March 31, 2016

Timothy Sullivan
Executive Director
California Public Utilities Commission
505 Van Ness Avenue
San Francisco, CA  94102-3298

Subject:  California Energy Systems for the 21st Century (CES-21)
Annual Report - 2015

Dear Mr. Sullivan:

The 2015 CES-21 annual report is submitted by Pacific Gas & Electric Company (PG&E), on behalf of itself, Southern California Edison Company (SCE) and San Diego Gas and Electric Company (SDG&E), pursuant to Ordering Paragraph 21 of Commission Decision 14-03-029.

This report provides information on the operations of the CES-21 program, including projects funded, results of research, efforts made to involve third parties, and intellectual property that results from the research.

Please contact George Zahariudakis at gxz5@pge.com or 415-973-2079, Aaron Renfro at Aaron.Renfro@sce.com or 714-895-0570, or Hannon Rasool at hrasool@semprautilities.com or 858-654-1590 regarding any questions about this report. Thank you.

Attachment

cc:  Edward Randolph, CPUC, Energy Division Director
     Maria Sotero, CPUC, Energy Division
     George Zahariudakis, PG&E, Regulatory
     Alexander Boutelle, PG&E, Program Manager
     Aaron Renfro, SCE, Regulatory
     Joy Weed, SCE, Program Manager
     Hannon Rasool, SDG&E, Regulatory
     Corey McClelland, SDG&E, Program Manager
California Energy Systems for the 21st Century (CES-21)

2015 Annual Report

PACIFIC GAS & ELECTRIC COMPANY
SOUTHERN CALIFORNIA EDISON COMPANY
SAN DIEGO GAS & ELECTRIC COMPANY

March 31, 2016
# Table of Contents

1. Executive Summary .................................................................................................................. 1  
   a. Overview of CES-21 Program and Plan Highlights ................................................................. 1  
   b. Status of Program ................................................................................................................. 1  
   c. Lessons Learned .................................................................................................................. 2  

2. Introduction and Overview ...................................................................................................... 4  
   a. Background on CES-21 ....................................................................................................... 4  
   b. CES-21 Program Components ............................................................................................... 4  
   c. CES-21 Program Regulatory Process and History ................................................................... 4  
   d. Pre-Filing Workshop Results .................................................................................................. 6  
   e. Industry Trends Impacting Program and Projects ................................................................... 6  
   f. Coordination .......................................................................................................................... 7  
      i. Industry Coordination ....................................................................................................... 7  
      ii. Internal Coordination ...................................................................................................... 7  

3. Budget (by Year, by Research Area) ....................................................................................... 8  

4. Projects ................................................................................................................................... 9  

   Cybersecurity: Machine-to-Machine Automated Threat Response .............................................. 9  
   a. High Level Summary .......................................................................................................... 9  
   b. Project Status Report ........................................................................................................... 9  
   c. Project Details ..................................................................................................................... 9  
      i. Objective .......................................................................................................................... 9  
      ii. Scope ............................................................................................................................... 9  
      iii. Deliverables .................................................................................................................. 10  
   iv. Business Case Analysis ...................................................................................................... 10  
   v. Evaluation Metrics .............................................................................................................. 11  
   vi. Schedule ............................................................................................................................ 11  
   vii. CES-21 Funds Spent ......................................................................................................... 11  
   viii. Treatment of Intellectual Property .................................................................................. 11  
   ix. Status Update .................................................................................................................... 12  

   Grid Integration: Flexibility Metrics ........................................................................................ 13  
   a. High Level Summary .......................................................................................................... 13  
   b. Project Status Report ........................................................................................................... 13
Table of Contents (Cont’d.)

c. Project Details .......................................................................................................................... 13
i. Objective .................................................................................................................................. 13
ii. Scope ...................................................................................................................................... 13
iii. Deliverables ............................................................................................................................. 13
iv. Business Case Analysis ........................................................................................................... 13
v. Evaluation Metrics ..................................................................................................................... 14
vi. Schedule ................................................................................................................................ 14
vii. CES-21 Funds Spent ............................................................................................................... 14
viii. Treatment of Intellectual Property ....................................................................................... 14
ix. Status Update ........................................................................................................................... 15

5. Conclusion ................................................................................................................................. 16
   a. Key Results for the Year ......................................................................................................... 16
   b. Next Steps for CES-21 Projects ........................................................................................... 16
   c. Issues That May Have Major Impact on Progress in Projects ............................................. 16
   d. Lessons Learned .................................................................................................................... 16

Appendix A – Scope by Task of CES-21 Cybersecurity Project ....................................................... 18
1. Executive Summary

a. Overview of CES-21 Program and Plan Highlights

The California Energy Systems for the 21st Century (CES-21) Program is a public-private collaborative Research and Development (R&D) program between the “Joint Utilities”—Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE) and San Diego Gas & Electric Company (SDG&E)—and Lawrence Livermore National Laboratory (LLNL).

The CES-21 Program is designed to research solutions for the medium- and far-term challenges of a fast-evolving energy marketplace. The program is comprised of two projects, a Joint Utilities Cybersecurity project and a Grid Flexibility Metrics project led by PG&E and SDG&E.

1. Cybersecurity: Researches—and lays the groundwork for—automated responses to the ever-growing number of cyberthreat vectors. The Machine-to-Machine Automated Threat Response (MMATR) project team is working to develop a shared language to encode cyberthreat descriptions, a modeling engine to simulate these threats and potential responses, secure system interfaces for Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), and a test bed on which to run MMATR scenarios and prove out simulated solutions with real-world equipment. One of the project’s priorities is to make this research on advanced threat detection and automated response extensible enough to work for all three California investor-owned utilities (IOU), and ideally the private sector vendors who could productize such research for the wider U.S. utility community.

2. Grid Integration – Flexibility Metrics: Simulates the impact of increased renewable penetration and market conditions on the accuracy of reliability and capacity metrics. As California leads the nation in Renewables Portfolio Standard (RPS) requirements, this project is working to determine if the utilities’ planning assumptions and reliability metrics are applicable under future conditions. This requires modeling the grid under thousands of permutations of market demand, weather conditions, and infrastructure investment, which will be accomplished through supercomputing resources at LLNL.

The CES-21 Cybersecurity project is comprised of a joint team of technical experts from the California IOUs, industry, academia, LLNL, and other national laboratories and contractors as appropriate. Similarly, Grid Integration is comprised of a joint team of technical experts from industry, software vendors, PG&E and SDG&E, and LLNL.

b. Status of Program

The California Public Utilities Commission (CPUC or Commission) authorized the CES-21 Program for five years beginning on October 2, 2014, upon the approval of the Joint Utilities’ CES-21 request (see PG&E Advice Letter 4402-E, approved by the Commission in Resolution E-4677). In December 2014, the major stakeholders defined participants’ rights and working relationship in the Cooperative Research and Development Agreement (CRADA). In 2015, the joint team was focused on ramping up resources, defining a Work Breakdown Structure, and making progress on research goals.
In 2015, the Cybersecurity project moved from planning to staging and process design for R&D of the MMATR system. During 2015, the 10 cybersecurity tasks were baselined and budgeted to reflect the team’s understanding and prioritization of tasks. LLNL was assigned lead over the modeling and simulation tasks as well as the final solution integrator, and Idaho National Laboratory (INL) was contracted to host the CES-21 Cybersecurity Test Bed and design the ecosystem for automatic remediation of threats to Industrial Control System networks. Specific highlights from 2015 include:

- **Program Governance and Foundational Collaboration:** Established subcontractor relationships and program governance guidelines;
- **Modeling Engine:** Continued development of components for processing/storing threat intelligence; completed two (of five) software development spirals for the Indicator Language;
- **Physical Test Bed:** Received hardware and software required for initial setup of test bed and completed initial configuration;
- **Extensible Research Package:** Coordinated knowledge-sharing with federal agencies to identify research synergies; developed initial documentation (functional requirements, organizational interface and process flow diagrams); and
- **Research Objectives:** Began work on basic research objectives across tasks.

In 2015, the Grid Integration project modeled over 150,000 simulations of yearly system performance under different weather conditions and demand expectations, and has held multiple public workshops demonstrating the results of these models. The models have been run on traditional computing resources; at the end of 2015, the models were in the process of being optimized to run on LLNL’s high-performance supercomputing resources. This will enable simulation rounds that would be prohibitively time-consuming if run on traditional resources. Specific highlights from 2015 include:

- Developed a holistic framework and model that can assess an electric system’s need for capacity and flexibility in terms of reliability, cost and emissions;
- Created new reliability metrics to explicitly measure loss of load occurrences due to lack of operating flexibility;
- Applied the framework and model on 40 projected California Independent System Operator (CAISO) systems through simulation of over 150,000 individual years of system conditions at 5-minute interval granularity; and
- Examined and quantified the value of flexibility using a holistic set of metrics.

c. **Lessons Learned**

**Cybersecurity:** Given that 2015 was the start-up year for the program, the learnings regarded the coordination of different utilities and national labs, as well as initial technical development.

- Model fidelity as a decision point for utilities working to produce models that are both extensible and actionable. If a model (and the language used to encode it) is too specific, it cannot be used by utilities with different equipment or configurations. If it is too vague, the results of the model are not actionable or applicable for a single utility. Finding the effective compromise between these
extremes is an important step toward producing a model that can be productized by the private sector and used by utilities across the country.

- The work to automate the grid’s cyberthreat responses is nascent but fast growing. California is at the forefront of a research area that is attracting increased funding at the state and federal level for machine-assisted threat detection for ICS.

**Grid Integration:** Initial results, based on the 2014 Long-Term Procurement Plan (LTPP) assumptions, were presented to the public at a Commission workshop in January 2016, and included the following key learnings:

- The projected CAISO system has sufficient flexibility and capacity to meet the 1 day in 10 years standard in 2024, assuming no incremental retirements for the 40% RPS case.
- A less flexible system yields higher costs and greenhouse gas emissions (across the flexibility sensitivities studied).
2. Introduction and Overview

The purpose of this annual report is to provide the Commission with a summary of the 2015 progress of the CES-21 Program and the two projects of which it is comprised (Cybersecurity and Grid Integration). This is part of the reporting requirements detailed in Ordering Paragraph 21 of Decision (D.) 14-03-029.

a. Background on CES-21

The CES-21 Program is a public-private collaborative R&D program between the Joint Utilities and LLNL. The CES-21 Cybersecurity project will utilize a joint team of technical experts as best fits the research objectives from the utilities, LLNL, industry, academia, and other contractors as appropriate to meet the research objectives consistent with the approved CES-21 Program. The Joint Utilities are using contractor partners and other national laboratories beyond LLNL.

b. CES-21 Program Components

Cybersecurity: The MMATR project is intended to develop automated response capabilities that could protect critical infrastructure against cyberattacks, with grid survivability as a primary objective. Due to the time criticality and increasing volume of cyberattacks, the only way to effectively protect the critical infrastructure is through automated response capabilities.

Grid Integration: The Grid Integration project proposes to study use of planning and reliability metrics (such as the 15% Planning Reserve Margin) under the future grid conditions caused by increased renewable energy penetration and market demand.

c. CES-21 Program Regulatory Process and History

On July 18, 2011, the Joint Utilities filed Application 11-07-008, which requested authority to recover the costs for funding the CES-21 Program up to a maximum of $152.19 million over five years, with the funding shared among the Joint Utilities as follows: PG&E – 55%, SCE – 35%, and SDG&E – 10%.

In December 2012, the Commission issued D.12-12-031, which authorized the Joint Utilities to enter into a five-year R&D agreement with LLNL. This decision authorized the Joint Utilities to spend up to $30 million a year for five years on research activities, for a total of $152.19 million. The decision also allocated these costs to each of the utilities (PG&E – 55%, SCE – 35%, and SDG&E –10%) and adopted a ratemaking mechanism for each utility to permit recovery of those costs.

On September 26, 2013, Governor Brown signed Senate Bill (SB) 96, which included language that limited the scope of the CES-21 Program to cybersecurity and grid integration R&D. These projects were not to exceed $35 million over a five-year period.1 As part of SB 96, the California legislature directed the Commission to require the Joint Utilities to prepare and submit a joint report by December 1, 2013.2 In compliance with this legislative directive, the Joint Utility Report described:

1. Scope of all proposed research projects

---

1 SB 96 added Section 740.5 to the Pub. Util. Code.
2. How proposed projects may lead to technological advancement
3. How proposed projects may lead to potential breakthroughs in cyber security and grid integration
4. Expected timelines for concluding the projects

On March 27, 2014, the Commission approved D.14-03-029, which modified D.12-12-031 to comply with SB 96. In this decision, the Commission:

- Reduces the CES-21 budget to $35 million (including “franchise fees” and “uncollectibles”) over a five-year period;
- Limits areas of research to “cybersecurity” and “grid integration”;
- Reduces the governance structure to three Program Managers from PG&E, SCE and SDG&E;
- Revises budget split to PG&E – 50%, SCE – 41%, and SDG&E – 9%;
- Voids any CES-21 Program Management expenditures incurred to date and caps future administrative expenses to no more than 10% of the total CES-21 budget;
- Requires enhanced Legislative and Commission oversight of the CES-21 Program; and
- Revises the CRADA guidelines and project criteria accordingly.

On April 25, 2014, the Joint Utilities filed Advice Letter 4402-E, which sought Commission authorization to implement the CES-21 Program pursuant to D.12-12-031 and D.14-03-029. The Commission approved Advice Letter 4402-E in Resolution 4677-E on October 2, 2014.

In compliance with Resolution 4677-E, on October 9, 2014, the Joint Utilities filed Advice Letter 4516-E with updated CES-21 business cases, an updated CRADA, a letter from LLNL confirming that the cybersecurity project reflects a new contribution and does not duplicate past research efforts, and an updated Joint Utility Report on the scope of the CES-21 Program’s proposed research projects.

The Commission also approved advice letters filed by the Joint Utilities, pursuant to D.12-12-031, to create a CES-21 balancing account or modify an existing balancing account to collect money related to CES-21.

The Commission requires the Joint Utilities to submit an annual report that provides information on the operations of the project, including projects funded, the results of the research, the efforts made to involve academics and other third parties, and the intellectual property that results from the research by March 31 of each year of the program. The Commission also requires the Joint Utilities to submit a report required by Public Utilities Code (Pub. Util. Code) Section 740.5(e)(2) summarizing the outcome of all funded projects, including an accounting of all expenditures by program managers and grant recipients on administrative and overhead costs, and whether the project resulted in any technological advancements or breakthroughs in promoting cybersecurity and grid integration.

---

3 Submitted to the Commission on November 27, 2013.
d. Pre-Filing Workshop Results

In D.14-03-029, the Commission required the following:

“As part of the Supplemental Advice Letter process, the Project Managers, in cooperation with Energy Division, shall hold a public workshop including the California Public Utilities Commission at least 45 days in advance of the filing to discuss the proposed research and priorities and to review the business case for proposed research. The Commission shall review the Tier 3 Supplemental Advice filing to ensure its consistency with the policy requirements adopted in this decision and enumerated in Ordering Paragraphs 15-16.” (D.14-03-029, OP 18.)

In 2015, the Joint Utilities did not file any Supplemental Advice Letters, and as such did not hold any public workshops.

e. Industry Trends Impacting Program and Projects

Cybersecurity: Information technology evolves quickly, particularly in cybersecurity. Attacks on enterprise Information Technology systems and operational ICS continue to increase at a staggering rate, and this has pushed the industry to respond. The “Dragonfly” attack⁴ was widely published in the summer of 2014,⁵ but details of the attack stayed within technical circles. In 2015, the threat of power grid attacks became more widely understood:

- U.S. law enforcement revealed in the fall of 2015 that terrorist groups were interested in attacking the nation’s power grid.⁶
- Journalist Ted Koppel’s Lights Out was published and quickly became a New York Times bestseller.⁷ Koppel’s book describes the potential effects of a cyber-caused blackout in stark terms.
- The December 2015 attack on Ukraine’s power grid made the public more aware that the power grid is vulnerable to cybersecurity threats.⁸

The complexity of the recent intrusions and the software used emphasize the need for automated or semi-automated response to future attacks on the grid. Specifics from these attacks have been used within the CES-21 Cybersecurity project to inform use cases that are referenced by each task area throughout the R&D lifecycle.

The growing need for cybersecurity research for the power grid is also being embraced by the federal government. Recently, the Department of Energy (DOE) announced $34 million of investment into two new R&D projects that will address security of the electric grid and oil and gas infrastructure.⁹ Additionally, DOE has launched the Grid Modernization Laboratory Consortium (GMLC)¹⁰ to address modernization of the

---

⁵ https://www.tofinosecurity.com/blog/dragonfly-malware-targets-ics-systems.
electric grid. One focus area of the GMLC is Security and Resilience. CES-21 team members are actively involved in the GMLC and are discussing ways to collaborate with the R&D projects previously announced.

*Grid Integration:* On October 7, 2015, Governor Brown signed SB 350, which includes language that requires 50% of the commercially-generated electricity sold to retail customers in California be generated from renewable sources by 2030.

As a result, the CPUC is currently undertaking the task of incorporating this requirement into the input assumptions and scenarios for the 2016 LTPP. The Grid Integration project team is actively participating in that effort, and will adopt a higher renewables scenario in the project’s final phase of analysis. This is consistent with the requirements from Resolution E-4677, and will capture any heightened grid integration challenges as California pursues an even higher renewables target.

f. **Coordination**

i. **Industry Coordination**

Throughout 2015, the CES-21 Program has engaged industry, federal agencies, and national labs in collaboration on cybersecurity research topics. This has assisted the MMATR project on two fronts:

- Research on potential duplication of cybersecurity R&D
- Knowledge sharing on machine-speed-learning-focused cybersecurity research

Specifically CES-21 staff have researched over 25 different companies and engaged those with leading-edge products capable of furthering the research objectives of the CES-21 Program. In addition to ongoing collaboration or partnerships with national labs (LLNL, PNNL and INL), the project has also been interfacing with DOE, the National Security Agency (NSA) and the Department of Homeland Security (DHS).

ii. **Internal Coordination**

The CES-21 partner group (IOUs and LLNL) has developed a strong working relationship and regular cadence of meetings, including:

- Weekly meetings of the Project Leads and Program Managers to discuss progress and surface program-wide challenges;
- Quarterly in-person technical meetings to share information, lessons learned and integration challenges, as well as understanding mutual progress and resolving coordination issues; and
- Quarterly Steering Committee Meetings with IOU and LLNL leadership.
3. Budget (by Year, by Research Area)

### MMATR

<table>
<thead>
<tr>
<th></th>
<th>Actuals</th>
<th>Actuals</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commitments/Encumbrances</td>
<td>-</td>
<td>-</td>
<td>5,030,802</td>
<td>14,979,290</td>
<td>13,119,526</td>
<td>33,129,618</td>
</tr>
<tr>
<td>In House Project Expenses</td>
<td>151,638</td>
<td>445,957</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

### Grid Integration

<table>
<thead>
<tr>
<th></th>
<th>Actuals</th>
<th>Actuals</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commitments/Encumbrances</td>
<td>-</td>
<td>-</td>
<td>583,229</td>
<td>1,240,000</td>
<td>-</td>
<td>1,823,229</td>
</tr>
<tr>
<td>In House Project Expenses</td>
<td>-</td>
<td>8,970</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>8,970</td>
</tr>
</tbody>
</table>

### CES 21 Program Total

<table>
<thead>
<tr>
<th></th>
<th>Actuals</th>
<th>Actuals</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commitments/Encumbrances</td>
<td>-</td>
<td>-</td>
<td>5,614,031</td>
<td>16,219,290</td>
<td>13,119,526</td>
<td>34,952,847</td>
</tr>
<tr>
<td>In House Project Expenses</td>
<td>151,638</td>
<td>454,927</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>606,615</td>
</tr>
</tbody>
</table>

**Definitions:**
- In House Project Expenses: all project and admin expenses not completed through vendor or partner sub-contract.
- Commitments: both contracted purchase orders and planned commitments.
4. Projects

Cybersecurity: Machine-to-Machine Automated Threat Response

a. High Level Summary

The MMATR project aims to further the research of advanced cybersecurity technology and tools not currently commercially available. This advancement in cyber technology could help the Joint Utilities to identify and take action on advanced cyberthreats to SCADA and ICS before they impact California’s critical infrastructure. The end result of the MMATR project is the advancement of research toward a threat-aware grid architecture capable of making real-time decisions to increase the grid’s survivability and resiliency.

b. Project Status Report

The MMATR project is divided into 10 tasks. Each is autonomous but represents a building block that may be integrated into an end-to-end system as the research reaches maturity and integration of the building blocks is shown to be feasible. The year 2015 was foundational for the MMATR project; the Joint Utilities team developed shared program management guidelines, tasks began work on their individual research objectives, and subcontractors were engaged. Use Case development began with a workshop facilitated by the Electric Power Research Institute and has continued throughout the year with the engagement of Transmission and Distribution subject matter experts. Vendors were placed under contract to deliver statements of work for research objectives using agile spiral development cycles. The first iteration of the Indicator and Remediation Language task (which will allow disparate systems to encode, and thus simulate, threat scenarios) was created. Three key technical meetings were also held to share information and work through dependency issues in person, and the teams meet in weekly conference calls to stay aligned and coordinated.

c. Project Details

i. Objective

The main objective of the CES-21 Cybersecurity Project is to conduct R&D toward building MMATR technology. Automated response capabilities could help IOUs’ critical infrastructure survive an increasing density of cyberattacks. Due to the time criticality of cyberattacks on ICS, the most effective way to effectively protect the critical infrastructure from a cyberattack is potentially through automated response capabilities. In the context of the MMATR R&D project, automated response capabilities will be explored through the combination of data integration, advanced modeling, simulation and analytics. The long-term goal is to provide proactive cybersecurity problem-solving capabilities for the current and future electrical system and ultimately protect grid stability, service reliability, and public safety.

ii. Scope

The scope of individual MMATR tasks may change over the course of the project, based on task progression, identification of technological requirements, and research needs. Please refer to Advice Letter 4516-E (Section 3c) for a detailed description of project scope, and see Appendix A for details on the scope of each task within MMATR. If any of the current tasks change during the course of the MMATR research the CES-21 Program Managers will inform CPUC Energy Division in advance.
iii. Deliverables

To meet the MMATR project’s main objective of researching automated response capabilities to protect IOU critical infrastructure against cyberattacks, the project is expecting to deliver:

- High-impact risk scenarios applicable to all California IOUs to serve as a research foundation for all other tasks;
- An updated open source Indicator Remediation Language (IRL) applicable to the Joint IOUs and encompassing their needs;
- Data aggregation and advanced analytics capabilities to collect and analyze ICS data pertinent to defending the network and support the detection of unknown cyberthreats to ICS networks;
- A modeling and simulation platform with associated documentation to test cyberattack scenarios under a variety of utility configurations;
- A physical Test Bed which can run physical test scenarios and uses the IRL to exercise modeling scenarios to understand responsiveness and effectiveness of MMATR solutions;
- A stronger SCADA Security Protocol to protect SCADA infrastructure and ultimately improve grid resilience and stability; and
- Documentation describing a process for public release of research findings and handling of sensitive information.

iv. Business Case Analysis

The value proposition and potential customer benefits detailed in the updated business case submitted as part of Advice Letter 3115-E (November 14, 2014) continue to apply to the MMATR project. The Joint Utilities are managing closely to the post-SB 96 budget, and are maintaining budget compliance requirements.
v. Evaluation Metrics

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement / Deliverable</th>
<th>2015 Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Semiannual progress update meetings held with ED or ED-named proxies</td>
<td>Achieved.</td>
</tr>
<tr>
<td>2</td>
<td>Monthly progress reports delivered to CPUC</td>
<td>Achieved.</td>
</tr>
<tr>
<td>3</td>
<td>Maintain project financial governance in line with compliance requirements</td>
<td>Achieved.</td>
</tr>
<tr>
<td>4</td>
<td>Establish guidelines for program management, shared responsibilities, and classification of sensitive data.</td>
<td>Achieved.</td>
</tr>
<tr>
<td>5</td>
<td>Development of IOU-agnostic threat scenario use cases</td>
<td>First use case developed, use case format and register established, use case development workflow ratified.</td>
</tr>
<tr>
<td>6</td>
<td>Development of machine-readable language conventions to describe threats</td>
<td>First iteration of the IRL developed.</td>
</tr>
<tr>
<td>7</td>
<td>Ability to model and simulate threat scenarios</td>
<td>Continued development of components for processing/storing threat intelligence</td>
</tr>
<tr>
<td>8</td>
<td>Ability to test models and scenarios using physical models of equipment configurations</td>
<td>Successfully received hardware and software required for initial setup of test bed and completed initial configuration.</td>
</tr>
<tr>
<td>9</td>
<td>Document learnings and requirements for integration of CES-21 funded research, and ensure non-duplication of research effort</td>
<td>Multiple coordination meetings held with agency and national lab representatives.</td>
</tr>
</tbody>
</table>

vi. Schedule

The CES-21 MMATR project launched in October 2014 (with authority to spend beginning on December 29, 2014), and currently anticipates completion in October 2017. The current schedule includes an additional three months after October 2017 to develop and finalize documentation.

The current project plan lasts three years (2014-2017) as the joint utilities anticipate the current funding level to be exhausted based on current research objectives, although the CPUC approved a five-year project schedule. The project team is performing periodic evaluations to determine whether research findings and project objectives require extension into the five-year timeframe.

vii. CES-21 Funds Spent

Please see Section B for all budget information.

viii. Treatment of Intellectual Property

Treatment of Intellectual Property is described by the CRADA, signed by the Joint IOUs and LLNL.
## ix. Status Update

<table>
<thead>
<tr>
<th>Program Governance and Foundational Collaboration</th>
<th>Physical Test Bed</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Established subcontract relationships with multiple vendors for CES-21 cybersecurity tasking</td>
<td>• Collected initial equipment lists and down-selected those relevant to the anticipated substation equipment</td>
</tr>
<tr>
<td>• Started individual laboratories at each of the IOUs for CES-21 research</td>
<td>• Successfully received hardware and software required for initial setup of test bed and completed initial configuration</td>
</tr>
<tr>
<td>• Drafted and agreed upon Program Governance Guidelines to define shared responsibilities and processes</td>
<td>• Provided training on the setup and operational use of the test bed devices for vendor partner and lab engineers</td>
</tr>
<tr>
<td>• Submitted monthly status reports to Energy Division and biannual check-in presentations</td>
<td>• Developed a set of wiring and communications diagrams to ensure setup process is repeatable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Modeling Engine</th>
<th>Extensible Research Package (for use by wider utility community and private sector vendors)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Finalized workflow for use case development and launched risk register to track use cases across the project</td>
<td>• Continue to work across industry and federal agencies to ensure non-duplication and identify areas of synergy with CES-21 research objectives</td>
</tr>
<tr>
<td>• Performed SCADA protocol network traffic analysis</td>
<td>• Developed a valid set of functional requirements as well as an organizational interface and process flow diagrams as part of efforts to document the operational concept for the MMATR Ecosystem</td>
</tr>
<tr>
<td>• Continued development of components for processing/storing threat intelligence; completed two (of five) software development spirals for the Indicator Language</td>
<td>• Designed and developed attack code model in scenario simulation</td>
</tr>
</tbody>
</table>
Grid Integration: Flexibility Metrics

a. High Level Summary
Simulate the effects of using existing reliability and capacity metrics under various conditions and greatly increased renewable penetration.

b. Project Status Report
Overall, the Grid Integration project has completed three of its five phases, and is currently expected to complete in 2016. Resolution E-4677 provided specific requirements and key deliverables which help shape the evaluation metrics and also facilitated the development of a revised work plan (details provided in Sections IV and VI below).

c. Project Details
i. Objective
The Grid Integration project seeks to analyze current flexibility metrics under future conditions and recommend (if appropriate) new or modified planning standards that explicitly consider operational flexibility.

Please refer to Advice Letter 4516-E (Section 3b) for a detailed description of project objective.

ii. Scope
The scope of the Grid Integration project is to develop a holistic framework (i.e., tools, models, and metrics) to study the flexibility needs of the California electrical system under higher Renewable Energy penetration.

Please refer to Advice Letter 4516-E (Section 3c) for a detailed description of project scope.

iii. Deliverables
For the Grid Integration project, Resolution E-4677 provided the following key deliverables:

- Preliminary results and recommendations, presented in a public workshop using input assumptions from the 2014 LTPP
- Demonstration of recommended metrics/standards in 2016 LTPP using at least one of the 2016 LTPP scenarios (Trajectory or expected scenario)
- Opportunity for 2016 LTPP parties to comment
- Database of detailed modeling input assumptions
- Ensured ability of LTPP parties to license and use new or improved tools (if any)
- Informal training session for Commission staff on new tools and models

iv. Business Case Analysis
The Grid Integration project is moving forward according to its original business case. Much of the work in 2015 was dedicated to reviewing, developing and demonstrating a holistic framework (i.e., tools, models, and metrics) to study the flexibility needs of a system. Specifically, the project team
determined it most effective to build on top of the Strategic Energy & Risk Valuation Model (SERVM) software tool. While this model will require procuring time on LLNL’s High Performance Computing (HPC) platform, such capability will significantly speed up the analytical process and allowing additional studies to be performed.

v. Evaluation Metrics

For the Grid Integration project, the requirements and deliverables specified by Resolution E-4677 helped shape the appropriate evaluation metrics. They are listed below, along with specific results delivered in 2015 (additional details are provided further below in Section IX, Status Update).

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement / Deliverable</th>
<th>2015 Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Form a collaborative Advisory Group and meet at least once every six months to review and connect project results with relevant CPUC proceedings</td>
<td>Held three in-person advisory group meetings</td>
</tr>
<tr>
<td>2</td>
<td>Present preliminary results and recommendations in a public workshop using input assumptions from the 2014 LTPP</td>
<td>Workshop held on January 6, 2016</td>
</tr>
<tr>
<td>3</td>
<td>Demonstrate recommended metrics/standards in 2016 LTPP using at least one of the 2016 LTPP scenarios (Trajectory or expected scenario)</td>
<td>To be completed in 2016 pending final CPUC approval of 2016 LTPP scenarios</td>
</tr>
<tr>
<td>4</td>
<td>Provide 2016 LTPP parties opportunity to comment</td>
<td>To be completed in 2016; informal comments already received following the January 2016 public workshop</td>
</tr>
<tr>
<td>5</td>
<td>Make database of detailed modeling input assumptions available</td>
<td>To be completed in 2016; provided advisory group members modeling changes to date</td>
</tr>
<tr>
<td>6</td>
<td>Ensured ability of LTPP parties to license and use new or improved tools (if any)</td>
<td>Updated SERVM software is available for license by LTPP parties</td>
</tr>
<tr>
<td>7</td>
<td>Offer informal training session for Commission staff on new tools and models</td>
<td>To be completed in 2016</td>
</tr>
</tbody>
</table>

vi. Schedule

Currently the Grid Integration project follows a two-year schedule and is expected to finish in 2016. Slight delays in the public release of the 2016 LTPP input assumptions had an impact on the project schedule, but the project is still on track to complete by the end of 2016.

vii. CES-21 Funds Spent

Please see Section B for all budget information.

viii. Treatment of Intellectual Property

Treatment of Intellectual Property is described by the CRADA, signed by the Joint IOUs and LLNL.
ix. **Status Update**

Grid Integration has completed three of its five phases. The project team defined a workplan and finalized consulting contracts. SERVM software was refined to incorporate new flexibility metrics. To date, two cycles of simulations (18 sensitivity studies using the 2014 LTPP 33% RPS scenario, and 22 sensitivity studies using the 2014 LTPP 33% RPS and 40% RPS scenarios) have been completed. The team held three advisory group meetings, participated in three CPUC briefings, and presented initial results in one public workshop.
5. Conclusion

a. Key Results for the Year

Grid Integration completed three of its five project phases and released initial simulation results to the public. Key Cybersecurity results for 2015 included:

- **Program Governance and Foundational Collaboration:** Established subcontractor relationships and program governance guidelines; instituted quarterly technical and steering committee meetings;
- **Modeling Engine:** Continued development of components for processing/storing threat intelligence; completed two (of five) software development spirals for the Indicator Language;
- **Physical Test Bed:** Received hardware and software required for initial setup of test bed and completed initial configuration; and
- **Extensible Research Package:** Coordinated knowledge sharing with federal agencies to identify research synergies; developed initial documentation (functional requirements, organizational interface and process flow diagrams).

b. Next Steps for CES-21 Projects

- **Cybersecurity:** Continue work on Tasks (see Appendix A) while maintaining compliance requirements. Encourage knowledge-sharing through program collaboration and interfacing with federal agencies, other utilities, and private sector vendors who are advancing research in this space.

  Grid Integration: Continue with project plan, including transition to the SERVM model on LLNL’s HPC Platform and integration of the finalized 2016 LTPP assumptions.

c. Issues That May Have Major Impact on Progress in Projects

The Joint Utilities have not identified any issues that may have a major impact on the CES-21 Program at this time.

d. Lessons Learned

- **Cybersecurity:** Given that 2015 was the start-up year for the program, many learnings regarded the coordination of different utilities and national labs.

  - Model fidelity is a decision point for utilities trying to collaborate on research. If models are too specific to a utility’s configuration, they are not applicable for other IOUs. If they are too broad, precision is lost and the model’s results are less actionable.

  - The work to automate threat responses is in a nascent phase in the energy community. Federal agencies like DHS and NSA are beginning to conduct machine-speed learning cybersecurity research, and the DOE is funding programs to pursue cybersecurity protections of the Bulk Electric System. California is at the forefront of state-based research for this necessary technological development, and the CES-21 Program is in close contact with federal research organizations to avoid duplication and increase synergies.
**Grid Integration:** Lessons learned in Grid Integration were from the successful initial flexibility analysis of the system. These results, based on the 2014 LTPP assumptions, were presented to the public at a Commission workshop on January 6, 2016, and included:

- The projected CAISO system—under the 33% and 40% RPS scenarios—has sufficient flexibility and capacity to meet the “one day in ten years” standard in 2024 assuming no incremental retirements (consistent with the 2014 LTPP assumptions);
- The projected CAISO system has sufficient hourly ramping capability largely due to flexibility obtained through RPS curtailments and net imports from neighboring Balancing Areas;
- The projected CAISO system must set aside sufficient intra-hour ramping capability (i.e., operating reserves) in order to meet the “one day in ten years” standard;
- A less flexible system yields higher costs and emissions (across the flexibility sensitivities studied); and
- Modeling a large number of novel, complex sensitivity cases can benefit from an iterative process: modeling results can inform the refinement of modeling assumptions and methodology.
Appendix A – Scope by Task of CES-21 Cybersecurity Project

<table>
<thead>
<tr>
<th>Task</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1 - Use Case Generation</td>
<td>Ongoing development of high-impact cyber risk scenarios that are applicable to all California IOUs with a primary focus on the transmission grid. Use cases will be developed throughout the life of the project. The CES-21 partners will select a small number of Use Cases (risk scenarios) to guide simulation and piloting across each of the MMATR tasks.</td>
</tr>
<tr>
<td>Task 2 - Data Aggregation</td>
<td>Development of methods to collect Industrial Control System information (SCADA data, Substation and Network Device Configurations) and the standardization of formats for structuring CES-21 information.</td>
</tr>
<tr>
<td>Task 3 - Modeling and Simulation</td>
<td>Identifying and fulfilling the capability requirements for modeling and simulating grid and communication systems in support of other MMATR CES-21 chartered tasks.</td>
</tr>
<tr>
<td>Task 4 - Test Bed</td>
<td>Evaluating replications of IOU equipment in a physical test bed against new and cutting edge exploits to verify responsiveness and effectiveness of MMATR solutions.</td>
</tr>
<tr>
<td>Task 5 - Advanced Threat Detection</td>
<td>Developing methods for monitoring and detecting anomalies in SCADA communications, processing Machine Readable Threat Intelligence, and translating this intelligence into threat scenarios.</td>
</tr>
<tr>
<td>Task 6 - Indicator and Remediation Language</td>
<td>Identifying and analyzing current available indicator languages and selecting one for use within the CES-21 Program. The selected language will be adapted to support additional needs that the IOUs have for such technology.</td>
</tr>
<tr>
<td>Task 8 - SCADA Ecosystem Resiliency</td>
<td>Developing the processes required for automatic recognition of ICS compromise and remediation in a control systems environment.</td>
</tr>
<tr>
<td>Task 9 - Grid Stability Framework</td>
<td>Evaluating detection and response strategies for a wide variety of viable attack scenarios affecting the California grid, through the delivery of a modelling and simulation platform. The modeling platform will test impacts from scenarios and from MMATR solutions in ICS networks.</td>
</tr>
<tr>
<td>Task 10 - Secure System Interface Environment</td>
<td>Developing a SCADA Security Protocol for the 21st Century (SSP-21) by providing certificate-based authentication and integrity with encryption options for any SCADA protocol. Additionally, Task 10 will include pursuing cutting edge research into secure authentication mechanisms.</td>
</tr>
<tr>
<td>Task 11 - Documentation and Integration</td>
<td>Provide guidelines and documentation to aid in information handling across the project, facilitating integration between tasks, and ensuring non-duplication of R&amp;D efforts.</td>
</tr>
</tbody>
</table>