Pacific Gas and Electric Company®

Brian K. Cherry
Vice President
Regulatory Relations

Pacific Gas and Electric Company
77 Beale St., Mail Code B10C
P.O. Box 770000
San Francisco, CA 94177

Fax: 415.973.7226

November 27, 2013

Mr. Paul Clanon
Executive Director
California Public Utilities Commission
505 Van Ness Avenue
San Francisco, CA 94102

Re: December 1, 2013 Joint Utility Report on the Scope of Proposed Research Projects

Dear Mr. Clanon:

Pursuant to Senate Bill (SB) 96, Public Utilities Code Section 740.5 (e)(1), Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), and San Diego Gas & Electric Company (SDG&E), collectively referred to as the Joint Utilities, submit the attached Joint Utility Report on the Scope of Proposed Research Projects for the California Energy Systems for the 21st Century (CES-21) Program.

On September 26, 2013, Governor Brown signed Senate Bill (SB) 96, which among other things, limits the scope of the CES-21 program, as previously approved by the California Public Utilities Commission (Commission) in Decision (D.) 12-12-031, to cyber security and grid integration research and development projects not to exceed $35 million over a five year period. 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. In compliance with this legislative directive, this Joint Utility Report describes (1) the scope of all proposed research projects, (2) how the proposed project may lead to technological advancement and potential breakthroughs in cyber security and grid integration, and (3) the expected timelines for concluding the projects.

If you have any questions regarding this report, please contact Erik Jacobson at (415) 973-4464 or ebj1@pge.com.

Sincerely,

Brian Cherry /IG

Brian Cherry
On behalf of PG&E, SCE, and SDG&E

Attachment: Joint Utilities' Report on CES-21 Program's Proposed Research Projects

cc: A.11-07-008 Service List
Edward Randolph, Energy Division Director
Damon Franz, Energy Division

Joint Utility Report on the Scope of Proposed Research Projects

December 1, 2013

As required by Senate Bill 96, Public Utilities Code Section 740.5 (e)(1)

1. Introduction

On September 26, 2013, Governor Brown signed Senate Bill (SB) 96, which among other things, limits the scope of the California Energy Systems for the 21st Century (CES-21) program, as previously approved by the California Public Utilities Commission (Commission) in Decision (D.) 12-12-031, to cyber security and grid integration research and development projects not to exceed $35 million over a five year period. As part of SB 96, the California legislature directed the Commission to require the Joint Utilities – Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), and San Diego Gas & Electric Company (SDG&E) – to prepare and submit a joint report by December 1, 2013. In compliance with this legislative directive, this Joint Utility Report describes (1) the scope of all proposed research projects, (2) how the proposed projects may lead to technological advancement, (3) how the proposed projects my lead to potential breakthroughs in cyber security and grid integration, and (4) the expected timelines for concluding the projects.[1]

This Report describes two projects that are being proposed at this time. As established by SB 96, one project is in the area of cyber security and the other is in the area of grid integration. Consistent with the general process established in D.12-12-031, the Joint Utilities plan to submit an advice letter in January 2014 that includes business cases for these two proposed research projects. These business cases will provide more information on the topics addressed in this report. As such, the proposal outlined herein is by its nature preliminary and subject to change based on further development of the business cases and input from stakeholders.

2. Cyber Security and Grid Integration

As a national energy policy leader, it is critically important for California to support cutting edge research and development (R&D) in the areas of cyber security and grid integration. Cyber-attacks against critical infrastructure are increasing in frequency and sophistication at an alarming rate. Technologies currently used to protect our grid infrastructure against such attacks are ill-equipped to deal with these emerging

[1] SB 96, Public Utilities Code Section 740.5 (e)(1).

threats. The proposed research is designed to develop automated response capabilities using innovative cyber security and grid technology. This research will analyze grid-connected cyber systems to develop a defense against cyber threats that would be pervasive throughout a more thoroughly integrated grid. A threat-aware grid architecture capable of making real-time decisions is needed in order to increase survivability and resiliency.

Similarly, the challenges of grid integration, particularly with respect to grid integration of renewable resources, are an important area for further research in order to move from the current levels of renewable resource integration to a much larger scale of renewable integration, even above the levels required to meet California's Renewable Portfolio Standard of 33% renewables integration by 2020.

2.a. Scope of Proposed Research Projects

i. Cyber Security

Fundamental research in industrial control systems (ICS) cyber security is lacking currently. Valuable future research topics include:

- Automatic detection of advanced threats given indicators;
- Automated response to threats;
- Operating ICS infrastructure in the face of constant attack (how to build a "resilient" grid); and
- Modeling and simulation of threats and response scenarios

The proposed cyber security research for CES-21 is focused on developing automated response capabilities to protect critical California infrastructure against cyber-attacks. Due to the time criticality of these cyber-attacks, the best way to effectively protect the critical infrastructure will be through automated, machine-to-machine communications to assess key indicators and develop appropriate responses. However, developing such automated machine-to-machine defenses is a very ambitious goal and it is uncertain where the research will lead. The research team will have flexibility to change direction depending on preliminary research results and findings. Such a dynamic approach will improve the chance of success in discovering new and innovative approaches, products, and solutions to emerging cyber security threats. Cyber security is a broad research topic and having a flexible approach to the R&D effort will have a positive effect on the outcome of the research.

ii. Grid Integration

Grid integration is a "cross cutting" research category that relates to electric resource planning and electric system operations, two of the four original research categories previously adopted in D.12-12-031. The challenges of grid integration, particularly with respect to grid integration of renewable resources, are widely recognized as an important research area for the state. In particular, in order to achieve important environmental goals, California's electric system is going through a significant transformation, replacing conventional generation with increasing amounts of intermittent renewable resources, and other resources that have limited operating flexibility.

While all of the research topics proposed by the utilities under the electric resource planning and electric system operations categories enable improved grid integration of renewable resources, the Flexibility Metrics and Standards project, as previously proposed, is anticipated to provide benefits to customers through improved long term resource planning.

In light of the revised research funding level established by SB 96, the utilities have narrowed the scope of the initially proposed Flexibility Metrics and Standards project. Specifically, the Flexibility Metrics and Standards project is intended to:

1. Review existing planning metrics and tools now in use or under development;
2. Develop and operationalize new planning metrics, such as insufficient ramping capacity, that a system requires to balance loads and resources during different time intervals; and
3. Develop new or improved resource planning models that incorporate the system's flexibility metrics and requirements with traditional production simulation and reliability models to: (a) measure the contribution of different types of resources toward the system's flexibility requirements, (b) determine the residual system needs, and (c) determine the cost-effectives of different alternatives to meet identified system needs.

2.b. How the Proposed Projects May Lead to Technological Advancement in Cyber Security and Grid Integration

Automated threat detection and response are areas that have been and continue to be heavily studied in the traditional enterprise cyber security space. These areas are virtually unstudied in industrial controls systems (ICS). With respect to grid operations, new operating flexibility metrics and targets are needed for effective long-term resource planning in California. The proposed research and development projects will bring automated threat detection and response to the ICS environment and improvements to planning methodologies and models will be used to improve the integration of renewable resources.

Cyber security as applied to ICS is a nascent industry and is ripe for research and development. Open research topics include: detection of advanced threats, detection of previously unknown threats ("zero-day vulnerabilities"), automated response to threats, operating ICS infrastructure in the face of constant attack (i.e., how to build a "resilient" grid), modeling and simulation of threats and response scenarios, and vulnerability assessments and supply chain analyses of grid components.

The Utilities propose conducting R&D in several of these areas, integrating existing technologies where applicable and performing applied research when necessary. A goal of this research is to advance the state-of-the-art in automated threat detection and response as well as modeling and simulation in support of grid resiliency.

The proposed Grid Integration Planning Flexibility Metrics and Standards project will help quantify the future operating flexibility requirements of the system and determine the needs for operationally flexible resources, if any, in order to continue to provide reliable and affordable service to customers while at the same time meeting California's energy policy objectives.

Expected advances in grid integration include defining flexibility metrics (such as insufficient ramping capacity), operationalization of the flexibility metrics for long-term planning purposes, developing new or improved resource planning models that incorporate flexibility metrics with traditional production simulation and reliability models, developing new or improved tools to measure the contribution of different types of resources toward the system's flexibility requirements, and developing new or improved tools to determine the cost-effectiveness of different alternatives to meet identified system needs.

These proposed cyber security and grid integration projects will bring together the Utilities, all nationally recognized leaders, with Lawrence Livermore National Laboratory (LLNL), a Department of Energy (DOE) laboratory with a rich history in mathematics and computer science R&D, cyber security expertise, and world-renowned capabilities in high performance computing. This collaboration will, in turn, leverage state-of-the-art R&D and technologies being developed at other national laboratories and universities throughout California and the rest of the United States. It is fully expected that the integration of these technologies and subsequent research and development will lead to technological advancement that will benefit the California grid and state ratepayers.

2.c. How the Proposed Projects May Lead to Potential Breakthroughs in Cyber Security and Grid Integration

i. Cyber Security

The goal of this research is a context-aware California electric grid capable of making real-time decisions in response to cyber threats that increase its survivability and resiliency. Potential breakthroughs are expected in:

- Standard descriptive semantics for threats, responses, infrastructure, and processes;
- A secure approach to management, command, and control of the defenses;
- A standard, open architecture for distributed threat detection and automatic, localized response that provides a basis for commercially viable prototypes;
- Modeling and simulation tools for cyber defense of ICS networks; and
- Recommended responses to threats and threat categories.

ii. Grid Integration

New operating flexibility metrics and standards are needed for long-term resource planning in California. Improvements to methodologies and existing models, or new models, are also needed to reduce the cost and the uncertainty about the resource adequacy of planned resources to integrate greater amounts of intermittent renewables. Improvements to methodologies and models are also needed to facilitate the consideration and decision making in regulatory and stakeholder processes of planning issues related to the integration of renewable resources, including: (a) quantification of system

operating requirements, (b) estimates of the contribution of different resources to meet those requirements, (c) quantification of system residual need for resources, and (d) evaluation of the cost-effectiveness of resources alternatives with different operating attributes to meet residual system needs.

Traditional resource planning methods have used reserve margin metrics and targets, expressed as a percentage of forecast electric demand, to ensure that enough capacity is procured and available for operating the system. In the past, because of the small amounts of renewable resources in the system, the uncertainty and intermittency of generation like wind and solar was dwarfed by the uncertainty in electric load. Also, in the past, conventional resource additions provided the operating flexibility required by the uncertainty and intermittency of electric load.

SB 96 requires the Commission to ensure that the research parameters reflect a new contribution to cyber security and grid integration and that there is not a duplication of research being done by other private and governmental entities. Although the California Independent System Operator, the California Energy Commission, and others have invested in efforts to develop new stochastic approaches to estimate the residual need for flexible resources, these approaches require further examination and development before the methodology and models built based on these approaches are ready for use in resource planning or policy decisions. In particular, this research project is targeting potential breakthroughs to determine:

- Weather uncertainty effects on customer load and renewable generation;
- The electric grid's operational flexibility requirements;
- Operating limits of the existing or planned grid to integrate additional amounts of intermittent renewable generation; and
- Additional resources and cost to integrate additional renewable generation.

These breakthroughs would significantly enhance existing planning methodologies and models to facilitate the assessment and implementation of future energy policy initiatives and help achieve California's ambitious environmental goals.

2.d. Expected Budget and Timelines for Concluding the Research Projects

The cyber security research project will be executed over a three-year period and the grid integration project will be executed over two years. In both cases, the R&D effort and the expected outcomes are needed by the Utilities as soon as possible. The Utilities believe this is the best and most efficient use of the R&D dollars from a time sequenced perspective and well under the five-year plan as adopted in SB 96 and the original CPUC decision. The Cyber Security Machine to Machine Automated Threat Response Project is projected to spend $28 million over three years and the Grid Integration Flexibility Metrics and Standards Project is projected to spend $2 million over two years. The following tables summarize the forecasted spending over time for these two projects. The Utilities propose to reserve the remaining $5 million as additional funding available for the two proposed research projects. Any new cyber security

or grid integration research projects would be subject to Commission approval via a separate advice letter.

Cyber Security Machine to Machine Automated Threat Response: Estimated Project Costs

Year 1	Year 2	Year 3	Year 4	Year 5	Total
$11M	$9M	$8M			$28M

Grid Integration Flexibility Metrics and Standards: Estimated Project Costs

Year 1	Year 2	Year 3	Year 4	Year 5	Total
$1.2M	$0.8M				$2M

3. Conclusion

This proposal leverages the relationship between the Utilities, in concert with LLNL as well as potential partnerships with other DOE national labs, academia, and industry partners to develop the automated response capabilities needed to protect the state's critical infrastructure against cyber-attacks and to advance grid integration capabilities to meet California's energy policy objectives.

For cyber security, the ability to observe and react to threats more rapidly than the attacker will significantly enhance the system's ability to survive an attack. The advancement in cyber technology will enable the Utilities to identify and take action on advanced cyber threats before they impact California's critical infrastructure.

For grid integration, the ability to improve the representation of weather uncertainty and to quantify the electric grid's operational flexibility requirements, operating limits, and additional resources and costs needed to integrate additional intermittent renewable generation will significantly enhance the existing planning methodologies and models and will facilitate the assessment and implementation of California's future energy policy initiatives.