEE 2030.5 systems and highlighting interoperability challenges that arose from testing different vendor RSG devices with the DER Headend Server. Improving the standardization of communication between the utility and customer devices will benefit customers and the grid.
- Lowered the cost of the telemetry requirement for interconnection customers 1MW or greater that are required to install telemetry to less than the $20,000 goal set for the project. The lower cost allows for a greater cost-effective penetration of renewables onto the distribution grid.
- Control testing and experience to be used in future development of DERMS and set PG&E up for future success with the development and rollout of DERMS.
- Used learnings for integrating IEEE 2030.5 communications into the future DERMS and ADMS.
- Shared and presented learnings with industry stakeholders. Specifically, with EPRI, SunSpec, the CPUC, the Smart Inverter Working Group, the annualEPIC Symposium, DistribuTECH, and more.
- Developed a process for new gateway or aggregator vendors to become PG&E certified-interoperable vendors.

[50] TD-2306P-01, Attachment 1: Certified-Interoperable Customer-Owned Telemetry Vendors; https://www.pge.com/includes/docs/pdfs/shared/customerservice/nonpgeutility/electrictransmission/handbook/TD-2306P-01-A1.pdf

5.3.2 Key Recommendations

- PG&E recommends:
  - Continued interoperability testing between CSIP/IEEE 2030.5 systems on the market and refinement of the protocols and standards to address remaining gaps or ambiguity in interpreting the protocol and standard requirements.
  - Continued testing of control capabilities to inform use in future DERMS/ADMS systems.
  - Emphasis on utilizing the CSIP standard to improve integrations between the utility and customers' DERs in a cost-effective way.
  - Ensuring the CSIP standard is able to keep RSG/aggregator/server vendors nimble to adapt to changes to the cybersecurity framework and requirements discovered and imposed by utilities or regulatory bodies.

5.4 Technology Transfer Plan

5.4.1 IOU's Technology Transfer Plans

A primary benefit of the EPIC program is the technology and knowledge sharing that occurs both internally within PG&E, and across the other IOUs, the CEC and the industry. In order to facilitate this knowledge sharing, PG&E will share the results of this project in industry workshops and through public reports published on the PG&E website. Specifically, below is information sharing forums where the results and lessons learned from this EPIC project were presented or plan to be presented:

Information Sharing Forums Held

- *Annual EPIC Symposium*
  Web Conference, October 2020
- *DistribuTECH*
  Dallas, Tx May 2022
- *Smart Inverter Working Group*
  Web Conference, July 2022
- *UNITE the Grid Presentation*
  Web Conference, July 2022
- *EPRI*
  Web Conference, September 2022
- *Interconnection Best Practices Meeting*
  Web Conference, March 2022

Information Sharing Forums Planned

- *Darcy Partners*
  Online, February 23, 2023

5.4.2 Adaptability to other Utilities and Industry

The following findings of this project are relevant and adaptable to other utilities and the industry:

- Other utilities and the industry as a whole will benefit from the development of an environment that allows zero-trust devices to be connected to utility networks. Customers and gateway/aggregator vendors have been positively impacted by this treatment because

of the reduced scope of requirements and liabilities they must endure to deploy a customer-owned and maintained RSG device.

- Documentation of challenges with interoperability between the DER Headend Server, the RSG devices and aggregator clients despite CSIP certification will help improve the CSIP and IEEE 2030.5 communication standards. The hope is that future systems will be plug and play and utilities will not have to test each vendor's gateway or aggregator for interoperability and troubleshooting with their DER Headend Server.

5.5 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.

6 Metrics

The following metrics were identified for this project and included in PG&E's EPIC Annual Report as potential metrics to measure project benefits at full scale.[51] Given the proof-of-concept nature of this EPIC project, these metrics are forward looking.

D.13-11-025, Attachment 4. List of Proposed Metrics and Potential Areas of Measurement (as applicable to a specific project or investment area)	Reference
1. Potential energy and cost savings	
a. Customer savings (dollars saved)	Reference Section 5 (Value Proposition)
2. Economic benefits	
a. Maintain / Reduce capital costs	Reference Section 5 (Value Proposition)
3. Environmental benefits	
a. GHG emissions reductions (MMTCO2e)	Reference Section 5.2 (Secondary Benefits)
4. Safety, Power Quality, and Reliability (Equipment, Electricity System)	
a. Electric system power flow congestion reduction	Reference Section 2.2 (Industry Trends)
b. Forecast accuracy improvement	Reference Section 4.10
c. Increase in the number of nodes in the power system at monitoring points	Reference Section 1.2 (DER Headend Overview)
5. Effectiveness of information dissemination	
a. Number of information sharing forums held	Reference Section 5.4.1 (IOU's

[51] 2015 PG&E EPIC Annual Report. Feb 29, 2016.
http://www.pge.com/includes/docs/pdfs/about/environment/epic/EPICAnnualReportAttachmentA.pdf

	technology transfer plans)
6. Adoption of EPIC technology, strategy, and research data/results by others	
a. Description/documentation of projects that progress deployment, such as Commission approval of utility proposals for widespread deployment or technologies included in adopted building standards	Reference Section 4.2 (Regulatory)
b. Successful project outcomes ready for use in California IOU grid (Path to market)	Reference Section 4.2 (Regulatory)
c. Technologies available for sale in the marketplace (when known)	Reference Section 5.3.1 (Key Accomplishments)

7 Conclusion

The EPIC 3.03 DER Headend System project successfully tested and configured a CSIP-certified IEEE 2030.5 server that is interoperable with two vendors' RSG devices and three different aggregators. It demonstrated that a utility can communicate with customer-owned devices on the public internet in a cybersecure way. It lowered the cost for PG&E interconnection customers to fulfill their telemetry requirements to below $20,000 in a ten-year period (vs $50,000-$150,000 previously) with costs likely to further decrease as the certified interoperable vendors mature their product offerings.

The success of this project does not diminish the work remaining to make CSIP-certified devices plug-and-play interoperable. Remaining still is the work to ensure the control functions can work when the need for that functionality arises, for example, through a distribution investment deferral (DIDF) project or an interconnection customer requiring a granular limited generation profile for their DER.

This project has laid the foundation for the future of DERMS at PG&E. As more DERs are interconnected to the grid, it becomes important to be able to coordinate these resources through the DERMS. Establishing a low-cost connection to the DERs is the first step to unlocking that greater potential.

8 Appendix A: DER Headend Server Vendor Final Report - Tantalus

DER Headend Server Vendor – Tantalus – Final Report (link)

9 Appendix B: RSG Device Vendor Final Report – Kitu

RSG Device Vendor – Kitu – Final Report (link)

10 Appendix C: RSG Device Vendor Final Report – ASE

RSG Device Vendor – ASE – Final Report (link)

11 Appendix D: Utility Procedure – Customer Owned Telemetry

Utility Procedure: TD-2306P-01 -Customer-Owned Telemetry (COT) Procedure (link)

12 Appendix E: Utility Procedure – Attachment 1 – Certified-Interoperable Vendors

Utility Procedure: TD-2306P-01 -Customer-Owned Telemetry (COT) Attachment 1, Certified-Interoperable Customer-Owned Telemetry Vendors (link)

13 Appendix F: Utility Procedure – Attachment 2 – LogEvent Descriptions

Utility Procedure: TD-2306P-01 -Customer-Owned Telemetry (COT) Attachment 2, PG&E IEEE 2030.5 LogEvent Descriptions (link)

14 Appendix G: Smart Inverter Working Group and Smart Inverter Manufacturer Survey

Survey Results:
The survey asked for the below and received the following responses:

1. Company name – *to determine the smart inverter vendor responding. This was an optional field.*
2. Email address – *to be able to follow up if needed with their response. This was an optional field.*
3. Do you sell CSIP certified smart inverters? – *a way of distinguishing respondents that had an installed base of smart inverters or not.*
    a. Yes
    b. No and don't plan to
    c. Not yet but plan to
4. Please Rank your preferred approach to integration with utilities for the purposes of telemetry and/or control (1=highest preference, 4=lowest preference) – *vendors that were not anticipating or planning to do direct communications would not be impacted by changes to communication requirements.*
    a. Direct Communication with Smart Inverter
    b. Local Site Gateway
    c. Aggregation Platform (i.e. cloud integration)
    d. Local Energy Management System

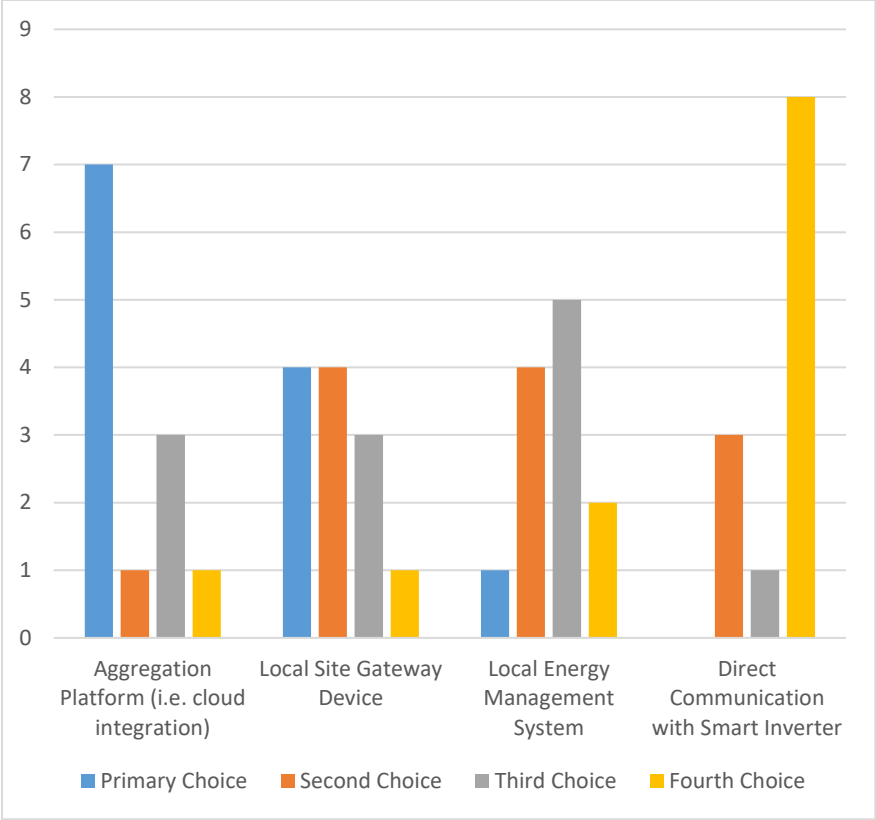


Figure 25: Ranked preferred integration approach between Smart Inverter and utility systems.

Analysis: The overwhelming response was for aggregator as the preferred integration with utility systems with a use of a local site gateway (i.e. RSG) as the runner up. No vendor that responded chose direct communication to smart inverter as a preferred integration method, it was the least desirable integration method from the respondents. This includes the one vendor that has CSIP-certification directly to the inverter.

5. What is your current capability for each method of integration into utility headend systems using IEEE 2030.5? – *intention here was to determine how installed smart inverters were planning to communicate to utility systems and whether that was an available capability. Each of the below had the option to choose whether it was an existing capability, on the product road map, or no plans to develop.*
    a. Direction Communication with Smart Inverter
    b. Local Site Gateway
    c. Aggregation Platform (i.e. cloud integration)
    d. Local Energy Management System

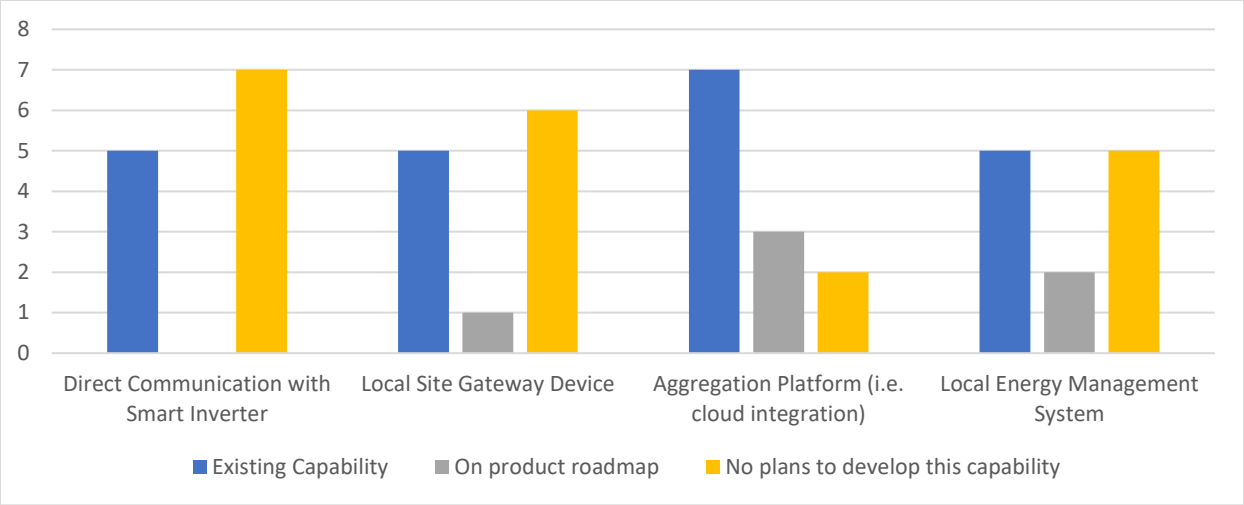


Figure 26: Current integration capability with utility headend servers using IEEE 2030.5.

Analysis: Aggregation is a current capability for most of the vendors responding. It is important to note that for direct communication with smart inverters, the only vendor that has this capability responded twice so the true number of respondents for that should have been two not five. The other three vendors were not listed on the CEC list as CSIP-certified for direct to inverter communications.

6. Have you successfully tested interoperability between a CSIP-certified Smart Inverter directly connected to a CSIP-certified headend server? – *Since it was determined that CSIP-certification did not inherently mean interoperability it was pertinent to ask whether integration had occurred on real CSIP-certified headend servers as opposed to just a test rig.*
    a. Yes
    b. No

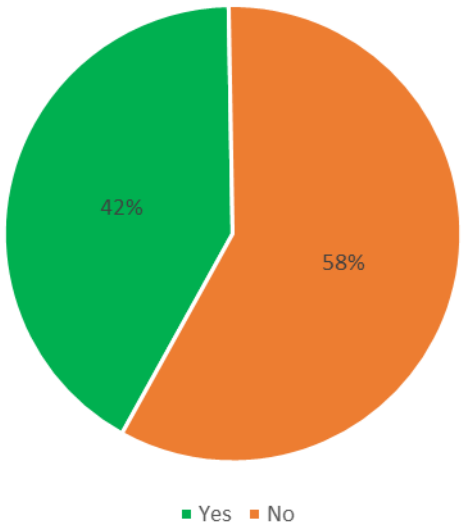


Figure 27: Testing interoperability with field deployed CSIP-certified IEEE 2030.5 server.

Analysis: Of the five vendors that responded that they have tested with a field deployed CSIP-certified server, only one is on the CEC-list as being CSIP-certified for direct communications to smart inverter (the same vendor responded twice to the survey). The other three vendors do not have CSIP-certified

direct communications to smart inverter products according to the CEC list. As shared in section 4.5 of this report, CSIP-certified does not yet mean interoperable so a smart inverter that has CSIP-certification for communication without a gateway would have to be tested and troubleshooted for interoperability to work with a deployed CSIP-certified server. Vendors in subsequent questions within the survey note that updating an installed smart inverter's software and firmware is likely cost prohibitive because they are more than likely no longer supported by the manufacturer.

7. If yes, which CSIP-certified servers have you successfully integrated with?
8. Are you able to update your existing installed base of Smart Inverters with new settings remotely? e.g. volt/VAR curves
    a. Yes
    b. No
    c. Other

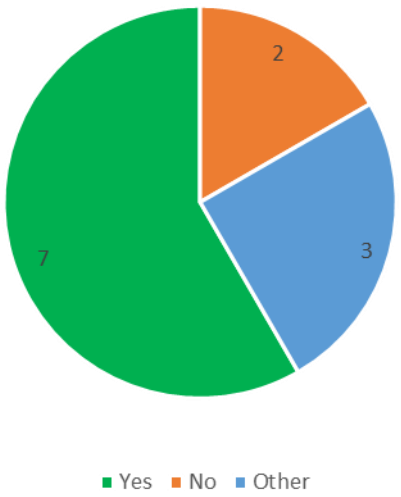


Figure 28: Can Smart Inverter perform settings changes?

9. Please provide more information on how inverter settings changes might be performed. (e.g. utilizing IEEE 2030.5 or utilizing another API?) – *since one of the requirements of a smart inverter is that they should be able to remotely update their settings for their characteristics, understanding how the vendor planned to communicate those settings was important.*

Analysis: Most respondents can remotely update settings to their smart inverters. For some vendors the lack of network connectivity with their smart inverters makes it impossible to connect to these DERs even if the smart inverter has that capability. Most of the vendors that can communicate with their smart inverters did so using a proprietary API.

10. Are you able to update your existing installed base of Smart Inverters to new versions of CSIP remotely (e.g. with an over-the-air firmware update)?
    a. Yes
    b. No
    c. Other
11. If no, please provide more information on how updates might be performed:

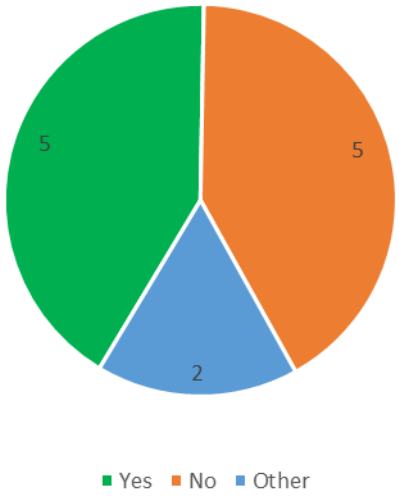


Figure 29: Are you able to update your smart inverters with new versions of CSIP?

Analysis: Rule 21[52] requires that a smart inverter's chosen communication option's software can be updated remotely. This question was worded incorrectly because it was not determined that CSIP-certification was possible using a gateway until after the results were received which led to some confusion in answering this question from some respondents. Some vendors responded that they would be able to update their version of CSIP as needed because they answered using a gateway. Those that answered no or other answered thinking that they were responding to just the smart inverter even though they leveraged a gateway for their CSIP-certification.

12. Reference Cipher Suite section 4.4.3 for discussion on this survey question.
13. Reference Cipher Suite section 4.4.3 for discussion on this survey question.
14. Reference Cipher Suite section 4.4.3 for discussion on this survey question.
15. What customer segment(s) are primarily served by the product(s) this response is for?
    g. Above 1MW
    h. 250 kW to 1 MW
    i. 20 kW to 250 kW
    j. Below 20 kW

[52] Rule 21, Section HH.5.b.ii

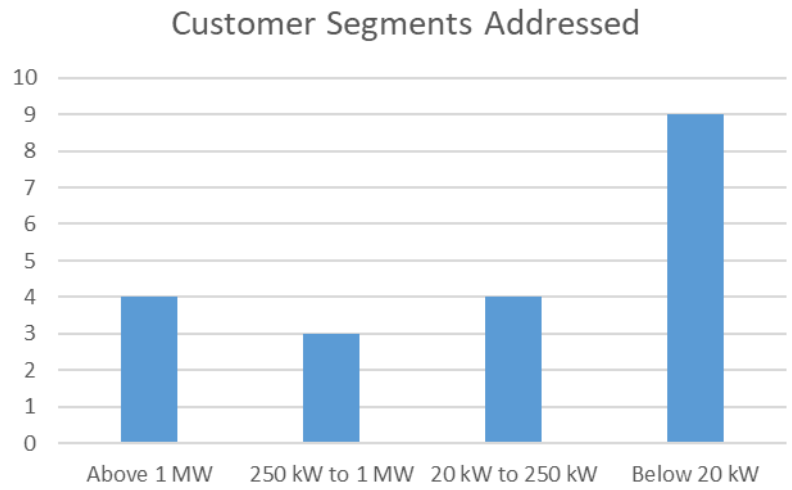


Figure 30: Customer segments of respondents.

16. Please share any additional comments, thoughts, or suggestions on how utility systems can integrate with existing installed base of inverter based DERs:

Some thoughts from our respondents worth adding to the discussion:

> "Any firmware update invalidates IEEE 1547 listing of the inverter. It's possible but not likely that an inverter with UL 1998 listing on the firmware could be updated without requiring retesting. But I'd be skeptical of any such conclusion and would expect any firmware update to necessitate at least some retesting for manufacturer-internal qualification and grid code compliance. Such a project could be extremely difficult or impossible to support on legacy equipment. The compliance projects are expensive and must be justified by a worthwhile return on investment."

It will be important for SunSpec and the industry to consider how to update CSIP's cybersecurity requirements in a way that ensures an ability to pivot quickly to ensure the safety of these systems without causing large amounts of rework or recertification.

> "After CA Rule 21 required Phase 2 compliance in 2020: Equipment meeting this has IEEE 2030.5/CSIP capability. However, the necessary communication interface (on site hardware or cloud-based gateway and required internet connection) may not be provided if it was not required by interconnection agreement for sites less than 1MW. Systems over 1MW would have whatever interface was required for that site. Previous to 2020 phase 2, some manufacturers may have access through their web-based portal, but only if customer signed up and maintains an internet connection."

Integrating with an installed base of smart inverters or smart inverters in general for sites that have not been required to make a connection to date from their interconnection agreements will be challenging due to a lack of internet connectivity established by the customers for these devices. Part of the rationale the project vendors had for using cellular communication chips for their gateways was so that they could have better control of their gateway's communications connection in order to troubleshoot issues as they arise without customer involvement and ensure connectivity to the utility. With the scale of interconnections on PG&E's grid that are smaller sized systems, it is likely that many will not be able to connect to the grid in the future due to connectivity and support of these devices.