California Energy Systems for the 21st Century (CES-21) Program

Final Report

December 6, 2019

Revised to incorporate CPUC Input
January 6, 2020

Revised to finalize program financials
August 27, 2020

The CES-21 Cybersecurity R&D effort is focused on the protection of critical infrastructure, therefore a secure process for reporting and a secure process for deliverables will need to be maintained. Detailed tactics, techniques, and procedures developed for use fall under DHS guidelines and will be marked and handled as: "Protected Critical Infrastructure Information (PCII)". While CES-21 produced PCII research this document is a Public Document.

Table of Contents

Preface

The following report represents the culmination of a five-year Cybersecurity Research and Development (R&D) program performed by California's Investor-Owned Utilities (IOUs) and Lawrence Livermore National Laboratory (LLNL) and funded by the IOUs' electricity ratepayers as authorized by California Legislation and the California Public Utilities Commission (CPUC). The cybersecurity R&D, which was intensely technical in nature, was broken into three major workstreams:

1. The development of a modeling & simulation platform, to explore the potential effects of various threat and response scenarios at grid scale
2. The establishment of a physical testbed with separate substation instances from each of the IOUs, to evaluate threats and responses on actual substation equipment
3. The development of a research package consisting of several capabilities to support the industry's evolution towards automated threat response and other next-generation cybersecurity techniques

Throughout the program, there was extensive collaboration between the program team and national laboratories, federal departments, academic institutions and industry organizations. Several of the tools developed through the program have been made available to the open source community, to enable faster adoption and continued development of important cybersecurity capabilities. While this program began to develop much of the foundation for automated threat response, much work remains to be done, and this report recommends a series of next steps.

While the Executive Summary below has been simplified as much as possible, the very technical nature of the subject matter would make further reduction difficult without causing meaning to be lost. Due to the sensitive nature of the research, some topics are intentionally covered at a high level to protect the research and therefore the electric grid and customers of California and the Nation. For further detail, clarification or questions we suggest discussion with the program team.

1. Executive Summary

Pursuant to CPUC Decision (D.)12-12-031 on December 20, 2012, the California Energy Systems for the 21st Century (CES-21) program began in December of 2012. This original decision was for a program for $152 million that encompassed innovative research for both gas and electric systems. It was followed by Senate Bill (SB) 96 in 2013. This bill resulted in D. 14-03-029, a decision that had the ultimate effect of modifying the original decision D.12-12-031. Subsequently, D.14-03-029 on March 27, 2014 modified D.12-12-031 to comply with SB 96 (Chapter 356, Statutes of 2013). SB 96 and D.14-03-029 created the CES-21 Program with $35 million in funding to encompass innovative research and development. Program research was authorized to begin on October 9, 2014 with approval of the IOUs' advice letters by the CPUC. Per Decision 14-03-029, spending on the program could not begin until after the Cooperative Research and Development Agreement (CRADA) was developed and signed by all parties. The CRADA was signed by the IOUs and LLNL on December 29, 2014. Research and Development (R&D) began the next day and continued until October 8, 2019. Per D.14-03-029 (hereafter referred to as the Decision), the CES-21 final program report is due to the CPUC 60 days past the end of research on December 6, 2019.

CES-21 was comprised of two distinct projects: 1) Cybersecurity Research and Development and 2) Grid Integration. The Grid Integration project ran from 2014 through 2017. The Grid Integration project final report was submitted to the CPUC shortly after its conclusion and is included as an appendix in this document. The Cybersecurity R&D project ran the full five years of the CES-21 program and is the focus of this final report.

CES-21's cybersecurity research has been at the forefront of advancements in Machine-to-Machine Automated Threat Response (MMATR). Several components of this research have been transitioned to practice by the Joint IOUs. The operationalization of research has included Open Source software, automation and orchestration tools for security operations centers, and testbeds used to introduce machine-to-machine use cases into the cyber defense repertoire of the IOUs. CES-21 accomplished cutting-edge research in the areas of threat attack simulation, quantum key distribution (using quantum entangled photon industrial control system communication protection for Supervisory Control and Data Acquisition (SCADA) and control system networks) and integrated substation testbed environments.

Since the beginning of the program, the IOUs asserted that the goal to implement MMATR for the California grid system was not achievable with the CES-21 program's budget and five-year duration. However, the R&D conducted through the program, as shown later in this report, made advances towards protecting against threats and attacks anticipated five years ago. In addition, the analysis conducted over the last year of the program has brought stakeholders closer to improving the protection of California's electric grid by identifying and prioritizing gaps in MMATR research and other cybersecurity research objectives. With nation-states and other threat actors making ever-increasing and aggressive attacks on the United States' electric grid and industrial control systems, subsequent research is needed to combat the landscape of ever-present and changing threats.

CES-21 was a unique program in many ways. The program charted an unprecedented level of collaboration among the IOUs, national labs, and industry on cybersecurity research. The program also drew interest from federal departments because of its unique cybersecurity research objectives and agile research approach when Industrial Control System (ICS) cybersecurity and the MMATR concept were nascent. CES-21 has brought the eyes of the cybersecurity research world onto California in a very positive and actualized manner. CES-21 has been recognized for its research by the Department of Energy (DOE), Department of Homeland Security (DHS), National Security Agency (NSA), numerous national laboratories, academic institutions, industry organizations, and individual companies. Federal departments were especially interested in the research being done under CES-21, noting not only the significance of automated threat response specifically, but also the need to do more research in the area of electric grid cybersecurity. As an example of their interest, DOE and DHS both had

individuals on the CES-21 team's Independent Advisory Committee. DHS shared its ongoing cybersecurity research as well as its applicable experience in transitioning research to practice. The NSA and John Hopkins Applied Physics Laboratory collaborated on ICS Orchestration and Automation, which lead to SDG&E adopting a similar product into the security operations center.

a. Overview of CES-21 Program and Plan Highlights

The purpose of this final report is to provide a summary of CES-21's accomplishments, along with lessons learned and recommendations for future research that will help to advance cybersecurity and grid integration.

CES-21 was designed to research potential solutions for the medium- and far-term challenges of a fast-evolving energy marketplace. Below are descriptions of CES-21's two projects:

1. Cybersecurity Project

Comprised of a team of technical experts from the Joint Utilities, LLNL, other national laboratories, contractors, and industry partners, the Cybersecurity project pursued research in next-generation areas of Industrial Control Systems (ICS) cybersecurity. This research was divided into three major work streams:

- Developed a modeling/simulation platform to simulate threat-and-response scenarios. The simulation engine has enabled virtual testing of advanced remediation methods (the ability to detect real-time simulated cybersecurity attacks, report the activity, and suggest and implement an automated course of action) at scale to identify potential negative externalities. It also enabled destructive tests to be performed without endangering actual equipment. The simulation engine represents the merging of two types of modeling systems: network data systems and grid configuration power flow models. Each of these categories has well-developed examples, but they are not typically combined. Each development cycle was designed to build on the functionality of the previous cycle, with the end goal of being able to model a mid-sized grid environment and the data communications which control it.
- Established a physical testbed to evaluate threats on actual substation equipment. This allowed testing of vulnerabilities and potential advanced remediation methods using real-world equipment, but in a contained sandbox environment. This also allowed equipment response assumptions from the simulation platform to be cross-checked against real devices.
- Compiled an automated response research package to support the industry's evolution towards MMATR and other next-generation security techniques. The Indicator and Remediation Language (IRL) research has produced standardization of an indicator-encoding language that has been adopted by the European Union. In addition, combined research on secure Supervisory Control and Data Acquisition (SCADA) protocol, the way Industrial Control Systems communicate, and Quantum Key Distribution (QKD), the use of quantum physics to secure communication, has produced unique capabilities demonstrated for the first time with CES-21.

At the onset of CES-21, it was expected that the program's grid-related cybersecurity research would begin to build the foundation of a future MMATR system, but that additional capabilities would remain to be developed at CES-21's conclusion. Five years later, that forecast has proven true. CES-21 has conducted groundbreaking research that has provided new understanding of: 1) cyberattacks' impacts on the power grid at scale, 2) automated responses to previously known cyberattacks, and 3) the variety of tools that can help characterize, describe, and prioritize threats to ICS. This research has been recognized by DOE, NSA, DHS, several national laboratories, and the cybersecurity industry at large. In addition to informing and contributing to existing standards, it has pushed the boundaries of research in the power grid cybersecurity domain. CES-21 has identified the path forward for developing

the capability to integrate a MMATR system with the California grid, as well as additional knowledge and capability gaps in the grid cybersecurity domain that should be addressed in future research efforts. Finally, the program has identified a role that the State of California is uniquely positioned to play in efforts to secure our grid against cyber threats. This includes research for post-event analysis and event reconstruction, basic automation for real-time isolation, supply chain verification, advanced cross-domain data analytics, real-time automated response to unknown threats, optimized strategies for blackstart leveraging DERs, simulation modeling and physical testbed integration, and decentralization of resources and assets.

2. Grid Integration-Flexibility Metrics Project

The Grid Integration project was led by PG&E with support from San Diego Gas and Electric (SDG&E) and LLNL. This project (which concluded in 2017) worked to determine if the utilities' planning assumptions and reliability metrics were applicable under future conditions, given the Renewable Portfolio Standard (RPS) goals California has already adopted to increase renewable generation. To do this, PG&E (with support from SDG&E and LLNL) implemented the Grid Integration-Flexibility Metrics project, which modeled the grid under thousands of permutations of market demand, weather conditions, and infrastructure investment. This model simulated the impact of increased renewable penetration and market conditions based on accurate grid reliability and grid capacity metrics. The full final report for this project can be found in Appendix E, while the summary of high-level accomplishments is provided below.

Modeling:

- Completed modeling of the entire geographic area represented by the Western Electricity Coordinating Council (WECC) using the 2026 Transmission Expansion Planning Policy Committee (TEPPC) dataset.
- Simulated over 87,500 full years of system operations under various 50% RPS scenarios.
- Fully leveraged the LLNL High Performance Computing (HPC) platform developed in 2016 and the 1,000% gain in run-time efficiency needed to complete timely analysis.

Sharing Results with Public

- Presented key findings and recommendations from the project on August 15, 2017 at a CPUC workshop as a part of the Integrated Resource Planning (IRP) proceeding.
- Provided all stakeholders with opportunities to comment on these results.

Providing Access to Project Results

- Filed the CES-21 Grid Integration project final report in CPUC's IRP proceeding on September 12, 2017.
- Provided public access to the entire set of modeling input assumptions.

The results of the Grid Integration project are aligned with CPUC's newly-created IRP proceedings. Some of the concepts and analytical framework developed by the project are being incorporated by CPUC's modeling team in future IRP proceedings.

b. Program Accomplishments

At its completion, CES-21 has left a legacy of change, research, and tools that has far exceeded the team's expectations compared to its initial vision. Its numerous advancements in modeling, sharing of Open Source communications tools, hardware advancements, and both proposed and community-accepted protocols

and standards have notably advanced cybersecurity in the electrical industry. In addition to technical accomplishments, CES-21 fostered and achieved strong collaborations between California utilities, DOE national laboratories, and the State of California.

Cybersecurity Project

Specific accomplishments of the Cybersecurity project's major work streams are detailed below:

1. **Simulation Engine:** The team successfully built a coupled modeling and simulation capability for evaluating impacts of cyberattacks on the power grid. It has also completed five simulation development cycles of different attack scenarios on the California Grid with increased complexity, fidelity and scale in each simulation cycle. The simulation engine built through CES-21 represents the merging of two types of modeling systems: communication network systems and electric grid systems. This resulted in the coupled modeling and simulation environment. The five simulation cycles started with the localized/substation focused scenario and ramped up to conclude with modeling the impacts, effects, and mitigations of an attack on the California grid similar in nature to the one suffered by Ukraine in 2016. This was accomplished by leveraging the modeling and simulation engine developed through the four previous cycles—a capability that was only enabled by a deep understanding of how cyberattacks propagate through a network, affect physical processes in the system, and impact system-level functions. Additionally, the modeling and simulation capability developed by CES-21 enables the identification of indicators that a system has been compromised. These indicators can be used to detect ongoing attacks as well as test the effectiveness and safety of automated response.

2. **Physical Testbed:** Each IOU worked with Idaho National Laboratory (INL) and other vendors to develop a physical testbed environment representative of their respective substations. The equipment was carefully specified, procured, and shipped to INL where it was configured as a realistic representation of the individual IOUs' operational environments. The testbed consisted of four racks of PG&E equipment, three racks of SCE equipment, and one rack of SDG&E equipment. This setup shows how of each of the IOUs' substation industrial control and communication and cybersecurity interfaces could be used in real life. In 2019, Security Information and Event Management (SIEM) software system used by cybersecurity teams to aggregate and analyze security related events within the enterprise environment was installed. This enabled LLNL and the Joint Utilities to conduct real-time analysis of the test scenarios applied to the testbed. Existing Indicator and Remediation Language (IRL) packages, which convey threats and associated courses of action, were also exercised against the testbed. Having the IOUs' equipment located at INL allowed the research team to compare the vulnerabilities and capabilities of different hardware and software configurations. Because each of the three IOUs implements substation devices and cybersecurity controls differently from the others, the vulnerabilities to various exploits would vary by IOU. As a result, the team gained value and insight from having three separate substation instances. In 2019, an Energy Management System (EMS) software system was also installed. This connected to all three IOU testbeds through the centralized SIEM interface. This allowed for test scenarios that were managed and monitored across all three systems—as well as the ability to add integration scenarios to the testbed.

3. **Automated Response Research Package:** Research into advanced cyber areas was conducted across a range of topics that will be critical to automated threat response systems. These are:
   - *Indicator and Remediation Language (IRL)*: Developed and submitted enhancements to the Structured Threat Information eXpression (STIX), an industry-leading indicator encoding language. These enhancements were focused on threat detection for ICS-specific communication protocols DNP3 and ModBus. Distributed Network Protocol 3 (DNP3) and ModBus are sets of communication protocols used between components in process automation systems.

- *Advanced Threat Detection*: Completed planned use cases which demonstrated the ability to detect additional real-time simulated cybersecurity attacks to portions of the grid. These cases included the detection of attack activity through use of a Threat Monitoring Appliance (TMA). After detection, a TMA ran an automated Course of Action (COA) response to hinder or stop the cyberattack.
- *Exploits, Malware, and Vulnerabilities (EMV):* Developed a process for quantifying risks and creating the accompanying risk assignments, as well as an accompanying graphical EMV interface.
- *Industry Control System (ICS) Quantum Key Distribution (QKD)*: Developed and successfully demonstrated QKD in a controlled, non-production, point-to-point environment, and continued to reduce the footprint of the physical device to the point where it is now sized appropriately for installation in substation racks.
- *Secure SCADA Protocol for the 21st Century (SSP21)*: Developed a secure SCADA protocol and submitted SSP21 for the Institute of Electrical and Electronics Engineers (IEEE) standards body review. SSP21 has also been integrated in the QKD technology to create a secure protocol with integrated key distribution. The research envisioned an industrial key infrastructure (IKI), a specific ICS key infrastructure, that could replace Public Key Infrastructure (PKI) using QKD and SSP21.
- *Integration Component Architecture*: Developed a functional diagram representing the vision for the MMATR capability enumerating all inputs, outputs, functionality, and requirements for components and subcomponents of the MMATR capability. This includes data aggregation, threat detection, global analysis center, modeling/simulation, and orchestration and remediation. The functional diagram and sub-diagrams serve as a vision statement for MMATR capabilities. It also can be used to assess the current state of MMATR components and subcomponents—along with the next steps to take beyond CES-21.

4. **Program Governance and Foundational Collaboration:** SB 96 and Decision D.14-03-029 mandated that the program management team be comprised of one program manager (PM) from each IOU. In the first year of the program, the PMs developed a Program Governance Guideline document that spelled out the processes and rules the program's projects would follow. The PMs were instrumental in creating the structure for the research environment that the IOUs and LLNL would use to become a powerful and effective cybersecurity research team. The PMs implemented an agile lean startup research methodology (with rapid prototyping) to learn swiftly and fail fast if needed. The lessons learned from the program management team can be used by other Joint Utility programs as a resource in how to build efficient teams that can achieve research objectives despite being both multi-disciplinary and geographically dispersed. The program's administrative spend was kept below the 10% cap for the program as a whole, as required by SB96 and the Decision. The CES-21 team conducted regular outreach sessions with industry, federal agencies, and other key stakeholders throughout the program's duration to identify synergies and help ensure that research efforts were not being duplicated. Senior officials from DOE, DHS, California Independent System Operator (CAISO), and the State of California were briefed on grid security and CES-21 research objectives (as well as outcomes in some cases). Meetings with the Independent Advisory Committee were conducted throughout the program's performance period. At these engagements, the team collected knowledge and feedback from representatives and subject matter experts of federal and regulatory agencies, academia, and industry.

   In addition to collaboration noted in the beginning of the executive summary with DOE and DHS, the DOE, through Idaho National Laboratory (INL), funded research on Validation and Measuring for Automated Response (VMAR), which assisted CES-21 on the metrics needed to measure the impact of automated response. NSA, John Hopkins Applied Physics Laboratory, and CES-21 collaborated on research in automation and orchestration to identify the clues and events that make up a cyberattack and the responses to them in a step toward automating security operation center response to cyberattacks. Numerous California cybersecurity companies participated in CES-21

research. Lawrence Berkeley National Laboratory and associated University of California researchers became involved with what CES-21 was accomplishing with a professor from UC Davis sitting on CES-21's advisory committee.

Grid Integration – Flexibility Metrics Project

The Grid Integration project was successfully completed in 2017 and delivered on all its requirements. Through the use of modeling and simulation, this project worked to determine if the utilities' planning assumptions and reliability metrics were applicable under future conditions given the goals California has adopted to increase renewable generation. This required modeling the grid under thousands of permutations of market demand, weather conditions, and infrastructure investment to simulate the impact of increased renewable penetration and market conditions on the accuracy of reliability and capacity metrics.

c. Lessons Learned

The following are the key lessons learned over the five-year course of CES-21's Cybersecurity project:

- Overall, the interest in CES-21 from cybersecurity professionals working in IOUs, laboratories, industry partners, government agencies, and professional security organizations was strong throughout the program—and higher than initially expected.
- Over the five-year course of the program, cybersecurity threats have evolved considerably and have provided more realistic use case examples that are more applicable to industry. As a result, future efforts should allow for research to adapt as the program is ongoing.
- Automated cybersecurity is a concept that operators are still not comfortable with, so future efforts should assess and quantify risks associated with it, engage with relevant stakeholders as early as possible, and plan for staged integration and deployment of developed capabilities.
- Constructing a physical installation of all three IOU testbeds provided immeasurable value to CES-21 and provided insight on how to build capabilities that will not be IOU-specific, but more broadly applicable.
- MMATR remediation actions (actions taken to respond to and mitigate a cyberattack) do not always need to involve making changes to the system or its operation and can be simple additional data collection from the operators or alerts to the staff monitoring or operating the equipment.
- Vendor support of Structured Threat Information Expression (STIX™), a structured language for describing cyber threat information, is an area that will require future efforts. Utilities, the government, and non-government agencies should work with vendors to further encourage them to develop products which are ready for cybersecurity and electric operations interoperability.
- MMATR use cases, a defined set of scenarios for the application of MMATR, have more value when they mirror real-world challenges. Selected use cases within CES-21 specifically targeted challenges that utilities' Security Operations Center (SOC) teams often struggle with. This approach allowed for real-world input and feedback and helped SOC teams understand what MMATR functionality can provide in the future.
- QKD is a viable ICS communication system protection. The QKD system used for CES-21 research showed it is a proven unconditionally-secure method for sharing secret cryptographic keys over telecommunication networks.
- The Concept of Operations (CONOPS) document proved to be a useful exercise in identifying common problem areas among IOUs when extending cybersecurity operations to OT environments. These common challenges helped with identifying cybersecurity use cases for future MMATR research.
- There is a need for more Open Source innovation in the R&D cybersecurity space. This will create faster adoption of the research by industry. Using lessons learned from the DHS transition to the practice playbook, the CES-21 research team realized that the quickest way to get its software adopted in the industry was to place it in the Open Source domain.
- More federal funding needs to be leveraged for Cybersecurity R&D applied research. This is starting to happen and CES-21 has been a prime reason the DOE has put more R&D dollars into MMATR-type research.

There is a need for near-term Technology Demonstration & Deployment (TD&D) efforts to implement findings or inform future research. This would be modeled after other transition-to- practice efforts to bring research to field operations as quickly as possible. This would enhance the methodology used in CES-21 for agile lean startup, fail fast methodology to demonstration and deployment in one cycle.

d. Next Steps

The following research & development activities are recommended to occur for continued maturation of MMATR concepts initiated by CES-21. Additional detail on each can be found in the final pages of this document.

- **Vendor Engagement**: Follow-on research could include further MMATR technology development and demonstrations.
- **Concept of Operations**: Enhance the Concept of Operations (ConOps) document developed in CES-21 to detail both current IOU cybersecurity processes and potential future cybersecurity processes utilizing MMATR.
- **Follow-on Simulation Work**: Enhance the CES-21 focused simulation work on the California transmission system to evaluate effects to the bulk electric system undergoing cyberattacks. With a recommendation for extending the mod/sim work to represent the distribution network.
- **Continued Engagement with OASIS**: CES-21 partners will continue to engage OASIS to incorporate CES-21 IRL development work in future STIX and Trusted Automated Exchange of Intelligence Information (TAXII™) and Open Command and Control (OpenC2) iterations. TAXII is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. OpenC2 is a concise and extensible language to enable machine-to-machine communications for purposes of command and control of cyber defense components. OASIS a respected international non-profit standards body. The STIX, TAXII and OpenC2 are overseen by the OASIS standards body.
- **SCADA Resiliency Ecosystem**: Indicator and Remediation Language (IRL) use case development and testing should continue to reflect varieties of both adversary and defense techniques, tactics, and procedures.
- **Open Source Release of Tools**: Releasing software tools as Open Source is important to promote and extend future MMATR research and development work.
- **Quantum Key Distribution (QKD)**: Continued development, validation, and pilot testing is needed to encourage adoption and promote technology maturity of quantum key distribution capabilities.
- **Orchestration and Automation**: Continued work is needed to test for integration of security orchestration and automation concepts with electric utility Operational Technology (OT) environments.
- **Data Aggregation**: Additional research is required to continue refining data aggregation and correlation methods for SCADA systems.
- **SSP21**: Lab and field testing of Industrial Key Infrastructure (IKI) concepts, SSP21 specifications, and SSP21 reference implementation and integration with quantum protected networks should occur to further validate recommendations identified by CES-21.
- **Physical Testbed**: PG&E and SDG&E will leverage their testbeds for internal research and testing related to cybersecurity.
- **Integration**: Future work should extend the integration diagram from MMATR's current state by the end of CES-21 to reflect new concepts and understandings of MMATR operations.

e. Conclusion

CES-21 represents an example of successful collaboration among the Joint Utilities, participating national laboratories, and vendors with unique experience. Collaboration among these groups helped to create and deliver multiple research accomplishments which will help inform and shape the future of cybersecurity across the grid. However, a key lesson learned from CES-21 is that the cybersecurity landscape is rapidly evolving, exposing California and the United States grid to advanced threats, and making it more vulnerable than ever. Continued research to protect the California grid is an imperative to ensure a secure and resilient grid.

Engagement with the external stakeholder community continued throughout the program, and the team also coordinated with and received invaluable feedback from the Independent Advisory Committee and Steering Committee representatives. Engagement across the cybersecurity domain was positive, and the CES-21 team put an emphasis on the need to develop an automated response to cybersecurity attacks.

As the CES-21 team finished the work across the Cybersecurity project's task areas, each were ramped down and completed by October 8, 2019. During the course of work, many new and innovative ideas and concepts were realized in the research labs. True success stories included: 1) a large-scale simulation of the impact of a Ukraine-like cyberattack on a wide area of the California grid, 2) the first industrial control system laboratory test of an entangled photon quantum network in the SDG&E Integrated Test Facility and Cybersecurity laboratory, 3) orchestration and automation research going from laboratory-scale testing to being tested in the SDG&E operational security operations center, and 4) the development of seven different software research packages (four approved and three pending CPUC approval at the end of the program) for release to the Open Source community. Getting research out of the lab and into use by IOUs or the utility industry was a key milestone accomplishment for CES-21. Using lessons learned from the DHS transition to the practice playbook, the CES-21 research team realized that the quickest way to get its software adopted in the industry was to place it in the Open Source domain. The focus of the final months of the program was mainly on documenting research and the accomplished achievements, defining the full MMATR roadmap, and identifying the capabilities on that roadmap that will not have been addressed by CES-21 and should be conducted after CES-21's conclusion. Emphasis was also placed on further engaging with the vendor community to encourage their adoption of the capabilities developed through CES-21. Such adoption would provide great benefits for the broader utility cybersecurity community.

2. Introduction and Overview

The purpose of this final report is to provide a summary of CES- 21, which was comprised of two projects: Cybersecurity and Grid Integration, as required in Ordering Paragraph 21 of D.14-03-029. The primary focus of this report is the Cybersecurity project, as the Grid Integration project was finalized in 2017. The Grid Integration final report can be found in Appendix E.

a. Background on CES-21

CES-21 is a public-private collaborative R&D program administered between the Joint Utilities and LLNL. The projects utilized joint teams of technical experts from the Joint Utilities, LLNL, industry, academia, and other contractors as appropriate to meet the research objectives consistent with the approved CES-21 program. For more details on the Regulatory History around CES-21, please see *Appendix B - Program Regulatory History*.

b. CES-21 Program Components

Cybersecurity Project: Intended to research automated response and next-generation security capabilities that could more effectively protect critical infrastructure against cyberattacks. Due to the time criticality and increasing volume of cyberattacks, automated response capabilities and new ways of securing utility communications are an increasingly important strategic goal for ICS cybersecurity systems. The cybersecurity project concluded in 2019.

Grid Integration Project: Modeled future iterations of the grid to study the applicability of planning, flexibility, and reliability metrics (such as the 15% Planning Reserve Margin) under future grid conditions caused by increased renewable energy penetration and market demand. The Grid Integration project concluded in 2017.

c. Industry Trends Impacting Program and Projects

Since the program's initiation in 2014, the threat landscape of cyberattacks on industrial control and Operational Technology (OT) systems has gotten worse. As a result, funding and executing research efforts such as CES-21 are an imperative to ensure U.S. infrastructure security in the face of threats that are both ever-evolving and highly sophisticated. Several events are highlighted below that indicate an escalation in willingness and intent to develop and deploy attacks that disrupt infrastructure systems and can result in the loss of human life. These events impacted the public's perception of the need to protect critical infrastructure using cybersecurity measures. They also caused shifts in both political and industry domains. Below are brief descriptions of the main events that contributed to these shifts and list some of the resulting trends.

- In 2014, the security breach of Target Corporation's networks demonstrated how adversaries can pivot through these systems. By gaining access to Target's Heating, Ventilation, Air Conditioning (HVAC) vendor and using their credentials for remote monitoring of energy consumption and temperature, hackers managed to break into their point of sales systems and access cash registers. As a result, the criminals stole data from more than 40 million debit and credit cards (Radichel, 2019).
- In 2015, the first publicly known attack occurred on Ukraine's power grid. Russian adversaries used credentials to remotely log into the substations and trip relays, leaving 230,000 customers without power for six hours (Zetter, 2016).
- In 2016, another attack on Ukraine's power grid took place. Though it received less publicity, this attack was much more concerning than the 2015 event from a cybersecurity perspective. It involved sophisticated malware specifically designed to target ICS and speak native protocols commonly used in

power grids. While the version deployed in Ukraine would not apply in U.S. systems, the malware was written in a modular manner—indicating that additional functionality and protocols could easily be added.

- In 2017, TRITON malware (TRITON was the name given to the malware) was found in a Saudi Arabian petrochemical plant (Giles, 2019). TRITON (also known as TRISIS) was specifically written to attack an industrial safety system rather than an ICS. The system specifically targeted was Schneider Electric's Triconex Safety Instrumented System, a safety system designed to protect equipment, people, and infrastructure from unintended consequences. This malware uniquely targeted the Triconex system and was only discovered because of a programming error that caused an inadvertent (though safe) shutdown of the industrial process. Deeper evaluation of the TRITON code showed that the version discovered contained the ability to override safety systems but did not contain any active plan to implement an attack. This showed that an adversary changed its strategy from having an intent to destruct in real-time to pursuing methods that in the long term would be successful through persistence. Further investigation showed this was likely created by a nation-state to potentially secure a future tactical advantage. It is evident from the systems involved and sophistication of the approach that adversaries focused on control systems have both the system knowledge and funding required to remain undetected in environments without its operators being alerted to the presence of malware. This attack is specifically concerning and is considered a significant escalation, as the adversaries demonstrated (if not intended) at least willingness to cause the loss of life as a consequence of their actions.
- In April 2019, the first cyberattack on the U.S. power grid resulting in operational impact was reported. Utah power provider sPower lost visibility of its solar and wind generation. This was due to a vulnerability in their firewall that was repeatedly being rebooted by adversaries. As a result, communications were disabled between its control center and distributed generation (Cimpanu, 2019).
- In June 2019, news media reported that the U.S. and Russian governments were threatening to attack each other's civilian infrastructure. While it's unclear if either of the parties acted, the threats normalized the concept of nation-states using civilian infrastructure as a battlefield (even though no armies are present for defense).
- The complexity and intensity of cyberattacks in the ICS/OT space continued to ramp up with an increasing amount of public news about nation-state attacks. The U.S. DHS and Federal Bureau of Investigation issued joint Alert TA18-074A through DHS's United States Computer Emergency Readiness Team (US-CERT) organization in March 2018. This alert details tactics, techniques and procedures (TTPs) utilized by Russian state actors to conduct cyberattacks against critical infrastructure dating back at least to March 2016. Multiple media outlets picked up on this story. The story's high profile resulted in a national conversation about the importance of protecting critical infrastructure.

In February 2018, U.S. DOE Secretary Rick Perry created a new Office of Cybersecurity, Energy Security, and Emergency Response. Many pieces of this office previously existed elsewhere in DOE but were consolidated at the Assistant Secretary level to reinforce the importance of cybersecurity and resiliency for energy infrastructure. Over the course of the Program ICS and OT security have become increasingly important topics. The number of companies addressing this area of cybersecurity has increased dramatically, and both startups and existing security companies are entering the ICS/OT cybersecurity space. Given these recent cyberattacks on the electric industry and the increased frequency of these attacks, it is critical that ICS industries and government partners continue to increase their coordination and sharing of knowledge. The program team has noticed that in general the federal budgets for cybersecurity have increased along with the increase in cyber attacks. As such the federal government has been making significant investments in cybersecurity during the course of CES-21. The CES-21 team also notes that the State of California—as the nation's leader in high distributed energy resource (DER) penetration and renewable energy—faces unique

cybersecurity challenges which need specific cybersecurity R&D funding. Therefore, continued research efforts are essential in ensuring that our grid keeps up with the evolving threat landscape.

d. Coordination

Industry Coordination

Throughout the program, CES-21 team engaged industry, federal agencies, and national labs in collaboration on cybersecurity research topics. This assisted the Cybersecurity project on two fronts:

- Ensured research differentiation to avoid potential duplication of cybersecurity R&D, and added to the emerging state of the art
- Ensured knowledge sharing about cybersecurity research focused on machine-speed-learning

To aid this effort, the project conducted face-to-face and teleconference meetings between the CES-21 team and its Independent Advisory Committee (comprised of members from DOE, North American Electric Reliability Corporation [NERC], DHS, Electric Power Research Institute, Lawrence Berkeley National Laboratory, and the University of California – Davis).

The project team also participated in several other outreach venues. INL hosted the Energy Sector Coordination Council in June 2018, where over 80 energy sector industry executives were briefed on CES-21 as a leading example of progress in electric utility cybersecurity. INL also shared CES-21 activities at Grid V, a classified briefing supported by NERC and the Energy Information Sharing and Analysis Center. LLNL presented modeling and simulation results at the DistribuTECH conference in 2017 and 2018. In addition, LLNL also hosted California Governor Jerry Brown in February 2018 and participated in a CES-21 briefing. LLNL also briefed Karen Evans, Assistant Secretary for DOE's Office of Cybersecurity, Energy Security, and Emergency Response Office. Evans visited the lab in March 2019.

Internal Coordination

The CES-21 partner group (the Joint Utilities and LLNL) maintained a strong working relationship and regular cadence of meetings driven by the CES-21 Governance Guidelines, 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.
- Steering Committee meetings with IOU and LLNL leadership.

3. Budget (by Year, by Research Area)

Below is the combined actual spend across the two projects from the start of the Program through to the end of the CES-21 Program*.

a. Definitions

- Commitments and Encumbrances: Both contracted purchase orders and planned commitments.
- In-House Project Expenses: All project and administrative expenses not completed through vendor or partner subcontracts.

	Cybersecurity Project – Program Totals								
	2013	2014	2015	2016	2017	2018	2019	2020	Total
Commitments/Encumbrances	$123,334	$23,179	$4,775,506	$9,442,149	$7,480,918	$4,754,058	$1,847,617	-$16,519	$28,430,242
In-house project expenses	$0	$0	$610,584	$484,840	$734,633	$741,127	$305,770	$12,492	$2,889,446
Total	$123,334	$23,179	$5,386,090	$9,926,989	$8,215,551	$5,495,185	$2,153,387	-$4,027	$31,319,688

	Grid Integration project – Program Totals								
	2013	2014	2015	2016	2017	2018	2019	2020	Total
Commitments/Encumbrances	$0	$0	$517,587	$392,054	$225,397	$0	$0	$0	$1,135,038
In-house project expenses	$0	$0	$6,174	$20,369	$26,361	$0	$0	$0	$52,904
Total	$0	$0	$523,761	$412,423	$251,758	$0	$0	$0	$1,187,942

	CES 21 Program - Total								
	2013	2014	2015	2016	2017	2018	2019	2020	Total
Commitments/Encumbrances	$123,334	$23,179	$5,293,093	$9,834,203	$7,706,315	$4,754,058	$1,847,617	-$16,519	$29,565,280
In-house project expenses	$0	$0	$616,758	$505,209	$760,994	$741,127	$305,770	$12,492	$2,942,350
Total	$123,334	$23,179	$5,909,851	$10,339,412	$8,467,309	$5,495,185	$2,153,387	-$4,027	$32,507,630

*This table has been updated from the December 6, 2019 final report delivery to include refunds from the national laboratories. The 2020 column reflects those refunds and administrative charges to finalize the report. Also, at the conclusion of the program, SCE conducted an internal assessment which warranted timekeeping adjustments within the five-year financial numbers as earlier reported by SCE.

4. Project 1 – Cybersecurity

a. High-Level Summary

The Cybersecurity project aimed to further the research of advanced cybersecurity technology and tools that are not currently commercially available. The project focused on developing: 1) a research package to lay the foundation for automated threat response and 2) new ways of securing utility communications and specific platforms for the IOUs to test vulnerabilities and apply advanced remediation methods. This advancement in cybersecurity technology could help the Joint Utilities identify and act on advanced cyberthreats to SCADA and ICS before they impact California's critical infrastructure.

The project was divided into 10 tasks. Each represents a building block that may contribute to a future system or multiple technology paths. The end result of the Cybersecurity project was the advancement of research toward realizing a grid architecture that can detect threats and can make real-time decisions to increase the grid's survivability and resiliency.

Objective

Due to the time criticality of cyberattacks on ICS, an effective way to protect the power grid is through advanced detection and automated response capabilities. Automated response is a cybersecurity goal of growing importance. This is because attack vectors from a growing number of bad actors are becoming more sophisticated and frequent. With the goal of improving reliability and operational efficiencies, MMATR is expected to:

- Enrich and streamline the gathering of intelligence about threats
- Reduce the mean time to discovery, prevention, and recovery
- Increase grid resiliency
- Lower risk and increase security posture
- Prevent attackers from reusing attacks

The research portfolio of CES-21 drives this strategy by prioritizing technology that can identify threats and execute remediation actions, as well as offering new channels for evaluation. The project extended the research on advanced threat detection and automated response for application across all CES-21 California IOU participants. It has also informed private sector vendors who could commercialize the technology developed through CES-21 research and make it available to U.S. utilities.

Scope

There is significant and legitimate concern about taking humans out of the loop. These concerns include operator staff not being educated in how fast a cyber threat can reach across the grid, concerns about what effects an automated response can have on the grid, and what kind of review will be done by humans in the loop, to name a few. As such, the research project did not include as part of its scope the development of production-level systems, nor did it provide the research that laid a foundation for vendors and utilities to explore security automation more strategically.

Please refer to Advice Letter (AL) 2656-E/3115-E/4516-E (Section 3c) for a detailed description of project scope and see Appendix A for details on the scope of each task within CES-21.

Deliverables

To meet the Cybersecurity project's main objective of researching next-generation security capabilities to protect IOU critical infrastructure against cyberattacks, the project researched the following:

- **Simulation Engine**: The Modeling and Simulation (M&S) platform's purpose was to evaluate the resilience of California's transmission system against cyber threats. The M&S platform provided the following key capabilities:

– Ability to test various MMATR technologies and concepts developed in this program at scale to evaluate performance and uncover any unintended or negative externalities introduced by automation.

– Modeling and simulation of grid and network devices to safely evaluate failures in a virtual environment to determine system-level impacts of cyber threats when applied at scale.

– Assisting in cybersecurity planning exercises to inform strategic investment and design decisions.

– Matching of anomalous ICS behavior with the most probable cyber scenario cause(s) and associated set of recommended remediation actions.

- **Physical Testbed Package:** A physical testbed environment, including substation equipment to test for vulnerabilities and potential advanced mitigations, was implemented at INL using the National SCADA Testbed and Transmission and Distribution (T&D) test configurations. The reference control system architectures built within the Physical Testbed were used to test various research results offered by the Cybersecurity Project.
- **Automated Response Research Package:** The package's research objective was to provide new understanding of the logistical challenges, ICS priorities of automated threat response, and secure automated remediation of threats. This supported the ultimate goal of the CES-21 to respond at machine speed to electric grid ICS component threats but did not have the goal of developing production-level systems. The automated response research package provided a research foundation for vendors and utilities to explore security automation and orchestration more strategically. This package included research on:

– *Advanced Threat Detection* – The goal of advanced threat detection research was to leverage ICS data collected from devices to detect and identify sophisticated and previously unknown ICS cyberattacks. Advanced threat detection explored various methodologies using whitelisting, machine learning, and artificial intelligence to evaluate possible resilient advanced mitigation strategies for emerging ICS threats.

– *Indicator and Remediation Language (IRL)* – IRL is a core component of a MMATR capability and is used to describe machine-readable and actionable ICS IOC and remediation logic. STIX is the standardized language selected for the IRL research. CES-21 research findings have been submitted and accepted as extensions to the Organization for the Advancement of Structured Information Standards (OASIS) standards body that governs STIX. OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. These extensions will improve the ability of STIX to describe ICS indicators of compromise (IOCs) and remediation.

– *SCADA Ecosystem Resiliency* – Investigation and testing on physical testbeds unique to each IOU was crucial to providing an accurate assessment of MMATR technologies and concepts developed in the program. These efforts included the development of processes for threat and exploit prioritization, as well as a tool to simplify IRL generation. The machine-readable IRL research will enable more resilient control system devices through early detection of illicit behavior and machine-speed remediation via pre-programmed responses, so that the threats are mitigated before there is a negative impact to the system.

– *Secure Systems Interfaces* – This effort included research and investigation of next-generation security protocols and quantum cryptography (the use of quantum mechanics for cryptography

instead of mathematical algorithms) mechanisms to protect end-to-end communications between ICS devices. Technologies developed here include:

- *Quantum Key Distribution* – Future-proof key distribution technology for immediate detection of interception of cryptographic keys.
- *Secure SCADA Protocol for the 21st Century (SSP-21)* – Cryptographic wrapper for existing legacy ICS protocols to ensure integrity of observation data and control signals.

– *ICS Data* Aggregation – Researched aggregation technologies, methodologies, and mechanisms to collect and process data from multiple and disparate sources, along with substation data and threat intelligence. This effort analyzed test cases, test equipment, and test environments, as well as evaluated the effectiveness of data collection mechanisms.

Evaluation Metrics

The Cybersecurity project launched on October 9, 2014 (with authority to spend beginning on December 29, 2014), and was authorized to continue until October 8, 2019. The table below describes CES-21's requirements and deliverables as well as their status.

ID	Requirement/Deliverable	Status	Program Results
1	Semiannual progress update meetings held with CPUC ED or ED-named proxies	Achieved	The CES-21 team met with the CPUCs Energy Division (ED) for bi-annual updates each year. These updates focused on program progress, financial updates, and occasional demonstrations of technology developed during the program.
2	Monthly progress reports delivered to CPUC	Achieved	Each month, Program Managers from the IOUs and LLNL compiled a report detailing monthly progress, collaboration activities, upcoming tasks, and program financial data.
3	Maintain project financial governance in line with compliance requirements	Achieved	At program's inception, a cap of 10% administrative cost to the program was set. The admin cost at program completion was 9.1% of total spend.
4	Establish guidelines for program management, shared responsibilities, and classification of sensitive data	Achieved	The Traffic Light Protocol (TLP) was adopted for data classification for all information shared between partners, CPUC, and when released as public information.
5	Development of IOU-agnostic threat scenarios	Achieved	Over 25 threat scenarios were developed. As the program progressed, these scenarios were applied against the physical testbeds of each IOU, and the tests were refined to operate independently on any of the testbeds that were used.
6	Development of machine-readable language conventions to describe threats	Achieved	The development of IRL throughout CES-21 delivered machine-readable language and was released to the Open Source community. These language adoptions were formalized through additions and changes to the STIX protocol submitted through CES-21.
7	Ability to model and simulate threat scenarios	Achieved	LLNL developed PARGRID (a simulation package), which enabled modeling and re-creation of electric utility cyberattack scenarios. This culminated in an emulation of a Ukraine-like attack progressing through the California gird.
8	Ability to test models and scenarios using physical models of equipment configurations	Achieved	Through GridDyn, LLNL enhanced the ability to simulate events based on the physical reactions/interactions of actual utility equipment.

ID	Requirement/Deliverable	Status	Program Results
9	Document learnings and requirements for integration of CES-21-funded research, and ensure non-duplication of research effort	Achieved	By way of annual reports, public presentations, and research reports, knowledge gained by CES-21 has been documented and shared thoroughly. IOU and national laboratory members ensured a non-duplication of work through interactions with DOE and DHS and through updates to the CES-21 Independent Advisory Committee.

CES-21 Funds Spent

Please see Section B for all budget information.

Treatment of Intellectual Property

Treatment of Intellectual Property is described by the CRADA signed by the IOUs and LLNL. All IP rights retained through project development work are shared equally by the participant IOUs. As the project progressed, there were two types of IP that were produced: IP that is optimized by being protected and held direct value to the CRADA participants and the ratepayer, and IP that best created value by being shared with the wider security community through Open Source and other non-chargeable channels. The methodology CES-21 used to differentiate these categories is whether the research's commercial value is heavily dependent on adoption such that without widespread adoption the material would have little or no direct value to the IOUs or ratepayer.

On January 17, 2018, the joint utilities filed Advice Letter (AL) 3175-E / 3726-E / 5215-E (Joint AL) requesting the release of the four cybersecurity R&D applications to the Open Source community. These applications included IRL, GraphIRL [now renamed as Structured Threat Intelligence Graph (STIG)], GridDyn, and SSP-21. On September 27, 2018, CPUC approved the open sourcing of these applications in Resolution E-4943. These were approved by the CPUC.

On September 26, 2018, CPUC approved the open sourcing of these applications in Resolution E-4943. On September 26, 2019, a second Joint AL was filled for additional applications (4078-E / 3433-E / 5646-E) requesting the release of three cybersecurity R&D applications to the Open Source community. These applications included Exploits, Malware and Vulnerabilities (EMV) Scoring Application; Structured Threat Observable Tool Set (STOTS) and SimView. As of the date of this final report the ALs are still awaiting a CPUC decision.

Status Update

The momentum across the Cybersecurity project's task areas continued from the start of the program through to the end of research on October 8, 2019. The research teams were fully engaged across all the task areas, added numerous use cases to explore, and continued to update the path forward for possible integration of the component parts of the research.

The following table is provided to synopsize the Program in bulleted fashion for ease of consumption.

Program Governance and Foundational Collaboration

Throughout the duration of the program, the IOUs and LLNL Program Managers maintained consistent communication to facilitate collaboration and to identify and resolve governance issues. Below are a few of the activities that contributed to the financial and research goals of CES-21:

- Published guidance documentation on data sensitivity (referred to as Traffic Light Protocol) and handling relating to CES-21. The published procedures for managing the release of CES-21 program information to the public are being used routinely.
- Submitted monthly status reports to Energy Division and biannual check-in presentations.
- Coordination and collaboration continued with government agencies including DHS, DOE, and the National Security Agency.
- An Independent Advisory Committee was stood up and met once every six months to give input and direction to the Program.

Physical Testbed

- A physical testbed environment, including substation equipment to test for vulnerabilities and potential mitigations, was implemented at INL. SDG&E, SCE, and PG&E all implemented instances of substations representative of their existing equipment at INL for testing of real equipment, real-world validation of simulations, and the development of utility-equipment-specific IRL. The objective was to evaluate replications of IOU equipment in a physical testbed against new and cutting-edge exploits to verify responsiveness and effectiveness of MMATR solutions.
- The IOU testbeds at INL were built, tested, and instrumented for performance metrics. They were integrated via the System Information and Event Management (SIEM). Cyber products were integrated to enhance and enable automated response capabilities as well as standardized communications between IOUs. An Energy Management System (EMS) was integrated into the testbed architecture for threat sharing and basic SIEM integration. In addition, EMS added the element of command and control to the IRL package testing and analysis. It was instrumented to collect performance metrics for latency analysis and automated response.
- At the conclusion of CES-21, the physical testbeds from PG&E and SDG&E were returned to their owners for potential use in their own research labs. SCE has left their testbed at INL for continued testing.

Modeling Engine

- The team developed a coupled simulation capability that co-simulated network traffic and power flow of the power grid. This enabled analysis and understanding of the impacts of cyberattacks at scale. Additionally, this capability provided insights into indicators of compromise for various attack scenarios, as well as the effectiveness and safety of proposed MMATR remediation (actions taken to respond to and mitigate a cyberattack) actions.
- The simulation engine represented the merging of two types of modeling systems: communication network systems and electric grid systems. Each of these categories has well-developed examples, but they were not typically combined. Each development cycle was designed to build on the functionality of the previous cycles, with the end goal of being able to model a mid-sized grid environment and the data communications that control it.
- The CES-21 team successfully completed five simulation development cycles. The first cycle focused on modeling physical damage to a transformer from a cyberattack on the remote terminal unit controlling a transformer bank. The second cycle focused on denial of service attack exploiting a known vulnerability in a specific device. The third cycle focused on a malware attack that had the goal of creating islanding conditions, while the fourth cycle focused on using critical failure analysis to understand which relays would result in the most impactful attacks if manipulated by adversaries. Simulation 5 leveraged extensive modeling and simulation capabilities developed through the four previous cycles to model and analyze impacts of a Ukraine-like attack on California. The team also identified how this type of attack would be detected, as well as which mitigations are effective.

Research Package on Automated Response
(for use by wider utility community and private sector vendors)

- Advanced Threat Detection – Through hardware and virtualization configurations, the TMA demonstrated the ability to detect real-time simulated cybersecurity attacks, report the activity, and suggest and implement an automated response called a Course of Action (COA). The detection was limited to a set of predefined use cases. Those use cases were developed to be representative of known attack types. Similar work was completed for more complex use cases that included multi-step COAs through integrations with third-party commercial products.
- Indicator and Remediation Language (IRL) – In 2018 and 2019, more complex IRL packages were developed to demonstrate and represent known types of potential cybersecurity threats in a machine-readable language. The TMA was utilized to automatically generate IRL packages, detect the attack, and mount a response. In machine-readable language, these packages described the characteristics of the attack and the recommended response to the predefined attack scenario. Development of these packages advanced to levels beyond the basic IRL packages that were proven successful in prior project years.
- SCADA Ecosystem Resiliency – The Structured Threat Intelligence Graph (STIG) tool, previously known in the program as GraphIRL, was completed and released as Open Source software. This provided researchers and users with a method to visually inspect threat intelligence and see how threat information is connected. This method greatly increased an analyst's ability to comprehend threat information and will lead to making better associations between IOC and reduced decision time for an appropriate COA.
- Threat Attribute Scoring Model – The project created a separate tool for threat scoring called Exploit, Malware and Vulnerability (EMV) Scoring for operator-specific risk analysis. EMV is a data-driven application for quantifying the risk of an EMV to a configuration-specific system. Initial releases of an accompanying graphical interface for EMV gave this project incredible potential for replicable and accurate risk analysis specific to partner environments.
- Structured Threat Observable Tool Set (STOTS) – The project created a tool set that enables operators and analysts to surgically detect malicious activity on their system. This tool used Structured Threat Information eXpression (STIX) as a method for detection and monitoring. These tools can be used by cyber personnel with familiarity of command line scripting to find indicators of compromise on configuration specific systems
- On January 17, 2018, the Joint Utilities filed Advice Letter (AL) 3175-E/3726-E/5215-E (Joint AL) requesting the release of the four cybersecurity R&D applications: IRL, GraphIRL [now renamed as Structured Threat Intelligence Graph (STIG)], GridDyn, and SSP21 to the Open Source community. On September 26, 2018, CPUC approved the open sourcing of these applications in Resolution E-4943. On September 26, 2019, a second Joint AL was filled for additional applications (4078-E / 3433-E / 5646-E) requesting the release of three cybersecurity R&D applications to the Open Source community. These applications included Exploits, Malware and Vulnerabilities (EMV) Scoring Application; Structured Threat Observable Tool Set (STOTS) and SimView. As of the date of this final report the ALs are still awaiting a CPUC decision.

Research Package on Automated Response
(for use by wider utility community and private sector vendors)

- Quantum Key Distribution (QKD) – Research created the first entangled photon quantum key distribution system tested for utility ICSs. The research developed a future-proof key distribution technology for immediate detection of interception of cryptographic keys, reduced key and certificate maintenance and overhead. QKD was successfully demonstrated. The footprint of the physical device continues to shrink and is now sized appropriately for installation in substation racks.
- Secure SCADA Protocol for the 21st Century (SSP21) –SSP21 protocol was completed in 2017 and was submitted for IEEE standards body review in 2018. SSP21 has also been integrated in QKD technology to create a secure protocol with integrated key distribution. The combination of these two technologies represents a response to the most basic security concerns in ICS communications.

- ICS Data Aggregation – The competed physical testbed environments provided CES-21 partners with the ability to collect data from real-world environments. The foundation of this work can support further data aggregation and data integration opportunities post CES-21.

Modeling and Simulation

As part of the CES-21 program a co-simulation capability that coupled power flow modeling with a communication network that modeled the impact and behavior of cyberattacks at scale was developed. Through five case studies, the team developed a strong foundational framework that leveraged Open Source software and high-performance computing. This enabled operators to understand cyberattacks at the device level, local level, and system level at scale. This framework will provide simulation capabilities that can be used to study cyber threats to the power grid. It also will help inform the design of automated detection and remediation strategies for such threats. A brief overview of each of the five case studies is provided below.

Simulation 1: Remote terminal Unit (RTU) Attack, Malware Execution on Substation Equipment, Transformer Bank

The focus of the first simulation cycle was to develop a prototype simulation whose primary function is to demonstrate the ability to model grid, communication, control, and malware components, as well as illustrate the simulation study process.

The scenario involved an attack on transmission substation equipment. The main question this simulation aimed to answer is what kind of impact the RTU attack scenario would have on the transformer life and transmission system behavior in the case where the attack continued undetected and in the case the attack is eventually detected and mitigated.

Simulation results showed that over time, the periodic overload malware was causing degraded the transformer throughout its lifetime until the transformer failed, which resulted in significant maintenance and replacement costs, loss of operational confidence in the system, and a potentially significant system outage.

Simulation 2: Denial of Service Attack (DoS) on General Electric D20 RTUs in Transmission Substations

This simulation identified and evaluated a cyber risk to a widely deployed device in the transmission grid. The second simulation case included a model of the MMATR system and enabled the model behavior to be tested in the context of a specific cyberattack scenario.

The DoS Attack scenario demonstrated a cyberattack on a class of industrial control system devices with a known vulnerability. In all considered scenarios the outcome of the attacks is persistent and results in potentially long-lasting loss of communication with the devices, but with no observable system-level impacts. However, time to remediation with MMATR is reduced compared to the time spent sending field technicians to investigate.

Simulation 3: Synchronized Malware Attack on Selected Substations Results in Grid-level Impact

The primary goal of the third simulation was to demonstrate the potential for a cyberattack to result in grid-level impact. It demonstrated how the distributed, interconnected nature of an electric utility power grid may be exploited through a simultaneous cyberattack on substation breakers and relays. This results in a grid-level impact causing an island condition (electrical isolation between one or more sections of the grid). A set of grid-islanding attacks was simulated in order to demonstrate the ability of a cyberattack to create multiple islands at a variety of locations in the grid. This simulation demonstrates conditions required to cause islands in the grid at the substation failure level.

Simulation 4: Insider-Based Malicious Changes to Protection Relay Settings Resulting in Grid Instability

This iteration of the development process was completed in November 2017 and builds on the simulation capabilities developed for the first three simulation studies. The primary enhancement developed for this simulation study is an automated cyber-resilience analysis tool to discover how protection relay configuration settings could be manipulated to lead to certain undesirable consequences.

The cyber-resiliency framework developed for this study can help utilities understand which assets to secure first since there are too many assets to secure simultaneously. The focus of this study was specifically on an insider with the ability to manipulate protection-relay settings.

Simulation 5: Cyberattack on the California Electric Grid Based on 2016 Industroyer/Crashoverride Attack in Ukraine

This simulation study was the culmination of the modeling and simulation effort for CES-21. Completed in March 2019, this iteration of the development process synthesized and expanded upon the capabilities developed throughout the first four simulation studies to simulate a Ukraine 2016 Crashoverride (Lee, accessed 2019) type of large-scale cyber attack on the California electric grid—and explored the efficacy and impact of one possible automated response. The simulation demonstrated that this type of attack, if left undetected and unmitigated would cause large voltage oscillations in the system ultimately resulting either generators tripping or load shedding. This simulation study demonstrated the use of a MMATR system on a realistic attack assessed impacts of such attack on California grid and identified what information a MMATR like system could use to detect Crashoverride attack.

Impact: The co-simulation capability provided the means to investigate different scenarios, measure impact at scale, and advise on remediation strategies. Simulation scenarios like the ones developed through CES-21 can be used to quickly test new attack scenarios, MMATR placement strategies, and remediation actions. Similar to how simulation is used today in electric system design, planning, and operation, simulations developed in CES-21 may play a role in future electric cybersecurity system design, planning, and operational contexts.

Research Package

SCADA Ecosystem Resiliency

Investigation and testing on SCADA systems (was done through testing on the physical testbeds) unique to each IOU is crucial to an accurate assessment of MMATR concepts and technologies developed in the program. The effort also includes the development of processes for threat and exploit prioritization. Machine-readable IRL generation will enable more resilient control system devices through early detection of illicit behavior and machine-speed remediation via preprogrammed responses to mitigate exploits before there is an impact. To achieve this, processes and tools were developed for automatic recognition of ICS compromise and remediation in a control systems environment. The ICS devices were configured by IOUs so that IRL could be tested based on a threat scenario and more specific use cases. The resulting test and performance results were analyzed to determine if there is an appropriate indication of an exploit followed by a successful remediation action. They were also analyzed to demonstrate whether or not operations are adversely impacted by the exploit or use of IRL.

The testbed environment included some of the ICS components embedded in each of the participating IOU's substation architecture, as well as what any hardware or software is being explored for possible deployment in each IOU's individual lab. Having the equipment located at INL allowed for a comparison between the vulnerabilities and capabilities of different hardware and software configurations. Because each of the three IOUs implements substation devices and cybersecurity controls differently from each other, the vulnerabilities to various exploits varied by IOU. As a result, there was value and insight to be gained from having three separate substation instances. Consequently, the team was able to assess what was being considered for operational deployment.

Outcomes:

This work performed within CES-21 moved the state-of-the-art technology for MMATR by pioneering indicators from static data points and alarm-only courses of action to dynamic time series indicators that mimicked cyber-adversary behaviors and courses of actions including mitigation responses. A wide variety of IRLs were created for each configuration in the test environment. These IRLs were repeated with performance metrics collected and analyzed to ensure minimal impact to the OT environment.

To ensure value by integrating IT advanced data analytics investments in the IOU SOCs, INL included the cyber observables from OT detection and mitigation actions into the SIEM applications.

The team developed visual analysis applications ensuring ease of use and communications between the multi-discipline roles for cyber defenders. These included compliance staff, threat analysts, risk managers, and field technicians. In addition, Structured Threat Intelligence Graph (STIG) enabled visual STIX programming, which allowed for enriching threat information for context using the STIX structures. The Exploit, Malware and Vulnerability (EMV) scoring application provided a repeatable and evolving prioritization of the multitude of cyber issues IOUs need to address daily. Finally, the Structured Threat Observable Tool Set (STOTS) allows cyber defenders familiar with scripting to create just-in-time applicability tests and detection to share agnostically across cybersecurity products. Such products allow for shareable, actionable and implementable threat information.

Significant Program Deliverables:

The capabilities/tools developed under SCADA Ecosystem Resiliency are agnostic in their application and built for integration regardless of substation/testbed architecture. These include:

- STIG tool enables operators to share actionable threat information. The tool can be applied in the operational environment. It provides a threat analysis capability with easy-to-use visual programming. This facilitates the process of creating, editing, analyzing and querying Structured Threat Intelligence eXpression (STIX) with graph theoretic queries. STIG's ability to visualize relationships between threat characteristics, exploit indicators, and courses of action is unparalleled for analyzing threat intelligence.
- The EMV scoring application, which targets efforts to protect the most critical component in control system cybersecurity (that will also result in the largest potential impacts) has been difficult to qualify due to the nascent capabilities in this area, which is a target for additional research. The EMV Scoring Application takes a structured, flexible, and reproducible approach that allows for a consistent and prioritized qualification of EMVs. This allows asset owners to focus limited defensive resources on cyber issues of the highest priority.
- STOTS provides a platform-agnostic, open, and scalable toolset to help gain necessary insight and knowledge to stay ahead of the dangers targeting our critical infrastructure. In order to provide an effective defense for U.S. critical infrastructure systems, it is vital for operators to have situational awareness and details of activities taking place within a grid system.
- The source code for STIG, EMV Scoring Application, and STOTS was released so that other developers can improve these tools, which will ultimately help to better protect critical infrastructure systems.
- Analysis of Lockheed Martin Cyber Kill Chain® and MITRE ATT&CK™ framework for implementation into STIX, as well as a trade-off analysis conducted as part of the Expert Guided Machine-to-Machine Actions portion of the five MMATR Core Concepts. The purpose of this effort was to determine which kill chain to use, how to implement it in STIX, and how to conduct a trade-off analysis using the kill chain for MMATR while providing methods for enriching threat information. This results in a better understanding of indicators and threat information, which prepares it for executing remediation actions more efficiently.
- IRL STIX code bundles were tailored to test configurations. The results were provided to each IOU.

5. Lessons Learned

The following are the key lessons learned through CES-21's Cybersecurity project over the five-year course of the program:

- Overall, the interest in CES-21 from professionals within cybersecurity across IOUs, labs, industry partners, government agencies, and professional security organizations has been strong throughout the program—and higher than initially expected.
- Over the five-year course of the program, cybersecurity threats have evolved considerably and have provided more realistic use case examples that are more applicable to industry. In future efforts, it would be beneficial to ensure that some flexibility in tasks exist to allow the integration of new threat scenarios into the grid protection R&D.
- In general, while the interest in grid automated security remains high within IOUs, there is still a general discomfort with automating grid control, especially if the automation can affect power delivery. To address this, future research efforts should: 1) characterize and when possible quantify the effectiveness and risks associated with automated response; 2) engage with IOU security and grid operations to help them understand the tradeoffs in effectiveness and risks of automated threat response (which will help inform their decisions on whether to adopt automated threat response); and 3) develop a staged approach (in collaboration with IOU security and grid operations) integrating MMATR capabilities starting with a semi-automated response to build operators' confidence in these capabilities.
- MMATR should be developed incrementally and must contain information regarding the risks associated with the Course of Action (COA). During the project, the team encountered pushback from the operational teams from each IOU as to what level of automation they were initially comfortable accepting before a human decision point was reached. As MMATR is advanced in future programs, operational teams will need to be shown consecutive building blocks of automation capability, and safety will need to be shown at each level. Specifically, operators were interested in knowing what risks an automated action represented to their system.
- Constructing a physical installation of all three IOU testbeds provided immeasurable value to the CES-21. The testbeds allowed researchers an understanding of the process of gaining more insight and information through tests on the testbed, and then refining those processes through that metrics and knowledge gained. This included processes across multiple operational systems and vendors ensuring that results will be broadly applicable and utility and vendor agnostic. Additionally, this ability helped the team to identify, refine, and adjust test scenarios to make the tests applicable and relevant. This was important to learn from each test and modify the next tests accordingly. As a result, the base types and formats of information available were more accurate and led to better recommendations for information exchange through STIX.
- MMATR remediation actions (actions taken to respond to and mitigate a cyberattack) do not always need to involve making changes to the system or its operations. Some remediation steps can be as simple as asking for more information from the operators or sending alerts to staff monitoring or operating equipment. Remediation steps such as these that do not involve MMATR directly interacting with the system are particularly important given concerns from Operational Technologies (OT) operations about automated cyber response that has the ability to interact with the control system. A staged approach to automating those processes from more conservative remediations to fully automated cyber response in the OT network is a means for adoption and integration of MMATR within OT operations.
- Vendor support of STIX is an area that will require continuous future efforts. Some vendors claim support for STIX, but do not always adhere to the standard or support the latest versions of STIX. Utility partners should begin requiring vendors to support STIX versions 2.x and specifically support STIX 2.x patterning to further encourage the vendor community to develop products which are ready for cybersecurity and electric operations interoperability. Future work should include engagement with the STIX interoperability sub-committee within the OASIS CTI technical committee.

- MMATR use cases have more value when they mirror real-world challenges. Selected use cases within CES-21 specifically targeted challenges that utilities' Security Operations Center (SOC) teams often struggle with. This approach allowed for real-world input and feedback and helped SOC teams understand what MMATR functionality can provide in the future.
- QKD is a viable ICS communication system protection. The QKD system used for CES-21 research showed it is the only proven unconditionally-secure method for sharing secret cryptographic keys over telecommunication networks. QKD is based on fundamental physical laws that guarantee resilience against future cyberattacks by intelligence agencies possessing either quantum or classical computers.
- The Concept of Operations (CONOPS) document proved to be a useful tool in identifying common problem areas among IOUs when extending cybersecurity operations to OT environments. These common challenges helped with identifying cybersecurity use cases for future MMATR research.

6. Conclusion

a. Key Results for the Program

- Effective Collaboration between IOUs, national labs, and industry experts: CES-21 is an example of the power of cross-industry collaboration between IOUs, national labs, and industry security partners. Success has been realized in areas such as grid modeling (from cybersecurity and load perspectives), grid environment replication in the lab, interaction with standards bodies, advancements in security hardware, and interaction with the security community through event participation. These are a testament to the ability of a focused group's commitment and drive to advance grid security in California and across the nation.
- Applications, Toolsets, Standards, and Technology for the Grid Security Community: Throughout the development of CES-21, sponsors and interested parties were frequently reminded that the goal of the program was to advance research in grid security versus advancing technologies to a production-ready commercial state. Even with ongoing focus on pre-production, the group unexpectedly created a series of resulting technologies that will continue to support and shape the industrial security community long after CES-21 has been completed.
- Tangible advancements directly influenced by the CES-21 program include:
  - **SSP21:** This protocol is a direct result of industry's inability to develop a non-proprietary solution for securing communications in grid environments. The protocol as defined for CES-21 is now under consideration as an IEEE standard.
  - **Industrial Quantum Key Distribution Technology:** Support from CES-21 was instrumental in creating the first working prototypes for quantum key distribution designed for grid environments. This technology has been demonstrated as a part of CES-21 and is being moved toward commercialization by vendors.
  - **Grid Simulation Tools:** As part of CES-21 research, two simulation tools were created to progress the ability to simulate cyber grid equipment, load balancing simulations, and a visualization program to enhance results sharing. These two applications have been released Open Source as GridDyn and SimView.
  - **Communications and Security Information Processing Tools:** Research was accomplished on a suite of tools required for reading and writing grid-relevant security data. These tools were central to the development of MMATR and formed the backbone of real-time communications in hardware environments. These tools were released Open Source as IRL and STOTS. Two graphical tools focused on improving a grid security analyst's ability to interpret threat information were also released. The resulting two toolsets were released to the security community as Open Source as Graph Indicator Remediation Language (GraphIRL) and the EMV Scoring Application.

    World-Class Physical Testbeds: One of the major deliverables from CES-21 was to create a lab environment which contained physical representations of a production substation from each of the partner IOUs. Having a physical test environment would enable the CES-21 team to test MMATR technology against a representative environment rather than virtualized approximations. To date, this level of integration between different grid operators is not known to exist outside of the CES-21 lab. The initial lab configuration was completed in 2018 and extended to include an Energy Management System (EMS) and centralized logging in 2019. The expanded connectivity added by centralized EMS and logging allowed interconnection of the IOU information domains.
  - **World-Class Grid Simulations:** The grid simulation products that have been mentioned prior were developed and executed on LLNL's High Performance Computing (HPC) cluster. The availability of a world- class supercomputing infrastructure combined with the industry knowledge of CES-21 partners allowed the scenarios that were completed during the duration of CES-21 to be the most complete and accurate models depicting actual effects of cybersecurity events on energy distribution produced to date.
  - **Influencing Security Standards to Support Grid Security Requirements:** One of the challenges faced in grid cybersecurity is that no standards body supported information exchange protocols

that met the needs of grid or SCADA environments. CES-21 developed extensions to the existing STIX standard, and coordinated with the STIX governing body OASIS through the OASIS committee. This involvement directly led to the adoption of grid specific fields and support in the STIX v2.0 release.

b. Next Steps

The CES-21 program (in association with DOE) has shared details of program results with both DOE and DHS through collaboration and Advisory Committee interaction. These shared results are a broader set of research results than has currently been made publicly available. The DOE has started to make research dollars available for work related to MMATR-type activities. The following research & development activities are recommended to occur for continued maturation of MMATR concepts initiated by CES-21:

- **Broader Dissemination of Research:** A broader set of CES-21 research results should be made available (to DOE and the federal government) than has currently been made publicly available. CES-21 should establish an agreement with DOE and the federal government to facilitate this data dissemination/sharing and help identify specific areas where it makes sense for the federal government to conduct future research that builds upon CES-21's progress.
- **Vendor Engagement**: Promotion of STIX and MMATR adoption in utility vendor products should continue to be advanced further. Follow-on research could include further MMATR technology development and demonstrations which leverage existing and new vendor products tested within utility environments or labs.
- **Concept of Operations**: CES-21 developed a ConOps document detailing both current IOU cybersecurity processes and potential future cybersecurity processes utilizing MMATR. As MMATR research evolves over time, future ConOps work should reflect new developments in research and reflect how threat detections and response concepts and strategies carried out by MMATR impact utility cybersecurity and grid operations.
- **Follow-on Simulation Work**: CES-21 focused its simulation work on the California transmission system to evaluate effects to the bulk electric system undergoing cyberattacks. Future work could include models of distributed energy resources, distribution management systems, and demand response systems. Visualization work should continue to build prototypes which convey simulation results and allow for user interaction to configure grid, network, and adversary models to assess cybersecurity and grid impacts resulting from scenarios of interest to the utility.
- **Continued Engagement with OASIS**: CES-21 partners will continue to engage OASIS to incorporate CES-21 IRL development work in future STIX/TAXII and OpenC2 iterations. Likewise, future IRL work should promote future ICS-specific capabilities for machine-readable languages through standards groups, including OASIS for STIX, TAXII, and OpenC2.
- **SCADA Resiliency Ecosystem**: Indicator and Remediation Language (IRL) use case development and testing should continue to reflect varieties of both adversary and defense techniques, tactics, and procedures. Statistical analysis of how remediation actions impact the performance of SCADA systems should continue and address systems not studied under CES-21, such as distribution system and grid-edge devices (such as smart inverters, electric vehicle charging stations, and distributed energy resources).
- **Open Source Release of Tools**: Releasing software tools as Open Source is important to promote and extend future MMATR research and development work. Future work should consider development and the open-sourcing of research tools to promote continued research, product maturity, and product development of MMATR.
- **Quantum Key Distribution (QKD)**: Continued development, validation, and pilot testing is needed to encourage adoption and promote technology maturity of quantum key distribution capabilities. Continued work for QKD should include: 1) hardening, performance improvements, and validation testing of QKD systems within utility field environments (such as substations), 2) pilot testing with multiple utility partners and use cases, 3) security vulnerability testing of QKD, 4) QKD integration with

complex network architectures, and 5) standardization of QKD specifications within standards bodies such as IEEE.

- **Orchestration and Automation**: Continued work is needed to test for integration of security orchestration and automation concepts with electric utility OT environments. This work can include testing of on-demand automated threat assessment (ATA) agents within embedded OT systems. Additional research and technology development is also required for integration of communication and power system simulations to supplement threat analysis activities as part of security orchestration and remediation workflows.
- **Data Aggregation**: Additional research is required to continue refining data aggregation and correlation methods for SCADA systems. Follow-on work should include aggregation of configuration and state information from emerging grid technologies (such as grid edge applications inclusive of DER and behind-the-meter devices) for use as sources of indicators which would trigger actions by security orchestration and remediation. Additional testing of data aggregation use cases is required to advise future ConOps work. Best practices should be implemented in order to eliminate false positives in data that could result in MMATR responses that could adversely impact electric operations.
- **SSP21**: Lab and field testing of IKI concepts, SSP21 specifications, and SSP21 reference implementation should occur to further validate recommendations identified by CES-21. Continued research and testing of SSP21 use within utility production environments should occur to further advise implementation within vendor products and integration within utility operations.
- **Physical Testbed**: PG&E and SDG&E will leverage their testbeds for internal research and testing related to cybersecurity. SCE will continue forward with its testbed research that incorporates substation and EMS applications and leave its equipment at INL. Future testbeds for MMATR research & development work should include IRL and performance testing for distribution applications such as Distribution Management Systems, FLISR, and emerging grid technologies such as smart inverters, DER head-ends, and facility DER management (FDEMS).
- **Integration**: Future work should extend the integration diagram from MMATR's current state by the end of CES-21 to reflect new concepts and understandings of MMATR operations. Overall, MMATR research should refer to the identified research gaps that were not addressed in this program. It should follow recommendations and pursue research aimed at achieving higher technology readiness levels (TRL) for MMATR.
- **Research Directions Beyond MMATR:** As previously mentioned, CES-21 is focused on automated detection and remediation of previously identified threats. However, since the threat landscape has significantly evolved in the last five years, further research is needed. This shift has created a gap in grid cybersecurity research that specifically addresses highly sophisticated, nation- state type threats. While this is certainly a problem for the U.S., California is one of the few states that is leading the country in high DER penetration of the grid. Though the presence of DERs comes with unique challenges due to the increasing surface area at risk for cyberattacks, it also provides opportunities for advancements in cybersecurity. If deployed strategically, such a DER-heavy configuration can be used to increase the resilience and security of the overall grid. Broadly, the research addressing this gap could fall into following categories:
  - Behavior-based verification of firmware updates
  - Real-time threat detection and remediation of previously unknown threats
  - DER-enabled distributed control systems that can remove single points of failure
  - Cross-infrastructure dependencies analysis and information sharing
  - DER-enabled black start operations when communications are down or cannot be trusted

c. Program Conclusion

At its completion, CES-21 has left a legacy of change, research, and tools that has far exceeded the team's initial expectations. The numerous advancements in modeling, sharing of Open Source communications

tools, protocols and standards (both proposed and accepted by the community), and hardware advancements have notably and tangibly advanced cybersecurity in the electrical industry.

In 2014, CES-21 set out to take on some of the industrial control challenges that the electrical industry had been struggling with for decades. This included creating a secure industrial control system protocol (SSP21) that was not vendor proprietary, allowed for encryption with modest processor performance, and did not rely on public key infrastructure (PKI) to manage. It also included engaging with information security industry groups on supporting ICS and grid-specific data fields in information sharing protocols. These projects resulted in SSP21 and STIX v2.0 respectively. CES-21 taught both the IOUs and the national laboratory partners that engaging in the creation of standards and processes as users of the technology can be far more effective than waiting for industry to create solutions. This underscores the need to continue to influence security at this level going forward.

As CES-21 matured, work began on building models of the California electric grid. Parallel projects were completed that focused on grid services as well as on how modeling and metrics standards could be used in research—as well as to make utilities more informed about their own systems. The modeling efforts culminated with CES-21's final simulation that showed the effects of a Ukraine-like attack on the California grid, and how MMATR could reduce the impact of that event. The results of the simulations showed how an attack could affect our state infrastructure and which improvements in the MMATR systems should be prioritized in future work to increase their effectiveness.

CES-21 research also produced many hardware firsts in the electrical Transmission and Distribution field. With its industry partner, CES-21 demonstrated for the first time in research history a quantum key exchange hardware platform designed to function in a grid environment. This platform supported a key exchange over existing technology and the SSP21 protocol. The project partners also created the first physical lab of its kind representing substation equipment from California's three largest IOUs. These testbeds were used to test MMATR automation use cases. In its final configuration, the consolidated lab was integrated to share threat intelligence among all three systems, setting the stage for better collaboration of grid connectivity partners going forward.

Overall, CES-21 has been an extremely successful example of the powerful benefits of collaboration among IOUs, national laboratories, and industry expert partners. While credit should be given to the team participants throughout the five-year program and the bodies that supported them, credit should also be given to those who built the vision of collaborating with the State of California to help secure its grid infrastructure. Given CES-21's success, while significant progress has been made towards MMATR, follow-on work will be needed to mature and add to research for the utility sector, ICS marketplace, and the electric grid to make MMATR an operational entity to help protect the grid from cyberattack.

7. Endnotes

Cimpanu, Catalin. 2019. "Cyber-attack hits Utah wind and solar energy provider." ZDNet.

https://www.zdnet.com/article/cyber-attack-hits-utah-wind-and-solar-energy-provider/

Giles, Martin. 2019. "Triton is the world's most murderous malware, and it's spreading." *MIT Technology Review*. https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/

Lee, Robert M. Accessed 2019 (no date listed). "CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids." https://dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/

Radichel, Teri. 2019. *Case Study: Critical Controls that Could Have Prevented Target Breach*. SANS Intitute Reading Room. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

Zetter, Kim. 2016. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Appendix A: 2019 Yearly Report January to October 8, 2019

Here we highlight specific activities and accomplishments for the period of performance of January to October 2019 In lieu of a standalone annual report. We focus on the Cybersecurity project of the CES-21 program as Grid Integration was completed in 2017.

Summary

The Cybersecurity project aims to further the research of advanced cybersecurity technology and tools not currently commercially available. The project is focused on developing a research package to lay the foundations for automated threat response and new ways of securing utility communications and specific platforms for the IOUs to test vulnerabilities and remediations. This advancement in cybersecurity technology could help the Joint Utilities identify and act on advanced cyber-threats to SCADA and industrial control systems before they impact California's critical infrastructure.

Project Status Report

The status of annual accomplishments and deliverables is provided in the table below.

ID	Requirement / Deliverable	Program Results
1	Semiannual progress update meetings held with ED or ED-named proxies	Achieved
2	Monthly progress reports delivered to CPUC	Achieved
3	Maintain project financial governance in line with compliance requirements	Achieved
4	Establish guidelines for program management, shared responsibilities, and classification of sensitive data	Achieved
5	Development of IOU-agnostic threat scenarios	2019 – Achieved. Use Case repository includes 86 use cases developed and tested with 64 scenarios identified.
6	Development of machine-readable language conventions to describe threats	2019 – IRL was released Open Source and has been refined through the conclusion of the project.
7	Ability to model and simulate threat scenarios	The development for this success metric is primarily conducted at LLNL due to its industry-leading experience in complex modeling and simulation. 2019 – Achieved. LLNL built a final simulation on top of the original five scenarios which took MMATR hardware countermeasures into consideration. The simulation results recorded a significant drop in cyber-affected nodes as well as a significant increase in power stability.

ID	Requirement / Deliverable	Program Results
8	Ability to test models and scenarios using physical models of equipment configurations	The development for this success metric is primarily conducted at INL due to their experience hosting the Critical Infrastructure Test Range. 2019 – Achieved. In addition to all IOU labs being installed and connected, an EMS was also installed at INL and logging was completed across all three IOU substation labs.
9	Document learnings and requirements for integration of CES-21- funded research and ensure non-duplication of research effort	2019 – Achieved. Continued to coordinate with federal agencies, national labs, industry, and university representatives. This coordination included the first face-to-face meeting between the CES-21 team and its Advisory Committee at LLNL on March 14, 2018. Made further additions and updates to the MMATR Capability Vision Diagram.

The Cybersecurity project achieved significant research milestones across its major work streams including the areas of simulation, the physical testbed, tools and applications, and community outreach.

- **Simulation Engine:** Building in complexity on previous years' simulations, Cycle 5 focused on modeling and predicting the effects of a Ukraine-like attack on California T&D systems. The simulation revealed gaps and opportunities in existing processes for data gathering, and added the capability to simulate automated responses from complimentary projects in CES-21.
- **Physical Labs:** All three IOUs had substation instances at INL. The newfound ability to test interoperability between IOU systems as well as the ability to share this information between the utility providers in the future—will allow real-world validation of security test scenarios as well as open up further avenues for collaboration between IOUs at the hardware level. Testing of the substation testbed scenarios has given the IOUs insight into potential attacks and has allowed for quick turnaround of subsequent changes to attacks with an understanding of the outcomes.
- **Tools and Applications**: The project completed tools such as STIG for graphical analysis of intelligence, threat vulnerability scoring through EMV with basic visualization capabilities, and the generation of machine-readable attack information and recommended automated responses. As the development of production-capable tools was not an expected outcome or goal of the program, the practicality and utility of these applications created within CES-21 are a significant achievement.
- **Security and Utility Community Contributions**: The CPUC granted the Open Source release of four major program advancements, which supported and furthered the utility security community. There are four additional software applications currently under review by the CPUC for Open Source release.

Coordination

Industry Coordination

During the shortened schedule of 2019, the program continued to engage industry, federal agencies, and national labs in collaboration on cybersecurity research topics. This assisted the Cybersecurity project on two fronts:

- Research differentiation to avoid potential duplication of cybersecurity R&D, as well as advance to the emerging state of the art
- Knowledge sharing on machine-speed-learning-focused cybersecurity research

CES-21 participants were invited to speak at many industry events including (but not limited to): DistribuTECH 2019, SANS ICS Security Summit, and S4. CES-21 was also featured by the CES-21 team at the 2019 National Lab Day on the Hill program sponsored by the Department of Energy as well as at the Electricity Subsector Coordinating Council National Lab Roundtable. CES-21 was also presented at LLNL's

Industry Day that included 24 attendees from over 15 companies (comprised of utilities, vendors, and security consultants). In addition, the CES-21 team has produced an 8-minute video for public release that provides an excellent visual summary of the advancements made in CES-21.

Internal Coordination

In 2019, the CES-21 partner groups (Joint Utilities, LLNL, and research partners) have maintained a strong working relationship and convened regular meetings. Coordination activities include:

- 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.
  - Steering Committee meetings with IOU and LLNL leadership

Lessons Learned

Cybersecurity

Considering the large amount of physical test equipment involved in this program, the draw down time and effort required to meet program requirements has been larger than expected and should be expanded in any future programs.

- With the high level of interest from the IOUs, national labs, and partners—as well as the value of CES-21 results perceived from CPUC—planning for future research should begin earlier in the program to allow for better continuity in the research and preserve the established team.
- Modeling and simulation are powerful tools that can provide deep insights into effects and impacts of cyber attacks at scale. Having models and the right data are essential in taking these capabilities to their full potential. Network models are not as readily available as transmission power flow models and can be burdensome to develop. Automating this capability could enhance future modeling and simulation efforts.
- Proving the usefulness of automated response technologies in operational environments—where the latency of control commands is a concern—requires gathering performance data and using statistical analysis for relevancy of potential changes in performance of the control system. Lessons learned in the statistical analysis of performance data includes strict alignment of version controls, allowing for multiple test runs to generate enough data to eliminate anomalous observations, and defining acceptable performance limits as the basis for statistical analysis.
- The core of the automated response technologies for CES-21 is IRL code creation. Lessons learned from coding IRL bundles include more detailed and complex code capabilities supported with multiple indicators and courses of action and connections to traditional cybersecurity products such as Security Information and Event Management (SIEM) to leverage existing cyber work flows in operations.
- Documenting and mapping requirements and design through development aids in identifying the testing tasks. Designing for Open Source code release ensures use of correct tools during the development. Also, identifying potential secure code concerns earlier in the development process helps to eliminate the need for code revisions in later phases.

Key Results for the Year

In 2019, CES-21 began to wind down and finalize research areas and results documentation. A large focus was placed on making project results available for other researchers to continue through additional Open Source requests for software release and preforming final analysis on test results.

- **Simulation Engine:** In 2019, the results from Cycle 5's Ukraine-like attack were combined with use cases from MMATR COAs to see what the impact would be with an automated response system in place during the simulation run. In over 50% of the simulated power transmission points, the effects of the attack were reduced or negated, and stability of the power levels increased.
- **Physical Labs**: In 2019, an Energy Management System (EMS) was implemented at the CES-21 lab provided by SCE. All three of the IOU labs were interconnected, and logs were collected between the EMS and IOU substations. This represented a major milestone in connectivity between both disparate systems and multiple substations with different architectures. Many of the uses cases that were tested on individual labs were run again with the fully interconnected lab, which provided better insight to information requirements needed for each IOU.
- **Tools and Applications**: Final revisions and improvements to software projects were completed in 2019. All tools that are being recommended for Open Source release have undergone a security-focused code review.
- **Security and Utility Community Contributions**: As the program closes, CES-21 partners have requested an that three more pieces of software (created during the funding period) be released as Open Source. By releasing these tools to the security community, CES-21 hopes to help propel a forward momentum in grid security, as well as reduce rework in future research efforts.

  The following 2019 annual tables will need to have financials updated. The tables below are through November 2019 and will be updated with final financial data by March 31, 2020 with a revision of the final report to CPUC. The revision will only modify the financials to include refunds expected from the National Laboratories and December 2019 IOU expenditures.

The following table will be delivered in Excel Spreadsheet format with the delivered document for ease of reading and as requested in the annual report delivery.

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY
2019 ANNUAL REPORT
AUGUST 27, 2019

ATTACHMENT 1
PROJECT STATUS REPORT TO ACCOMPANY ANNUAL REPORT

Column	Information Reported by the Joint Utilities	Response
A	Investment Year	2019
B	Project Name	California Energy Systems for the 21st Century
C	Project Type	Grid Integration: Flexibility Metrics
D	A brief description of the project	The CES-21 Flexibility Metrics and Standards project studied and recommended alternative planning metrics and standards that explicitly consider operational flexibility needed to integrate increasing levels of renewable generation. The project also aims to supplement present and future Long Term Procurement Plan (LTPP) modeling studies with an alternative set of standards and an analytical framework. The CES-21 Flexibility Metrics and Standards project utilized a joint team of technical experts from industry, software vendors, Utilities and the Lawrence Livermore National Laboratory (LLNL).
E	Date of the Award	2-Oct-14
F	Funding Amount	$2,000,000
G	Funds Expended to date: Contract/Grant Amount	$1,135,038
H	Funds Expended to date: In house expenditures	$52,904
I	Funds Expended to date: Total Spend to date	$1,187,942
J	Description of why this project was selected above other	Grid Integration is a State of California priority since new operation flexibility metrics are needed for long-term resource planning in California. Improvement to methodology and existing models, or new models, are also needed to reduce the cost, and/or the uncertainty about the resource adequacy of planned resources, to integrate greater amounts of intermittent renewables.
K	Administrative and overhead costs to be incurred for each project (In-House)	$52,904
L	Intellectual Property	No intellectual property has been brought to date
M	Update year	Project ended in 2017
N	Update	The Grid Integration project was completed in 2017

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY
2019 ANNUAL REPORT
August 27, 2019

ATTACHMENT 1
PROJECT STATUS REPORT TO ACCOMPANY ANNUAL REPORT

Column	Information Reported by the Joint Utilities	Response
A	Investment Year	2019
B	Project Name	California Energy Systems for the 21st Century
C	Project Type	Cybersecurity Research and Development (R&D)
D	A brief description of the project	The CES-21 Machine to Machine Automated Threat Response (MMATR) project is a public-private collaboration R&D project between PG&E, SDC, SDG&E, Lawrence Livermore National Laboratory (LLNL) and other entities (industry, academia, etc.) dependent on the capabilities needed to meet the research objectives. The objective of the CES-21 MMATR project was to apply computationally-based and other problem solving resources to the emerging challenges of the 21st century electric system of California. The CES-21 Program utilized a joint team of technical experts as best fit the research objectives of the Joint Utilities, Industry, Academia, LLNL and other national laboratories that participated. The team combined data integration with advanced modeling, simulation, analytical tolls and agile R&D techniques to provide problem solving and planning necessary to achieve California's ambitious energy and environmental goals for the 21st century.
E	Date of the Award	2-Oct-14
F	Funding Amount	$33,000,000 (Program Overall)
G	Funds Expended to date: Contract/Grant Amount	$28,430,242
H	Funds Expended to date: In house expenditures	$2,889,446
I	Funds Expended to date: Total Spend to date	$31,319,688
J	Description of why this project was selected above other	Electric grid security is a national and State of California priority due to the risk and impact a cyber incident can have on the delivery of safe and reliable electric service to the residents of California.
K	Administrative and overhead costs to be incurred for each project (In-House)	$2,889,446
L	Intellectual Property	No patent filings and other IP protections have been pursued. Over the course of the CES-21 Program and Cybersecurity project six software products were approved by the CPUC for release to the open source community. By releasing these tools to the security community, CES-21 hopes to help propel a forward momentum in grid security, as well as reduce rework in further research efforts.
M	Update year	2019
N	Update	In 2019, CES-21 began to wind down and finalize research areas and resulted documentation of the R&D efforts. A large focus was placed on making project results available for other researchers to continue with additional open source requests for software releases and performing final analysis as approved by the CPUC.

Appendix B: Scope by Task of CES-21 Cybersecurity Project

Task	Scope
Task 1 - Use Case Generation	Ongoing development of cyber risk scenarios with a primary focus on the transmission grid. Cyber risk scenarios will be applicable to all California IOUs and will feature use cases which are employed by individual tasks for testing. Scenarios and use cases will be developed throughout the life of the project. The project will also develop a ConOps as a potential target for the MMATR Response end research solution.
Task 2 - Data Aggregation	Development of methods to collect ICS information (SCADA data, Substation and Network Device Configurations) and the standardization of formats for structuring CES-21 information.
Task 3 – M&S	Identifying and fulfilling the initial capability requirements for modeling and simulating grid and communication systems in support of other MMATR CES-21 chartered tasks. In 2016, this task completed its scope and is now closed.
Task 4 - Testbed	Evaluating replications of IOU equipment in a physical testbed against new and cutting-edge exploits to verify responsiveness and effectiveness of MMATR solutions.
Task 5 - Advanced Threat Detection	Developing methods for monitoring and detecting anomalies in SCADA communications, processing Machine-Readable Threat Intelligence, and translating this intelligence into threat scenarios.
Task 6 - Indicator and Remediation Language	Development and maturation of a machine-readable language conventions and standards to describe ICS threats and remediation. CES-21 selected STIX as the standard to be used. IRL is the term used within CES-21 to denote the machine-readable language.
Task 7 – Software/Device Vulnerability Assessment	De-scoped in 2015
Task 8 – SCADA Ecosystem Resiliency	Developing the processes required for automatic recognition of ICS compromise and remediation in a control systems environment. Conduct a vendor showcase to solicit their participation.
Task 9 - Grid Stability Framework	Evaluating detection and response strategies for a wide variety of viable attack scenarios affecting the California grid through the delivery of a modeling and simulation platform. The modeling platform will test impacts from scenarios and from MMATR solutions in ICS networks.
Task 10 - Secure System Interface Environment	Developing a SSP21 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.
Task 11 - Documentation and Integration	Provide guidelines and documentation to aid information handling across the project, facilitating integration between tasks, and ensuring non-duplication of R&D efforts.

Appendix C: Program Regulatory History

On July 18, 2011, the Joint Utilities filed Application 11-07-008, which requested authority to recover the costs for funding CES-21 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, CPUC 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 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.[5] As part of SB 96, the California legislature directed CPUC to require the Joint Utilities to prepare and submit a joint report by December 1, 2013.[6] In compliance with this legislative directive, the Joint Utility Report described:

1. Scope of all proposed research projects
2. How proposed projects may lead to technological advancement
3. How proposed projects may lead to potential breakthroughs in cybersecurity and grid integration
4. Expected timelines for concluding the projects[7][7]

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 CPUC oversight of CES-21
- Revises the CRADA guidelines and project criteria accordingly

On April 25, 2014, the Joint Utilities filed AL 4402-E, which sought CPUC authorization to implement CES-21 pursuant to D.12-12-031 and D.14-03-029. CPUC approved an 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 AL 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 CES-21's proposed research projects.

---

5 SB 96 added Section 740.5 to the Public Utilities Code (Pub. Util. Code)

6 Pub. Util. Code Section 740.5 (e)(1).

7 Submitted to the Commission on November 27, 2013.

CPUC 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.

By March 31 (for each year of the program), CPUC requires the Joint Utilities to submit an annual report that provides information on project operations (including projects funded, research results, efforts made to involve academics and other third parties, and intellectual property that results from the research). CPUC also requires the Joint Utilities to submit a report required by Pub. Util. 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.

On January 17, 2018, the Joint Utilities filed AL 3175-E / 3726-E / 5215-E (Joint AL) requesting the release of the four cybersecurity R&D applications to the Open Source community. These applications included IRL, GraphIRL (now renamed as STIG), GridDyn, and SSP21. On September 27, 2018, CPUC approved the open sourcing of these applications in Resolution E-4943.

On September 26, 2019, a second Joint AL was filled for additional applications (4078-E / 3433-E / 5646-E) requesting the release of three cybersecurity R&D applications to the open source community. These applications included Exploits, Malware and Vulnerabilities (EMV) Scoring Application; Structured Threat Observable Tool Set (STOTS) and SimView. As of the date of this final report the ALs are still awaiting a CPUC decision.

SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

Gary A. Stern, Ph.D.
Managing Director, State Regulatory Operations

September 26, 2019

ADVICE LETTER 4078-E
(Southern California Edison Company - U 338-E)

ADVICE LETTER 3433-E
(San Diego Gas & Electric Company – U 902-E)

ADVICE LETTER 5646-E
(Pacific Gas and Electric Company - U 39-E)

PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA
COMMUNICATIONS DIVISION

SUBJECT: Request of Joint Investor-Owned Utilities for Approval of the Public Release of License Rights to Intellectual Property to Open Source Pursuant to Public Utilities Code Section 851 and General Order 173

PURPOSE

Pursuant to Section 851 of the California Public Utilities Code and General Order (GO) 173, Southern California Edison Company (SCE), on behalf of SCE, Pacific Gas and Electric Company (PG&E), and San Diego Gas & Electric Company (SDG&E) (collectively, the IOUs), respectfully request authority to release the following cybersecurity research and development (R&D) applications described in *4b* below to the open-source community under the terms and conditions specified in the License Agreement designated as the Berkeley Software Distribution Three Clause (BSD3)
License Agreement. A true and correct copy of the License Agreement is attached as Attachment A. Although the open-source license agreement of pre-commercial information and tools is a standard process for incenting the development of commercially beneficial cybersecurity applications as intended by the business case for the Machine to Machine Automated Threat Response (MMATR) project approved by the Commission in Advice Letter (AL) 4516-E, the IOUs are requesting approval out of an abundance of caution under Section 851 pursuant to the intellectual property requirements of Decision (D.)12-12-031 approving the 21st Century Energy Systems (CES-21) program.[1]

The IOUs believe that making these R&D applications more broadly available will have a positive impact in mitigating cybersecurity threats to the electricity grid. This request is

[1] D.12-12-031, p. 73.

consistent with the release of CES-21 intellectual property approved in CPUC Resolution E-4943 on October 17. 2018.[4] For these reasons, the IOUs respectfully urge the Commission to approve this advice letter without delay.

BACKGROUND

The IOUs, as part of the CES-21 Program, have acquired and now possess certain intellectual property they believe, if further developed, could result in products that will enhance the ability of California and nationwide utilities to protect Critical Infrastructure. The CES-21 Program, through on-going and collaborative cybersecurity research and development efforts, has developed three new applications that the IOUs and Lawrence Livermore National Laboratory (LLNL) believe can be developed into practical, commercial applications once released to the open-source community.

Pursuant to Resolution E-4943, the Commission agreed that it is desirable for those who are interested in developing the results of the CES-21 research into practical, commercial applications to be given an opportunity to do so with minimum restrictions or impediments. Although these entities would be required to sign an open-source license agreement, they would not be required to pay a license fee and the terms and conditions for the Open Source license would be "user friendly" since the selected terms and conditions are already familiar to the Open Source community. Although other models (such as selecting a single entity that would pay the IOUs and LLNL for the right to develop applications that use the results of the CES-21 effort) may result in some near-term revenues to the IOUs' customers, the amount of any revenues is likely to be insignificant when compared to the benefits that would result from accelerating the development of tools that would help the IOUs in addressing cybersecurity threats.

Competition among multiple entities (some of which may not be known to the IOUs and LLNL) using the open-source model should encourage the development of multiple products and applications sooner than other more restrictive licensing models (such as a single-source license) would provide.

The three specific applications that the IOUs and LLNL would like to offer to the industry on an open-source basis are described below (see *4b* for further detail on the applications):

1. Exploits, Malware and Vulnerabilities (EMV) Scoring Application enables a repeatable EMV prioritization scoring process that allows a focus on cyber defense operations for the most impactful issues while managing the analysis of other cyber concerns to be addressed during regularly scheduled maintenance.

2. Structured Threat Observable Tool Set (STOTS) enables users to capture and send Structured Threat Information eXpression (STIX) observed data objects for remediation regarding changes in industrial control system configurations, network architecture, and Syslog entries.

[4] Jointly submitted: SDG&E Advice Letter 3175-E; SCE Advice Letter 3726-E; PG&E Advice Letter 5215-E.

3. SimView is a web-based visualization tool for graphically exploring data from cyber-physical simulations.

The targeted licensee(s) for these three open-source products would be unique to each product. In other words, each of these products will be available under separate Open Source licensing agreements.

I. Releasing this research as Open Source to be adopted by industry vendors will not create any residual risk to the IOUs and their customers and will increase the security posture of Utilities Energy Delivery Systems improving reliability, resiliency and safety.

II. Open Source products reduce the cost to industry vendors. The increased reliability, resiliency and safety of the Utilities Energy Delivery Systems will be a significant value given the improved customer service.

COMPLIANCE WITH GENERAL ORDER 173

Rule 3 Requirements

SCE is permitted to submit this advice letter seeking CPUC approval under Section 851 because the company believes it has satisfied the eligibility requirements set forth in Rule 3 of GO 173:

3a: The activity proposed in the transaction will not require environmental review by the CPUC as a Lead Agency under California Environmental Quality ACT (CEQA).

The transaction is not a "project" for the purposes of the California Environmental Quality Act (CEQA). There is no work that requires CEQA review because the transaction involves only a licensing of intellectual property on an open-source basis and no direct or indirect environmental impacts will occur as a result of the transaction.

3b: The transaction will not have an adverse effect on the public interest or on the ability of the utility to provide safe and reliable service to customers at reasonable rates.

This transaction is in the public interest and will not diminish the ability of the utility to provide safe and reliable service to customers at reasonable rates.

In fact, the IOUs expect that the open-source licenses will result in the vendor community's development and commercialization of new cybersecurity solutions, that IOUs and other utilities can deploy, thereby increasing the security posture of Utilities Energy Delivery Systems improving reliability, resiliency and safety.

This advice letter will not increase any other rate or charge, cause the withdrawal of service, or conflict with any rate schedule or rule.

3c: Any financial proceeds from the transaction will either be booked to a memorandum account for distribution between shareholders and ratepayers during the next general rate case or be immediately divided between shareholders and ratepayers based on a specific distribution formula previously approved by the Commission for that utility.

No financial proceeds are expected.

3d: If the transaction results in a fee interest transfer of real property, the property does not have a fair market value in excess of $5 million.

Not applicable because no real property is at issue.

3e: If the transaction results in a sale of a building, the building does not have a fair market value in excess of $5 million.

Not applicable because no sale of a building is at issue.

3f: If the transaction is for the sale of depreciable assets, the assets do not have a fair market value in excess of $5 million.

Not applicable because no sale of an asset is at issue.

3g: If the transaction is a lease or a lease-equivalent, the total net present value of the lease payments, including any purchase option, does not have a fair market value in excess of $5 million, and the term of the lease will not exceed 25 years.

Not applicable because no lease or lease-equivalent is at issue.

The applications likely have minimal market value pending further development by third parties for commercial use.

The total net present value of the applications is below the $5 million limit for eligibility in GO 173.

3h: If the transaction conveys an easement, right-of-way, or other less than fee interest in real property, the fair market value of the easement, right-of-way, or other interest in the property does not exceed $5 million.

Not applicable because no transfer of an interest in real property is at issue.

3i: The transaction will not materially impact the ratebase of the utility.

The transaction will have no impact on ratebase.

3j: If the transaction is a transfer or change in ownership of facilities currently used in regulated utility operations, the transaction will not result in a significant physical or operational change in the facility.

Not applicable because no transfer or change in ownership of facilities is at issue.

3k: The transaction does not warrant a more comprehensive review that would be provided through a formal Section 851 application.

This transaction is typical of transactions for which the Section 851 Pilot Program was developed. This transaction does not contain any issues that would trigger a need for a more comprehensive review via a formal Section 851 application.

Rule 4 Requirements

Rule 4 requires that the following information be included in advice letters submitted under GO 173:

4a: Identity and addresses of all parties to the proposed transaction.

San Diego Gas & Electric Company, Seller
8330 Century Park Court MS 42C
San Diego, CA 92123

Southern California Edison Company, Seller 2244
Walnut Grove Ave.
Rosemead, CA 91770

Pacific Gas and Electric Company, Seller 77 Beale
St.
San Francisco, CA 94105

Open Source Community, Licensee(s)

4b: A complete description of the property, including its present location, condition, and use.

Intellectual Property

1. Exploits, Malware and Vulnerabilities (EMV) Scoring Application fills the gaps of other vulnerability scoring methods by including exploits, malware, applicability, consequence and guidance that feeds into actionable indicators and courses of action. It incorporates the asset owner's view for applicability, consequences and how to apply the guidance for defense of
their systems. Storing the analysis results enables learning and refinement with use, resulting in faster future analyses. Analysis sections can be tailored to the utility's needs and capabilities, with the stored results enabling reevaluation as the adversary's or defender's capabilities evolve. The EMV Scoring Application provides a repeatable process that adds context, identifies the most critical cyber issues for judicial use of limited cyber security resources, can be tailored with data driven design, and is moving toward the value of graph theoretics to match today's dynamic environment of multiple threat methods.

2. Structured Threat Observable Tool Set (STOTS) provides users modular, customizable and platform agnostic tools to monitor selected aspects of their network environment. STOTS enables users to generate and transmit Structured Threat Information eXpression (STIX) observed data objects for notification and or remediation. The STIX objects are capable of transmitting details regarding

devices added to or removed from a network, changes made to a device configuration within the network, as well as filtered Syslog entries from existing equipment. The flexibility and standardized format of the STIX objects will allow for enhanced abilities to share data amongst utilities and ultimately provide better protection for critical infrastructure regarding illicit changes in industrial control system configuration and network architecture.

3. SimView provides a visual method for exploring results from simulations. It aids in analysis of numerical results and provide insights not possible when examining large amounts of textual data. SimView provides the ability to simultaneously visualize data from multiple simulations (e.g. communications simulation and transmission power flow simulation). Additionally, the simulation playback can be paused, fast forwarded, and rewound.

Each of these products will be available under separate Berkeley Software Distribution (BSD) three clause (BSD3) Open Source licensing agreements.

4c: Transferee's intended use of the property.

Since there are likely to be multiple entities that will have rights to use the intellectual property, the individual uses of the intellectual property may vary among these entities. But it is likely that any Licensee would try to incorporate the Joint IOU intellectual property into Licensee's technology already being developed and then use the result to develop and commercialize cybersecurity products that can protect the grid. For clarity, the model proposed by the IOUs and LLNL is a license model, so ownership of the IP would remain with the original owner of this intellectual property.

4d: A complete description of the financial terms of the proposed transaction.

The BSD3 Open Source license agreement with no financial terms is attached.

4e: A description of how the financial proceeds of the transaction will be distributed.

No financial proceeds are expected.

4f: A statement of the impact of the transaction on ratebase and any effect on the ability of the utility to serve customers and the public.

The transaction will have no impact on ratebase.

This transaction is in the public interest and will not diminish the ability of the utility to serve customers and the public.

If the transaction results in the development and availability of new cybersecurity solutions, the IOUs and other utilities will increase the security posture of Utilities Energy Delivery Systems improving reliability, resiliency and safety.

4g: *For sales of real property and depreciable assets, the original cost, present book value, and present fair market value, and a detailed description of how the fair market value was determined (e.g., appraisal).*

Not applicable because no sale is at issue.

4h: *For leases of real property, the fair market rental value, a detailed description of how the fair market rental value was determined, and any additional information necessary to show compliance with Rule 3(g).*

Not applicable because no real property is at issue.

4i: *For easements or rights-of-way, the fair market value of the easement or right-ofway and a detailed description of how the fair market value was determined.*

Not applicable because no easements or rights-of-way are at issue.

4j: *A complete description of any recent past (within the prior two years) or anticipated future transactions that may appear to be related to the present transaction, such as sales or leases of real property that are located near the property at issue or that are being transferred to the same transferee; or for depreciable assets, sales of similar assets or sales to the same transferee.*
There is one example in the prior two years of a transaction related to the present transaction. On January 17, 2018 SDG&E submitted Advice Letter 3175-E.[5] This was a Joint Advice Letter on behalf of the Joint Utilities for four applications that the IOUs and LLNL wanted to offer to the industry on an Open Source basis. On September 27, 2018 in Resolution E-4943, the Commission approved the Joint Advice Letter.

CES-21 will sunset in October 2019 and no future related transactions are anticipated other than the expectation that the IOUs will be able to deploy the vendor-developed products and services.

4k: *Sufficient information and documentation (including environmental documentation) to show that all of the eligibility criteria stated in Rule 3 have been met.*

As presented in the discussion on Rule 3, SCE believes that all applicable eligibility criteria stated in Rule 3 have been satisfied.

4l: *The filing utility may submit additional information to assist in the review of the advice letter, including recent photographs, scaled maps, drawings, etc.*

x Berkeley Software Distribution-3 (BSD-3) Open Source License Agreement

4m: *Environmental Information: If the applicant believes that the transaction is not a project under CEQA, the applicant shall include an explanation of its position.*
Please see SCE's response to Rule 3a above.

[5] Jointly submitted: SDG&E Advice Letter 3175-E; SCE Advice Letter 3726-E; PG&E Advice Letter 5215-E.

TIER DESIGNATION

Pursuant to Section 851, GO 96-B, and GO 173, this advice letter is submitted with a Tier 3 designation.

EFFECTIVE DATE

This advice letter shall become effective when approved by the Director of the Energy Division, the Executive Director, or the Commission.

NOTICE

Anyone wishing to protest this advice letter may do so by letter via U.S. Mail, facsimile, or electronically, any of which must be received no later than 20 days after the date of this advice letter. Protests should be submitted to:

CPUC, Energy Division
Attention: Tariff Unit
505 Van Ness Avenue
San Francisco, California 94102
E-mail: EDTariffUnit@cpuc.ca.gov

Copies of the protest should also be sent via e-mail to the attention of the Energy Division at EDTariffUnit@cpuc.ca.gov. A copy of the protest should also be sent via email to the address shown below on the same date it is mailed or delivered to the Commission.

Gary A. Stern, Ph.D.
Managing Director, State Regulatory Operations
Southern California Edison Company
8631 Rush Street
Rosemead, CA 91770
Telephone (626) 302-9645
Facsimile: (626) 302-6396
E-mail: AdviceTariffManager@sce.com

Laura Genao
Managing Director, State Regulatory Affairs c/o
Karyn Gansecki
Southern California Edison Company
601 Van Ness Avenue, Suite 2030
San Francisco, California 94102
Facsimile: (415) 929-5544
E-mail: Karyn.Gansecki@sce.com

Attn: Megan Caulson
Regulatory Tariff Manager
8330 Century Park Ct. – CP31D
San Diego, CA 92123-1550
E-mail: MCaulson@sdge.com

Erik Jacobson
Director, Regulatory Relations c/o
Megan Lawson
Pacific Gas and Electric Company
77 Beale Street, Mail Code B13U
P.O. Box 770000
San Francisco, California 94177
Facsimile: (415) 973-3582
E-mail: PGETariffs@pge.com

There are no restrictions on who may submit a protest, but the protest shall set forth specifically the grounds upon which it is based and must be received by the deadline shown above.
In accordance with General Rule 4 of GO 96-B, SCE is serving copies of this advice letter to the interested parties shown on the attached GO 96-B list and, in accordance with Resolution ALJ-244, on the Energy Division, the Commission Public Advocates Office, the Commission CEQA Team (clu@cpuc.ca.gov; jnr@cpuc.ca.gov; jmu@cpuc.ca.gov). Address change requests to the GO 96-B service list should be directed by electronic mail to AdviceTariffManager@sce.com or at (626) 302-4039. For changes to all other service lists, please contact the Commission's Process Office at (415) 703-2021 or by electronic mail at Process_Office@cpuc.ca.gov.

Further, in accordance with Public Utilities Code Section 491, notice to the public is hereby given by submitting and keeping the advice letter at SCE's corporate headquarters. To view other SCE advice letters submitted with the Commission, log on to SCE's web site at https://www.sce.com/wps/portal/home/regulatory/advice-letters.

For questions, please contact Owen K. Goldstrom at 714-895-0230 or by electronic mail: Owen.Goldstrom@sce.com.

Southern California Edison Company

/s/ Gary A. Stern, Ph.D. Gary A. Stern, Ph.D.

GS:jh:jm
Enclosure

Attachment A

SCE Advice Letter 4078-E

SDG&E Advice Letter 3433-E

PG&E Advice Letter 5646-E
Berkley Software Distribution-3 (BSD-3)
Open Source License Agreement

Exhibit A

Agreement

Berkeley Software Distribution-3 (BSD-3) Open Source License Agreement

September 29, 2017

Berkeley Software Distribution Three Clause (BSD-3) Agreement

California Public Utilities Commission

ADVICE LETTER SUMMARY

ENERGY UTILITY

MUST BE COMPLETED BY UTILITY (Attach additional pages as needed)

Company name/CPUC Utility No.: Southern California Edison Company (U 338-E)

Utility type:
☑ ELC ☐ GAS ☐ WATER
☐ PLC ☐ HEAT

Contact Person: Darrah Morgan
Phone #: (626) 302-2086
E-mail: AdviceTariffManager@sce.com
E-mail Disposition Notice to: AdviceTariffManager@sce.com

EXPLANATION OF UTILITY TYPE
ELC = Electric GAS = Gas
PLC = Pipeline HEAT = Heat
WATER = Water

(Date Submitted / Received Stamp by CPUC)

Advice Letter (AL) #: 4078-E

Tier Designation: 3

Subject of AL: Request of Joint Investor-Owned Utilities for Approval of the Public Release of License Rights to Intellectual Property to Open Source Pursuant to Public Utilities Code Section 851 and General Order 173

Keywords (choose from CPUC listing): Compliance, Section 851

AL Type: ☐ Monthly ☐ Quarterly ☐ Annual ☑ One-Time ☐ Other:

If AL submitted in compliance with a Commission order, indicate relevant Decision/Resolution #:

Does AL replace a withdrawn or rejected AL? If so, identify the prior AL:

Summarize differences between the AL and the prior withdrawn or rejected AL:

☐ Yes ☑ No

5

☑ Yes ☐ No

5

No. of tariff sheets: -0-

Estimated system annual revenue effect (%):

Estimated system average rate effect (%):

When rates are affected by AL, include attachment in AL showing average rate effects on customer classes (residential, small commercial, large C/I, agricultural, lighting).

Tariff schedules affected: None

Service affected and changes proposed[1]:

Pending advice letters that revise the same tariff sheets: None

[1]Discuss in AL if more space is needed.

Clear Form

Protests and all other correspondence regarding this AL are due no later than 20 days after the date of this submittal, unless otherwise authorized by the Commission, and shall be sent to:

CPUC, Energy Division
Attention: Tariff Unit
505 Van Ness Avenue
San Francisco, CA 94102
Email: EDTariffUnit@cpuc.ca.gov

Name: Gary A. Stern, Ph.D.
Title: Managing Director, State Regulatory Operations
Utility Name: Southern California Edison Company
Address: 8631 Rush Street
City: Rosemead
State: California Zip: 91770
Telephone (xxx) xxx-xxxx: (626) 302-9645
Facsimile (xxx) xxx-xxxx: (626) 302-6396
Email: advicetariffmanager@sce.com

Name: Laura Genao c/o Karyn Gansecki
Title: Managing Director, State Regulatory Affairs
Utility Name: Southern California Edison Company
Address: 601 Van Ness Avenue, Suite 2030
City: San Francisco
State: California Zip: 94102
Telephone (xxx) xxx-xxxx: (415) 929-5515
Facsimile (xxx) xxx-xxxx: (415) 929-5544
Email: karyn.gansecki@sce.com

Clear Form

ENERGY Advice Letter Keywords

Affiliate	Direct Access	Preliminary Statement
Agreements	Disconnect Service	Procurement
Agriculture	ECAC / Energy Cost Adjustment	Qualifying Facility
Avoided Cost	EOR / Enhanced Oil Recovery	Rebates
Balancing Account	Energy Charge	Refunds
Baseline	Energy Efficiency	Reliability
Bilingual	Establish Service	Re-MAT/Bio-MAT
Billings	Expand Service Area	Revenue Allocation
Bioenergy	Forms	Rule 21
Brokerage Fees	Franchise Fee / User Tax	Rules
CARE	G.O. 131-D	Section 851
CPUC Reimbursement Fee	GRC / General Rate Case	Self Generation
Capacity	Hazardous Waste	Service Area Map
Cogeneration	Increase Rates	Service Outage
Compliance	Interruptible Service	Solar
Conditions of Service	Interutility Transportation	Standby Service
Connection	LIEE / Low-Income Energy Efficiency	Storage
Conservation	LIRA / Low-Income Ratepayer Assistance	Street Lights
Consolidate Tariffs	Late Payment Charge	Surcharges
Contracts	Line Extensions	Tariffs
Core	Memorandum Account	Taxes
Credit	Metered Energy Efficiency	Text Changes
Curtailable Service	Metering	Transformer
Customer Charge	Mobile Home Parks	Transition Cost
Customer Owned Generation	Name Change	Transmission Lines
Decrease Rates	Non-Core	Transportation Electrification
Demand Charge	Non-firm Service Contracts	Transportation Rates
Demand Side Fund	Nuclear	Undergrounding
Demand Side Management	Oil Pipelines	Voltage Discount
Demand Side Response	PBR / Performance Based Ratemaking	Wind Power
Deposits	Portfolio	Withdrawal of Service
Depreciation	Power Lines	

Clear Form

Appendix D: Outreach To Ensure Non-Duplication of Research

Throughout the duration of the program the CES-21 team had continuous interactions with vendors, companies and other research institutions to ensure that work performed under the CES-21 program is not duplicative of any other efforts. Additionally, whenever possible, the team participated and presented the CES-21 results at conferences and public. Below is a subset of those interactions. Complete list of all interactions is available upon request.

Outreach Event	Date
STIX Workshop with INL	2016
ICSJWG Next Evolution in Agile Response	2016
Attend IACD	2016
Attend Borderless Cyber	2016
RSA Luncheon	2016
Operator Workshop 1	2017
Operator Workshop 2	2017
PG&E IT Briefing	2017
CyberStrike Briefing	2017
OpenC2 Forum Presentation	2017
ICSJWG Patterning in STIX 2.0	2017
RSA Luncheon	2017
Attend Borderless Cyber	2017
PG&E SIOC Briefing on PG&E Use Case 1 and 2	2018
EnergySec Presentation	2018
STIX Training for PG&E	2018
Johns Hopkins IACD Presentation	2018
EPRI Presentation	2018
RSA Luncheon	2018
Attend Borderless Cyber	2018
PG&E SIOC Briefing and Feedback on Workflow	2018
Western Energy Institute - Electric and Natural Gas Ind	2019
DistribuTech 2018	2018
California ISO - multiple discussions	
TCIPG Workshop	

Appendix E: Grid Integration Report

California Energy System for the 21st Century

FINAL REPORT

Project	**Flexibility Metrics and Standards Grid Integration**
Title	***Role of Operating Flexibility in Planning Studies***
Project Team	
Pacific Gas and Electric Company	Antonio Alvarez, Will Dong, Ben Moradzadeh, Carl Nolen
San Diego Gas and Electric Company	Rob Anderson
Lawrence Livermore National Lab	Thomas Edmunds, John Grosh, Deepak Rajan
Astrape Consulting	Kevin Carden, Nick Wintermantel, Parth Patel , Alex Krasny
Electric Power Research Institute	Aidan Tuohy, Erik Ela, Eamonn Lannoye, Qin Wang
Date	September 7, 2017
Version Type	Final

Abstract

This project was conceived to examine the flexibility needs of the future California power grid. The analysis explores the need to establish generation planning metrics and standards that explicitly consider the operating flexibility needs of the system as the State pursues its aggressive renewable power generation goals. New methods and tools have been developed to use high resolution models of the grid that take into account uncertainties regarding renewable generation, load, equipment reliability, and economic growth. These models leverage high performance computational resources to fully explore the range of possible grid conditions that may lead to loss of load. The cost effectiveness of operating policies and hardware configurations that increase grid flexibility are examined with the tools to provide actionable information to grid planners and stakeholders.

Acknowledgement

The project team would like to thank the following Advisory Group members for their support and guidance throughout this project:

CPUC Energy Division (ED)
Maria Sotero
Patrick Young
Donald Brooks
David Miller
Forest Kaser

CPUC Office of Ratepayer Advocates (ORA)
Christopher Myers
Radu Ciupagea
Cindy Li

The California Independent System Operator (CAISO)
Shucheng Liu

The California Energy Commission (CEC)
Mike Jaske

The Utility Reform Network (TURN)
Kevin Woodruff

Southern California Edison Company (SCE)
Mark Nelson

Table of Contents

List of Tables

List of Figures

1 INTRODUCTION

1.1 Background

The California Energy Systems for the 21st Century (CES-21) Program is a collaborative research and development effort between the three California investor owned utilities – Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), and San Diego Gas and Electric Company (SDG&E) – and the Lawrence Livermore National Laboratory (LLNL). The objective of the CES-21 program, through two separate projects, is to explore the emerging challenges of cybersecurity and grid integration. The CES-21 program was approved by the California Public Utilities Commission (CPUC or Commission) on October 2, 2014 by Resolution E-4677.[6]

The Grid Integration Flexibility Metrics and Standards project ("Project") was conceived to examine the flexibility needs of the California Independent System Operator (CAISO) system, and to recommend, if appropriate, generation planning metrics and standards that explicitly consider the operating flexibility needs of the electric system. This report details the project's objectives, methods, results and recommendations, as well as requirements for the project managers set forth by the Commission.[7]

1.2 Project Requirements and Deliverables

In approving the CES-21 program, the Commission ordered specific requirements be met for successful completion of the project.

Table 1.1 below lists each requirement and demonstrates how the project delivered on these requirements.

Table 1.1 Project Requirements and Results

No.	Requirement	Delivered Results
1	Form a collaborative Advisory Group and meet at least once every six months to review and connect project results with relevant CPUC proceedings.	Formed an Advisory Group of CAISO, CEC, Energy Division (ED), ORA, SCE, and TURN. In total, the group held four meetings, and the project team provided several email updates.
2	Leverage learnings from PG&E's earlier collaborative review of planning model work.[8]	Based on the findings from the 2014 collaborative model review effort, selected the SERVM resource adequacy / production cost modeling tool to perform analysis for the project.
3	Present preliminary results and recommendations in a public workshop	Preliminary analysis and results were completed in 2015, and presented at a public workshop held on 1/6/2016.[10]

[6] http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M116/K104/116104291.PDF

[7] *See*, Res. E-4677, OP 2-5.

[8] http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M116/K104/116104291.PDF

[10] http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=9281

	using input assumptions from the 2014 Long-Term Procurement Plan (LTPP)[9]	
4	Demonstrate recommended metrics/standards in 2016 LTPP using at least one of the 2016 LTPP scenarios (Trajectory or expected scenario)	Final analysis was completed using 2016 LTPP assumptions. Project results and recommendations were presented to LTPP/IRP parties at a CPUC Integrated Resource Planning (IRP) proceeding on 8/15/2017. [11]
5	Provide 2016 LTPP parties opportunity to comment	Following the release of this CES-21 final report, the 2016 LTPP/IRP parties will be given the opportunity to provide written comments on the project's final results and recommendations.
6	Make database of detailed modeling input assumptions available	The entire set of input data used for the study will be made publicly available by the Energy Division.
7	Ensured ability of LTPP parties to license and use new or improved tools (if any)	Updated SERVM software is available for license by LTPP/IRP parties[12]
8	Offer one informal training session for Commission staff on new tools and models	The Project team held several calls during the project and met with CPUC staff on 8/16/2017 to provide training and updates on the SERVM tool and the CES-21 analytical framework.

1.3 Project Purpose

As a national energy leader, California has adopted aggressive goals to increase renewable generation to at least 50 percent of energy deliveries to customers by 2030, doubled efforts for cost-effective incremental energy efficiency, and invested in other alternatives such as transportation electrification. These efforts are key contributions to the wider goal of reducing GHG emissions economy-wide by 40 percent from 1990 levels by 2030. The electric grid needs to be operationally flexible to accommodate the diurnal patterns and hourly variability and forecast uncertainty of increased solar and wind generation needed to achieve the GHG emissions reductions. As a result, resource planners must gain a deeper understanding of the emerging flexibility needs of the system.

This need for deeper understanding is evident in recent LTPP proceedings. During the 2012 and 2014 LTPP proceedings, ED and CAISO staff facilitated a number of stakeholder workshops and working group meetings to discuss the flexibility needs of the CAISO system, with a particular focus on reliability. While significant progress was made through these discussions, a few important and challenging questions were not addressed fully, and provided an opportunity to be explored in this CES-21 research project.

Specifically, in an effort to enable resource planners to gain a deeper understanding of the emerging flexibility needs of the California electrical system, the project set out to answer the following questions:

[9] The project was implemented in two phases. Phase 1 was completed using 2014 LTPP assumptions with a simplified representation of the WECC. Phase 2 was completed using 2016 LTPP assumptions with a detailed representation of the WECC (see Technical Appendix for details). Unless otherwise noted, discussions in this report are based on results from Phase 2 of the study.

[11] http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=6442454487

[12] www.astrape.com

1. **Reliability Impact – Did the range of projected CAISO system scenarios have sufficient capacity and operating flexibility to meet the 1 day in 10 years reliability standard in 2026?** Reliability is the primary binding constraint of all resource planning processes. In order to better understand the interaction between operating flexibility and reliability, the project examined a range of CAISO system scenarios (some with more flexibility, some with less flexibility), and then measured each scenario's results against a specific reliability standard.

2. **Other Impacts – How did operating flexibility, or the lack of it, impact costs and emissions (i.e., system operations)? What are the main drivers?** Given that flexibility is a multifaceted system characteristic that impacts system operations in different ways at different times of the year, this project was designed to analyze flexibility needs in a range of weather conditions, economic forecast scenarios and unit performance scenarios. Furthermore, the project sought to analyze and explore the relationship between different flexibility solutions and their effectiveness, including some system level solutions that had not been modeled in previous reliability and operating flexibility studies.

3. **New Standards – Are new planning standards needed to maintain operational flexibility; and if so, what would those standards be?** This is an explorative, research question that looks to the future needs of the planning community. Properly used, planning standards can provide for easily measured threshold tests, thus avoiding the need for detailed reliability studies. For example, instead of conducting the more time intensive Loss of Load studies, the Planning Reserve Margin (PRM) metric has often been used by planners as an estimate of a system's surplus or deficiency for peak capacity needs. It was thought that if the project were able to detect systematic flexibility deficiencies, it could potentially help quantify such flexibility needs with new easy-to-measure metrics and standards that could be used in planning, similar to how planners use PRM for peak capacity planning.

1.4 Project Scope

To support its stated objectives, the research project focused on the following areas.

First, the project focused on the ability of the generating system to provide adequate capacity at all times of the year while respecting generating unit constraints and considering forecast uncertainty. This is broader than typical resource adequacy analysis which generally assumes all available capacity can be used to serve load. However, the simulations were performed using a transportation model of the electric system, so more granular transmission reliability concerns were not addressed. For example, topics such as frequency response and voltage control were beyond the project scope.

Secondly, the project adopted a resource planning perspective and assumed the physical characteristics of the system – such as curtailment and net imports – could be fully accessed by system operations. In other words, the project did not take a position on policy issues, such as how much renewable curtailment is appropriate. Similarly, the project did not address some operational issues such as how much net import the system operator could actually rely upon, nor market design issues such as how much of the available physical flexibility would be economically provided to the system based on market compensations. Instead, the project simply assumed a range of clearly stated values, and focused on understanding their impact on resource planning.

Finally, the goal of the project was to provide directionally useful information, not precise results. Rather than drawing precise conclusions based upon static input assumptions, this

project was designed to gain broader understanding through various sensitivities aimed at identifying key drivers and testing the magnitude of their impacts. The project's goal was to develop a robust framework and a set of insightful findings to help policy makers and other stakeholders to further explore and better understand the topic of operational flexibility.

1.4.1 Relationship with Other Resource Planning Studies / Analyses

Project results here should not be compared against those from any specific capacity expansion modeling exercises, as the assumptions developed for this analysis were only vetted to the level of providing directional information. Instead, insights drawn from this project can inform inputs into other resource planning analyses, and the analytical framework designed for this project can be used to examine particular scenarios in other modeling exercises.

1.4.2 Connection with Other Studies

Informed by the collective knowledge of the project team and the Advisory Group, the project built upon the latest knowledge in the resource planning space.[13] At the same time, this project was uniquely designed to answer its own objectives, which led to the detailed modeling of the entire WECC region, the inclusion of uncertainties, and the testing of the CAISO system under a unique set of system scenarios.

Although the project was focused on the operating flexibility needs and performance of the California electric grid, the project's analytical approach, as well as its results and recommendations, can inform other systems that have, or anticipate having, large amounts of renewable generation.

1.5 Summary of Findings and Recommendations

- Under the assumed resource mix studied, up to 50% RPS, the CAISO system has sufficient operating flexibility to meet demand in a reliable manner, subject to the assumption that the system operator can fully access the flexibility available including curtailments and net imports
- In terms of new planning standards, the CES-21 results suggest there is no need, at this time, to add additional flexibility-related standards for addressing reliability-related issues
- Planning Reserve Margin (PRM) is still a useful metric to assess adequacy, but the Effective Load Carrying Capability (ELCC) of all resources needs to be accurately calculated and used in the PRM calculation
- Sufficient load following capability must be carried in order to ensure intra-hour flexibility sufficiency – and there is a potential tradeoff between reliability and economics in calculating requirements
- Use of new Loss of Load Expectation (LOLE) metrics – $LOLE_{INTRA\text{-}HOUR}$ and $LOLE_{MULTI\text{-}HOUR}$ allow for greater understanding of the flexibility needs and resources. How these relate to $LOLE_{CAPACITY}$ needs to be further considered.

[13] For example, the CPUC's recent Effective Load Carrying Capabilities (ELCC) studies in the RA proceeding, CAISO's 2014 LTPP studies, and E3's 2016 WECC Flexibility Assessment

2 ANALYTICAL FRAMEWORK

2.1 Overview

In order to answer the key questions, this project needed to develop an analytical framework that can characterize the flexibility needs of a system and also capture its full impact on system operations.

For model inputs, the project need to consider a range of wind and solar profiles in order to reasonably cover generation patterns from renewable resources under different weather conditions. This is analogous to the need to simulate multiple forced outage patterns for conventional generators. The load corresponding to these weather patterns also had to be represented. To do this, the project leveraged Astrape Consulting's expertise to develop 35 sets of correlated wind, solar, and load hourly profiles based on historical weather patterns observed during 1980 – 2014.[14] Similarly, intra-hour volatility (e.g., forecast errors for wind, solar and load) also needed to be modeled in order to create a realistic representation of system conditions with high renewable penetration. Finally, other uncertainties such as economic load growth forecast errors and generation forced outages, commonly modeled in resource adequacy studies, are also included.

In selecting a modeling tool, the project needed to simulate system behavior at sub-hourly intervals over the entire year. This required an enhancement relative to previous resource adequacy tools that only focused on evaluating system needs during peak demand hours. The framework also needed to produce probabilistic results, a feature common in resource adequacy tools, in order to measure reliability. To provide statistically meaningful results in the presence of all of these sources of uncertainty, the test year would need to be simulated thousands of times. Hence, production cost modeling software with fast execution times was needed. With these features in mind, the Strategic Energy Risk Valuation Model (SERVM) modeling tool was selected for this project.

Finally, the analytical framework also needed metrics to capture the flexibility requirements and deficiencies of the system. Accordingly, the project developed new metrics to explicitly detect loss of load events due to the inability to meet multi-hour, or intra-hour ramping needs[15] rather than insufficient capacity. To help us understand the holistic impact of operational flexibility challenges, the framework also provided standard system performance measures such as production costs (including net market purchases), emissions, and renewable curtailment.

Table 2.1 below summarizes the overall analytical framework developed for the project.

[14] See Technical Appendix for details

[15] Specifically, loss of load expectation (LOLE) due to multi-hour or intra-hour events.

Table 2.1 Analytical Framework Used for the Study

Inputs	Model	Results
Load and Resource Assumptions Each study case is a 2026 projected CAISO system with detailed WECC representation	**Strategic Energy Risk Valuation Model (SERVM)** A hybrid resource adequacy and production cost model	**System Performance** Reliability (capacity / flexibility), Cost, and Environmental Impact
Uncertainties considered for each study case • 35 weather years (correlated profiles for load / wind / solar) • 5 economic load growth uncertainty levels • 25 (or more) resource outage draws • Forecast errors for load / wind / solar (intra-day and intra-hour) • 20 study cases / scenarios[16]	Number of simulation iterations: 35 * 5 * 25 * 20 = 87,500 full years (8,760 hours each at 5 minute intervals) of simulated system operations	Key metrics captured: • Loss of load expectation (LOLE) due to lack of capacity • LOLE due to lack of flexibility (new metrics) • Production variable costs • CO_2 emissions • Renewable curtailment

The SERVM software was selected based on its unique set of features as reported in a recent collaborative review of planning models performed in 2014[17]. The features that are essential to this project include the ability to:

- Represent planning and operating uncertainties;
- Simulate system conditions within the hour and across all hours of the year;
- Calculate traditional reliability metrics and the ability to incorporate new operational flexibility metrics;
- Model a wide range of scenarios and sensitivities and complete the analysis within time available; and
- Calculate various system performance metrics, such as production costs, renewable curtailment, and GHG emissions, which are useful to assess the desirability of planning standards

[16] The list of study cases are described in the Data and Study Cases section of the report

[17] Pacific Gas and Electric Company, et al., Collaborative Review of Planning Models, (April 2014), available at www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=6626

In addition, parties to CPUC proceedings are already familiar with the model since the Energy Division is using it to estimate the effective load carrying capacity (ELCC) of wind and solar generation in the RA proceeding. SERVM is readily available and can be licensed by any party.

2.2 Key Metrics

This section lists and describes the key metrics produced by SERVM. Because SERVM is a stochastic modeling tool, each metric represents the expected annual value from a specific study case. However, if desired, iteration specific results (down to hourly levels) can be extracted from SERVM by re-running the desired study case.[18]

2.2.1 Reliability Metrics

LOLE is the main reliability metric used in the study. This is a generally accepted metric used in planning to measure the expected number of loss of load events over a given time period. The most commonly used time frame for LOLE is the number of events in 10 years, and that is the measure used in this study.[19]

In the past, the LOLE metric is solely used to measure loss of load events caused by capacity inadequacy (i.e., lack of available capacity to meet load during an hour of peak demand). In this study, loss of load events are further disaggregated by the type of resource deficiencies that caused them. The SERVM software logic that performs this disaggregation is detailed in the Technical Appendix.

- $LOLE_{CAPACITY}$ (events / 10 years) – Loss of load expectation due to generic capacity inadequacy to meet peak load
- $LOLE_{INTRA\text{-}HOUR}$ (events / 10 years) – Loss of load expectation due to flexible capacity inadequacy to meet intra-hour net load volatility
- $LOLE_{MULTI\text{-}HOUR}$ (events / 10 years) – Loss of load expectation due to flexible capacity inadequacy to meet multi-hour net load ramp
- $LOLE_{TOTAL}$ (events / 10 years) – Loss of load expectation due to capacity inadequacy of any kind[20]

2.2.2 Other CAISO System Level Metrics

- Renewables Curtailment (GWh) – Expected aggregate annual curtailment [21]
- Emissions (MMT) – Expected aggregate annual emissions calculated as the sum of all emissions from CAISO resources (using resource specific emissions

---

[18] This can be accomplished by turning on detailed reporting features and re-running the case. By default, iteration specific results at the monthly, daily, or hourly level are not recorded in order to speed up simulation run-time.

[19] See CPUC's "Production Cost Modeling Requirements" ruling for additional discussion on reliability metrics http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M167/K501/167501732.PDF

[20] Total LOLE represents the number of days with events of any LOLE type, and does not necessarily equal to the summation of LOLEs by type (e.g., two types of LOLE events can occur on a given day and only counts as one occurrence under $LOLE_{TOTAL}$).

[21] In this project, SERVM's economic commitment and dispatch algorithm attempted to minimize curtailment subject to economic and reliability constraints. No separate curtailment penalty was included in inputs to further limit curtailment beyond the economic commitment solution.

rates) and the sum of all emissions from net imports (using an hourly import emissions rate based on a proxy heat rate of 8,000 Btu/kWh)

- Production Cost ($ Billions) – Expected aggregate annual CAISO cost to operate the system, including costs incurred by internal resources and also net purchase costs from external, non-CAISO regions
- Total Cost ($ Billions) – this is the sum of the production cost defined above and the expected approximation for the cost of curtailment (which is calculated by multiplying the Renewable Curtailment GWh metric by an assumed curtailment replacement cost of $50 / MWh)[22]

2.3 LLNL's High Performance Computing (HPC) Environment

The design of this project required a very large number of simulations. Specifically, to model the many uncertainties and range of study cases (discussed in the following section), more than 87,500 years of CAISO system operations had to be simulated. Moreover, LOLE values of one day in 10 years of operation at five minute intervals corresponds to detecting one event in over a million time intervals. Although SERVM includes many algorithm features and heuristics to speed execution time, the large scale of this computational campaign suggests the need for high performance computing (HPC) resources.

HPC resources and the expertise to utilize them were available at Lawrence Livermore National Laboratory (LLNL). The computer systems at LLNL contain over a million individual microprocessor cores, which allowed simultaneous execution of thousands of SERVM models in parallel. This enabled completion of the computational campaign thousands of times faster than execution on a single computer.

In order to access this computing power, however, the project team had to first reconfigure the SERVM software so that it could be deployed in an HPC environment and jobs executed in parallel. The Astrape Consulting and LLNL team was able to develop the software infrastructure for massively parallel deployment of the SERVM code. This research effort resulted in a new capability for industry. Now that the research effort has been completed, the capability could also be duplicated using commercial cloud computing services.

Deploying SERVM on LLNL's HPC system resulted in significant efficiency gains. For example, the ability to access 1,000+ cores of CPU and to process SERVM simulations in parallel resulted in program execution speeds hundreds of times greater than that of desktop computers.[23] Even compared to a cluster of dozens of desktop computers, the ability to access HPC systems effectively reduced run time from days to hours.

---

[22] Similar to past LTPP analysis, the project did not replace any curtailed energy with additional RPS resources (which is what a capacity expansion model would do); instead, a $50/MWh value is used to approximate the replacement cost for any curtailed energy.

[23] For example, a typical modern laptop computer has between 4 – 8 cores of CPU, so an HPC environment of 1,000 cores will achieve an efficiency gain of 1,000 / 4 to 8 = 250 to 125 fold.

3 DATA AND STUDY CASES

3.1 Projected 2026 CAISO System

Similar to the approach taken in previous LTPP cycles, the project first developed a system model for the 2026 planning year. The model captured both the CAISO system, using the approved 2016 LTPP assumptions and other systems in the WECC, using the latest available TEPPC 2026 Common Case.[24]

Detailed modeling of internal CAISO transmission and sub-regions of the WECC is especially important for this project as it allows for detection of flexibility issues caused by intra-regional transfer limitations that may otherwise be masked.[25] The Technical Appendix to this report provides additional details and lists all the sub-regions modeled.

Overall, the project's general modeling approach follows the guidelines provided by the Commission's September 23, 2016 ruling, and the attachment to this ruling titled "Production Cost Modeling Requirements."

3.2 Modeled Uncertainties

As discussed in the framework section, fundamental to a reliability study that examines portfolios with large amounts of variable generation is the need to model uncertainties. On top of the deterministic 2026 representation of the CAISO/WECC system, the project injected the following uncertainties:[26]

- 35 wind, solar, and load profiles and hydro inputs that correlate with historical weather patterns from 1980 – 2014
- 5 levels of economic load growth forecast errors
- Forecast errors for load, wind and solar (both hourly and within the hour)
- Generation forced outage patterns

With each modeling draw, a specific combination of uncertainties and hence a unique projection of a 2026 system is selected.

3.3 Study Cases / Scenarios

Whereas the range of uncertainties allows us to examine how random events affect a given study case, a set of carefully chosen study cases allows us to explore reliability challenges faced by different scenarios.[27]

Here, the Project tested the performance of the CAISO grid under 20 different scenarios with different amounts and types of renewable resources, and different amounts of flexibility

[24] 2016 LTPP approved scenarios and assumptions http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=11673

[25] For instance, a coarser representation of the WECC may not reveal ramping limitations between sub-regions.

[26] See Technical Appendix for details on how each uncertainty is developed, including data sources and methods

[27] In this report, study cases and scenarios are used interchangeably to represent different 2026 CAISO systems.

being available to the grid, to determine at what point, and under what conditions, operating flexibility could become a reliability issue, and to quantify cost and emission impacts associated with higher or lower levels of flexibility.

At a high level, the scenarios are created by varying and testing the three aspects of reliability discussed under the Metric sections and grouped as such:

- **Capacity adequacy**: by varying the amounts and type of renewable resources (cases BC_01, BC_02, and BC_03);
- **Flexibility adequacy (intra-hour)**: by varying the amounts of flexible reserves, also known as load following reserves (cases SC_02 through SC_07); and
- **Flexibility adequacy (multi-hour)**: by varying the amounts of system flexibility in terms of
    - Ramping capability available from existing fossil fleet; (cases SC_08 through SC_11)
    - Ramping capability available through managing CAISO's net imports (cases SC_12 through SC_14)
    - Export capability to CAISO's neighboring balancing areas (cases SC_15 through SC_17)

Table 3.1 below provides a high level summary of the scenarios used for the final analysis. High level description of each group of cases is provided below, with additional details in the Technical Appendix.

Table 3.1 List of Study Cases

Case #	Type of Case	RPS % by 2026	Load Following	System P_{MIN}	Interchange 3-Hr Ramp	Net Exports Limit
BC_01	PRM Base Cases	33%	5% of Load	LTPP Default	Unlimited	2,000 MW
BC_02		43%	7% of Load			
BC_03		50%	9% of Load			
SC_01	**Reference Case**	**50%**	**9% of Load**	**LTPP Default**	**Unlimited**	**2,000 MW**
SC_02	Load Following (% of Load)		5% of Load			
SC_03			7% of Load			
SC_04			11% of Load			
SC_05	Load Following (Net Load Observed)		95th Pct			
SC_06			99th Pct			
SC_07			100th Pct			
SC_08	System P_{MIN} (+/- MW)			(-4,000)		
SC_09				(-2,000)		
SC_10				(+2,000)		
SC_11				(+4,000)		
SC_12	Interchange 3-Hour Ramp Limit				3,000 MW	
SC_13					6,000 MW	
SC_14					9,000 MW	
SC_15	Net Exports Limit					3,500 MW

SC_16	5,000 MW
SC_17	8,000 MW

3.3.1 Capacity Adequacy Cases (BC_01, BC_02, BC_03)

The Planning Reserve Margin (PRM) base cases represent 2026 systems with different levels of RPS penetration ranging from 33% to 50% (i.e., wind, solar) and also behind the meter PV; they are otherwise identical in load and generation assumptions. Specifically, the 43% RPS case (BC_02) is the "Reference Case" Scenario 2: the Default Scenario with the mid-level additional achievable energy efficiency sensitivity, described in the May 17, 2016 Assigned Commissioner's Ruling Adopting Assumptions and Scenarios for Use in the California Independent System Operator's 2016-17 Transmission Planning Process.

3.3.2 CES-21 Reference Study Case (SC_01)

This case is identical to the 50% RPS base case (BC_03), except in this reference case, instead of adding generic conventional resources, 600 MW of Energy Efficiency was added to achieve the $LOLE_{CAPACITY}$ standard of 1 day in 10 years.[28] All other study cases (SC_02 through SC_17) are built upon this reference case.

3.3.3 Intra-Hour Flexibility Adequacy Cases (SC_02 through SC_07)

These cases modeled different amounts of load following reserves available to mitigate intra-hour variability and forecast uncertainty of customer demand, and wind and solar generation. Two different methods were deployed to set LF requirements: one as a % of load, the other based on the amount of net load variation observed in the previous 60 days.[29]

3.3.4 Multi-Hour Flexibility Adequacy Cases (SC_08 through SC_17)

SC-08 through SC-11 quantified the impact of higher and lower ramping capability being available from the existing fossil fleet by adjusting their P_{MIN} levels, making these cases more or less flexible than the reference case.

SC-12 through SC-14 imposed maximum 3-hour ramping limits varying from 3,000 MW to 9,000 MW to CAISO imports and exports, making these cases less flexible than the reference case, which had no such limit.

SC15 through SC-17 examined the effect of expanding the net export limits to CAISO neighboring balancing areas from 3,500 MW to 8,000 MW in any given hour, making these cases more flexible than the reference case.

[28] See Results section for analysis on the amount of capacity that is needed to reach the 1 day in 10 years standard for the PRM base cases.

[29] Net load is calculated as load net of wind and solar generation

3.3.5 Additional Storage Sensitivity Cases

Given the ongoing public interest in battery storage as a grid integration solution, the project tested two additional set of sensitivity cases to better understand storage's contribution in terms of:

1. Reliability contribution; and
2. Economic and curtailment benefits

To examine storage's reliability contributions, the project tested three cases by adding 3,000 MW, 6,000 MW, and 10,000 MW of 4 hour duration battery storage to the reference study case and measured the average capacity value (i.e., ELCC) for the entire class of 4-Hour battery storage.

For the economic and curtailment benefit runs, the project created four cases, each adding 1,000 MW of a different type of storage device – 2-hour, 4-hour, 6-hour, and 8-hour battery storage – to the reference case.

3.4 Access to Input Data

The SERVM model inputs used for the final analysis will be made publicly available by the Energy Division.

4 RESULTS

This section presents study case results along with some high level descriptions. Detailed interpretation and synthesis of results are captured in the next section on recommendations.

The results section is organized in the same three groupings of cases as presented earlier:

1. Capacity adequacy results
2. Intra-hour flexibility adequacy results
3. Multi-hour flexibility adequacy results

Table 4.1 below provides a summary of results for the 20 defined study cases. Key metrics shown in this table are defined in the Key Metrics subsection of this report.

Table 4.1 Summary of Results (CES-21 Study Cases)

Case #	Type of Case	Description	LOLE CAPACITY[30]	LOLE INTRA-HOUR	LOLE MULTI-HOUR	LOLE TOTAL	Curtailment		Emissions	Total Cost
			(Events / 10 Years)				(GWh)[31]	(%)[3]	(MMT)	($ Billion)[32]
BC_01	PRM Base Cases	33% RPS	1.0	0.1	0.0	1.0	242	0.2%	61	7.2
BC_02		43% RPS	1.0	0.1	0.0	1.0	2,652	2.1%	52	6.4
BC_03		50% RPS	1.0	0.1	0.1	1.0	6,129	4.9%	49	6.5
SC_01	**Study Case**		**1.0**	**0.1**	**0.1**	**1.0**	**6,466**	**5.2%**	**48**	**6.4**
SC_02	Load Following (% of Load)	5%	0.8	0.6	0.0	1.4	5,503	4.4%	47	6.1
SC_03		7%	0.9	0.1	0.0	0.9	5,961	4.8%	47	6.3
SC_04		11%	1.1	0.1	0.0	1.1	7,045	5.6%	49	6.7
SC_05	Load Following (NL Observed)	95 Pct	0.9	99.5	13.6	113.0	4,797	3.8%	46	5.9
SC_06		99 Pct	0.7	25.3	1.5	27.4	4,987	4.0%	46	6.0
SC_07		100 Pct	0.7	2.4	0.0	3.1	5,624	4.5%	47	6.2
SC_08	P_{MIN} (+/- MW)	(-4,000 MW)	1.0	0.2	0.1	1.2	3,751	3.0%	46	6.0
SC_09		(-2,000 MW)	1.0	0.1	0.1	1.0	4,802	3.8%	47	6.2
SC_10		(+2,000 MW)	0.9	0.1	0.1	0.9	9,940	8.0%	49	6.7
SC_11		(+4,000 MW)	1.0	0.1	0.0	1.0	15,447	12.4%	51	7.3
SC_12	Interchange 3-Hour Ramp Limit	3,000 MW	1.7	0.2	0.1	1.7	8,548	6.8%	49	8.5
SC_13		6,000 MW	0.9	0.1	0.0	0.9	6,835	5.5%	48	7.1
SC_14		9,000 MW	0.9	0.1	0.0	0.9	6,572	5.3%	48	6.7
SC_15	Net Exports	3,500 MW	1.0	0.1	0.0	1.0	5,259	4.2%	48	6.3
SC_16		5,000 MW	1.0	0.1	0.0	1.0	4,553	3.6%	47	6.3
SC_17		8,000 MW	1.1	0.1	0.0	1.1	4,113	3.3%	47	6.3

[30] See Framework section for definition of key metrics

[31] This study did not model resources needed to replace any curtailed energy in order to meet a given RPS %

[32] This includes the total system production cost (includes cost of net imports), plus an approximated cost of curtailment (by assuming a replace cost of $50 / MWh)

4.1 Capacity Results (PRM Cases)

As discussed in the Study Case section, the Planning Reserve Margin (PRM) cases tested three different systems, each carrying a different level of wind and solar generation with otherwise identical load and generation. **Table 4.2** below shows the generation portfolio by resource type for each of the three scenarios.

Table 4.2 Name Plate Capacity by Resource Type (Planning Reserve Margin Cases)

Resource Type (Name Plate MW)	33% RPS	43% RPS	50% RPS
Aggregated GHG Free Portfolio	**38,888**	**50,000**	**54,289**
Solar (IFM + BTM PV)[33]	13,075	23,897	27,495
IFM	8,035	12,764	16,362
BTM	5,040	11,133	11,133
Wind	6,027	6,317	7,008
Other Renewables[34]	4,522	4,522	4,522
Energy Efficiency (EE)[35]	4,491	4,491	4,491
Energy Storage	1,350	1,350	1,350
Demand Response	1,559	1,559	1,559
Hydro and PSH[36]	7,863	7,863	7,863
Conventional			
Fossil Resources (CAISO)	26,740	26,740	26,740
Imports	11,665	11,665	11,665

4.1.1 ELCC Results

As shown in **Table 4.2**, the 43% RPS scenario carries far more solar and wind resources than the 33% RPS case, by a combined 11,112 MW. This difference in name plate capacity, however, does not directly translate into difference in dependable capacity to mitigate loss of load events. As various other planning studies have shown, when it comes to reliability assessments, a meaningful comparison can only be made if resources are measured by their reliability contributions – not name plate capacity – via methods such as the Effective Load Carrying Capability (ELCC) calculation. This calibration is especially necessary at higher renewable levels and particularly important for non-dispatchable resources such as solar and wind, whose reliability contributions are significantly impacted by the particular portfolio mix, which affects the timing of the system reliability need (i.e., the hours of system peak net load).

[33] In front of the meter and behind the meter PV

[34] This includes geothermal and biomass resources, also includes certain small, non-dispatchable hydro resources

[35] Energy Efficiency values are based on IEPR Mid Base - Mid AAEE forecast (e.g., 1xAAEE)

[36] Pumped storage hydro

In this project, with the exception of fossil resources and imports, ELCC calculation is performed for every resource type – including demand side resources such as Energy Efficiency (EE) and BTMPV – in order to capture any changes in reliability contribution as more renewables were added to the system.[37]

Figure 4.1 below shows the average ELCC value for the aggregated GHG free portfolio and selected resource types, for the three cases. Overall, the aggregate ELCC decreases as RPS levels rise, largely driven by the diminishing ELCC value of solar.[38] The effect on other resource types are also visible, though less dramatic. For example, there is a slight decrease in EE due to the shift in timing of the peak net load.[39] Conversely, there is a slight increase in the value of storage due to shortening of the duration of the system peak net load as more solar is added to the system, an effect further discussed in the storage sensitivities section.

37 For this project, ELCCs are calculated relative to a generic fossil resource. First, each projected system is calibrated to a given reliability level by adding or removing generic fossil resources to achieve an $LOLE_{CAPACITY}$ of 1 day in 10 years. Then, for each resource type evaluated (e.g., wind), the entire portfolio of this specific resource type is removed from the system (e.g., 5,000 MW of wind). Following this, generic fossil resources were added to the system until an $LOLE_{CAPACITY}$ of 1 day in 10 years is regained (e.g., 1,000 MW of generic resource). The amount of generic capacity added divided by the name plate of all the specific resource type removed is the ELCC % shown here. Such an ELCC calculation implicitly considers the reliability needs of the system across all hours of the day, thus obviating the need to focus on specific hours and can accurately reflect system changes (e.g., when the system peak net load is pushed further into the evening)

38 The average ELCC of solar resources did not decline as rapidly as expected between 43% and 50%. The primary reason is that the mix of solar resources between 33% and 40% RPS was heavily weighted toward BTMPV while between 43% and 50% RPS was heavily weighted toward fixed and tracking utility scale PV. The solar profiles for BTMPV reflect suboptimal orientation and tilt and thus provide limited output in late afternoon hours, while the utility-scale solar configurations are more optimized and show higher output in these hours. So while the net load peak was later in the day in the 50% RPS cases, the more optimized solar shapes partially offset the impact of the net load shift.

39 The EE data is limited to a static 8,760 hourly profile published by the CEC, which was assumed as constant and used across all the weather years in this analysis. Depending on the EE programs, this assumption may have underestimated or overestimated EE's ELCC, and is an area that can benefit from future research.

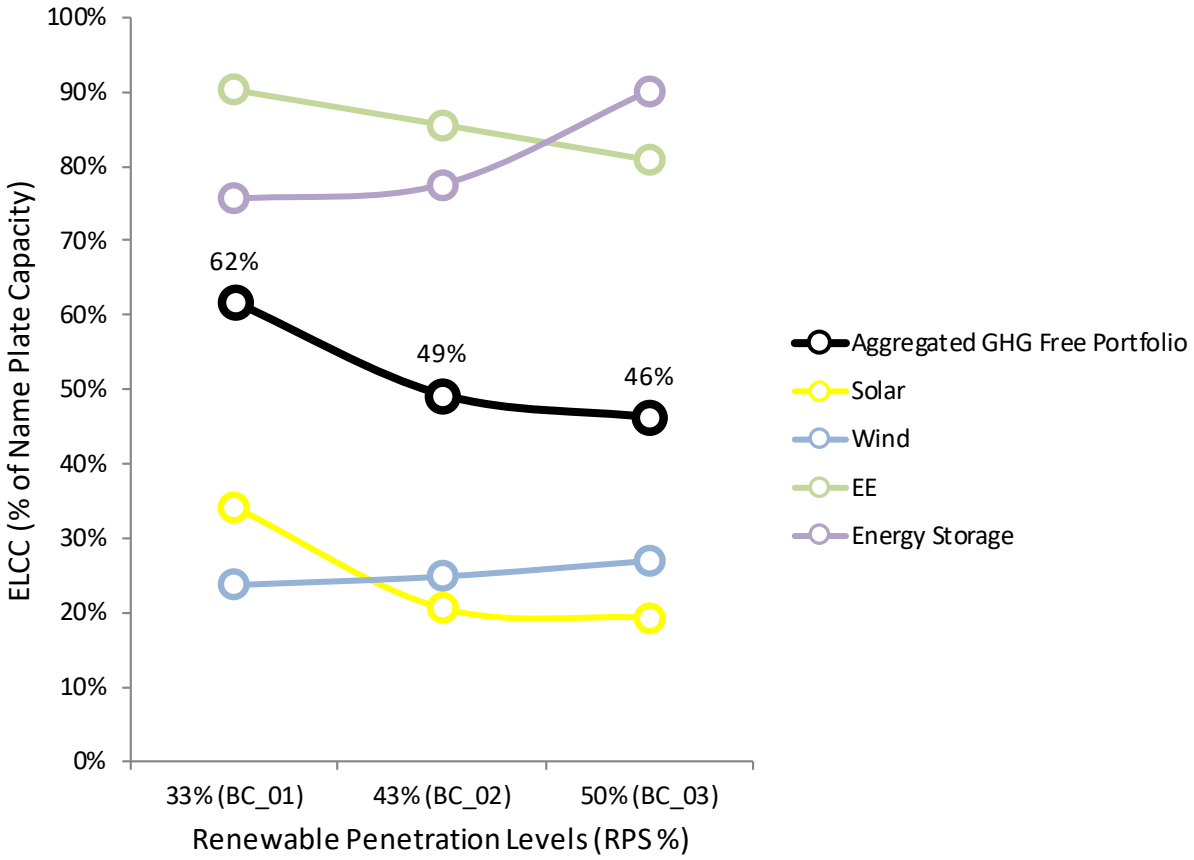


Figure 4.1 Average Effective Load Carrying Capability (ELCC) at Various RPS % Levels

4.1.2 Capacity Adequacy Results

For the PRM cases, the project team performed a capacity adequacy analysis for each of the three systems. **Table 4.3** below shows the amount of capacity that is needed for each system to reach the reliability standard of $LOLE_{CAPACITY}$ of 1 day in 10 years.[40]

Table 4.3 Reliability Results for As-Is PRM Base Cases

	33% RPS	43% RPS	50% RPS
Reliability Results ("as is")			
$LOLE_{CAPACITY}$ (days / 10 years)	2.9	1.9	1.4
Deficiency / (Surplus) to reach 1 day in 10 years standard			
Generic Resource Additions (MW)	1,348	730	393

As these results show, all three systems, as is, are less reliable than the standard.

[40] In all three scenarios, the project assumed the same Energy Efficiency level of 1xAAEE

4.1.3 Calculating Planning Reserve Margin

Having calibrated all three cases to a common reliability standard, the corresponding Planning Reserve Margins are calculated and shown in **Table 4.4** below.

Table 4.4 PRM Calculation – Method 1 (Treating all resources as supply side measured by ELCC)

Line #	PRM Calculation	33% RPS	43% RPS	50% RPS
	Demand			
1	Gross Consumption (MW)	54,727	54,727	54,727
	Supply			
2	Aggregate GHG Free Portfolio (excluding EE)	19,971	20,817	21,490
3	Fossil Resources	26,740	26,740	26,740
4	Imports	11,665	11,665	11,665
	Demand Side Resources Modeled as Supply			
5	Energy Efficiency	4,053	3,844	3,631
	Deficiency / (Surplus) to reach LOLE standard			
6	Generic Resource Additions	1,348	730	393
	PRM to satisfy LOLE standard (%)[41]	**116.5%**	**116.6%**	**116.8%**

It is critically important to understand that there are multiple methods to calculating PRM used throughout the electric industry. Each PRM is derived based on a specific method, and meaningful comparison between PRMs can only occur if the methods match; otherwise, comparisons are meaningless. For the PRMs shown above, two unique features define its method: 1) all resources are calculated with their ELCC (even demand side resources); 2) demand side resources are treated as supply resources and not netted out of the gross consumption data.

Using a different method, the resulting PRM that correspond to the same reliability standard would look significantly different. The following example illustrates that point. **Table 4.5** below shows the same three systems, except in how EE is treated in the PRM calculation. Under this method, EE is treated as a load modifier, where it is netted out of load based on EE's contribution at the time of system coincident, gross peak.

Table 4.5 PRM Calculation – Method 2 (Treating EE as load modifier)

Line #	PRM Calculation	33% RPS	43% RPS	50% RPS
	Demand			
1	Gross Consumption (MW)	54,727	54,727	54,727

[41] Calculated as the ratio between a) sum of lines 2 through 6 and b) line 1

2	Energy Efficiency	4,491	4,491	4,491
	Supply			
3	Aggregate GHG Free Portfolio (excluding EE)	19,971	20,817	21,490
4	Fossil Resources	26,740	26,740	26,740
5	Imports	11,665	11,665	11,665
	Deficiency/ (Surplus) to reach LOLE standard			
6	Generic Resource Additions	1,348	730	393
	PRM to satisfy LOLE standard (%)[42]	**118.9%**	**119.3%**	**120.0%**

This set of PRMs is higher than the previous set for two reasons First, using EE's output at the gross peak load in this set assumes a higher reliability contribution for EE than it would actually provide during time of the net load peak (this effect is shown using an illustrative example in **Figure 4.2** below). Second, netting EE from gross demand in the PRM calculation essentially credits EE with the full PRM (i.e., PRM is calculated here by dividing capacity needed against the gross load net of EE), thus produces a higher PRM.

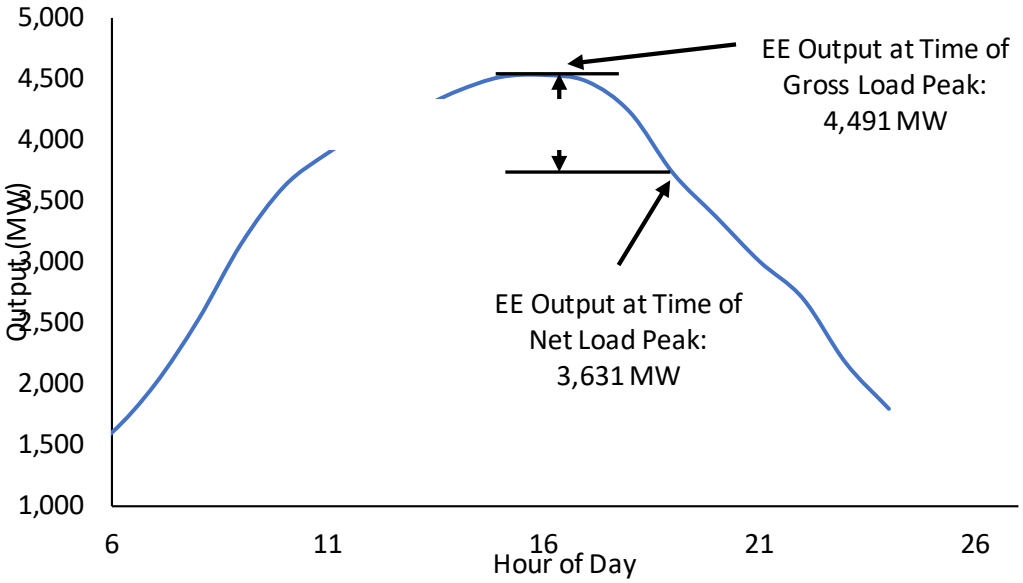


Figure 4.2 Energy Efficiency Output at Time of Gross and Net Load Peaks

However, these two calculations are done on the same system. Re-calculating the PRM using a different formula doesn't change the MW of generic resource additions needed to satisfy the LOLE standard.

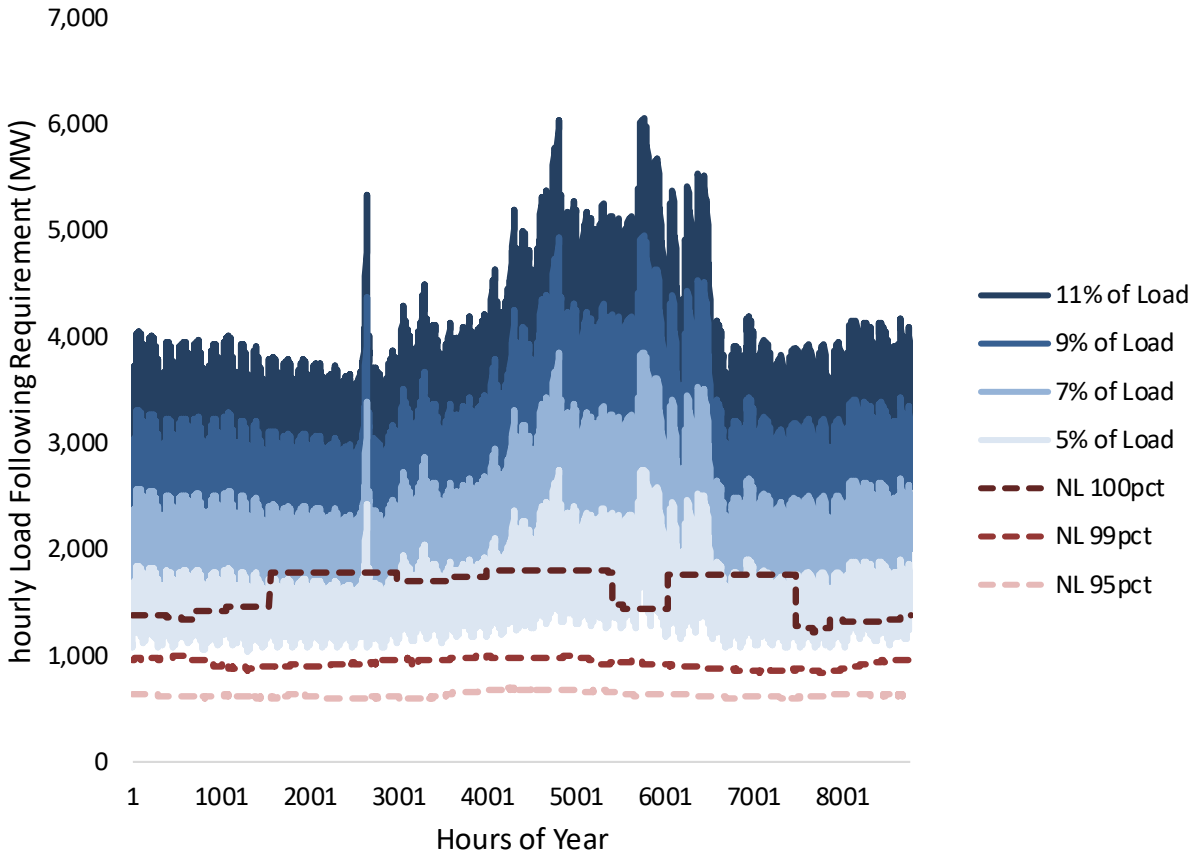
These PRM tables show the importance of applying and using PRM correctly, a topic that is further discussed in the recommendations section.

[42] Calculated as the ratio between a) sum of lines 3 through 6 and b) difference between lines 1 and 2

Other than capacity adequacy, these PRM cases also needed different levels of LF to maintain the same $LOLE_{INTRA-HOUR}$.[43] Very little $LOLE_{MULTI-HOUR}$ events were detected in all three cases. Instead, system flexibility challenges showed up under economic metrics such as curtailment. Specifically, the 33%, 43%, 50% RPS cases resulted in annual curtailments of 0.2, 2.6, and 6.1 TWh respectively (corresponding to 0.2%, 2.1%, and 4.9% of annual output from all RPS eligible resources).

4.2 Intra-Hour Flexibility Results (Load Following Cases)

As discussed in the study case section, the project tested seven different levels of load following reserves. **Figure 4.3** below shows the hourly amount of load following that is carried in each case. It illustrates the wide range of load following covered among these cases (e.g., the maximum hourly load following reserves difference between the 11% of hourly load and the NL 95th percentile cases is over 5,000 MW).



[43] The relationship between LF and $LOLE_{INTRA-HOUR}$ is presented in the Intra-Hour Flexibility results section, and the recommendations section. For the 33%, 43%, and 50% RPS PRM base cases, hourly load following requirements were set to 5%, 7%, and 9% of hourly load in order to maintain a similar level of $LOLE_{INTRA-HOUR}$ at roughly 0.1 events / 10 years.

Figure 4.3 Hourly Load Following Requirements (Load Following Cases)

For each of these cases, reliability results were measured by the $LOLE_{INTRA\text{-}HOUR}$ metric. Results in **Table 4.6** shows a clear relationship between the amount of load following reserved and the number of $LOLE_{INTRA\text{-}HOUR}$ events detected.[44]

Table 4.6 Load Following Requirement vs. $LOLE_{INTRA\text{-}HOUR}$

Case #	LF Method	Description	Annual LF Amount (TWh)	$LOLE_{INTRA\text{-}HOUR}$ (Events / 10 Years)
SC_05	NL Observed	95 Pct	6	99.5
SC_06		99 Pct	8	25.3
SC_07		100 Pct	14	2.4
SC_02	% of Gross Load	5%	14	0.6
SC_03		7%	19	0.1
SC_01		9%	25	0.1
SC_04		11%	31	0.1

While the timing of the addition of reserves was not optimized in any case, the difference in LOLE between cases SC_07 and SC_02 highlights the impact that timing has on results. Both cases supplied 14 TWh of annual load following, but $LOLE_{INTRA\text{-}HOUR}$ ranged from 0.6 to 2.4. Case SC_07 utilized a rolling 60-day window for setting reserve requirements. When large volatility events drop from the window, load following requirements drop, and the likelihood of events rises. But the addition of load following as a function of load (Cases SC_01-SC_04) is likewise not optimized for cost or reliability either.

It is worth noting that in the majority of the cases studied (all but the 95th percentile case, which carried far less reserves), $LOLE_{INTRA\text{-}HOUR}$ events occurred mostly during the low load, high renewable seasons, where less resources is committed to serve load yet a large amount of intra-hour volatility existed on the system due to large output from variable generations.[45]

Other than reliability, results from these cases show a converse trend in system cost. That is, while carrying additional reserves help mitigate $LOLE_{INTRA\text{-}HOUR}$, it comes at a higher cost as more resources are committed. For instance, the difference in total

44 As described in the Study Case section, the Net Load (NL) observed method sets LF reserves based on the volatility observed in the previous 60 days. For example, the NL 100th percentile (case SC_07) uses the largest volatility observed in the previous 60 days. But even that does not eliminate $LOLE_{INTRA\text{-}HOUR}$, as what is observed on day 61 may be higher than any of those observed in prior days.

45 Also in these cases, a subtle relationship was observed between $LOLE_{INTRA\text{-}HOUR}$ and $LOLE_{CAPACITY}$, where because LF is set at a higher level, the increased use of energy limited resources and commitment of fossil generators for reserves resulted in slightly higher $LOLE_{CAPACITY}$

system costs between the cases with the least amount of load following reserves (SC_05) and the most (SC_04) was nearly $800 million a year.

The Recommendations section further interprets these results and provides a discussion on the level of load following reserves to be considered in planning studies.

4.3 Multi-Hour Flexibility Results

4.3.1 System P_{MIN} Cases

In these study cases, relative to the reference scenario, more or less flexible systems were created by decreasing or increasing the overall P_{MIN} level of the system.

Reliability Results

Figure 4.4 below shows the reliability results measured by the $LOLE_{MULTI-HOUR}$ metric for all the cases.[46]

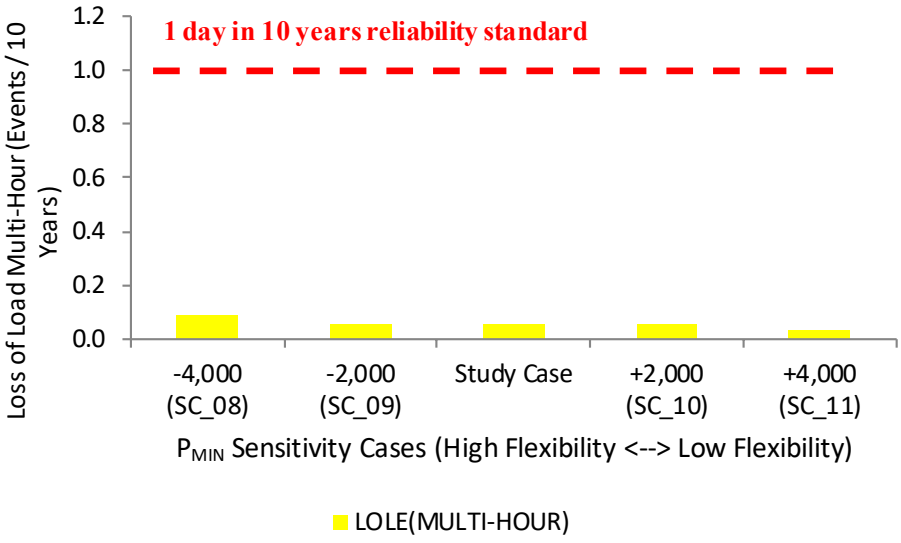


Figure 4.4 Impact of System P_{MIN} on Multi-Hour LOLE

These reliability results show very few $LOLE_{MULTI-HOUR}$ events were detected in all of the cases, indicating the system is physically able to manage the large ramping needs presented in a 50% RPS scenario even under highly challenging situations (e.g., the most inflexible +4,000 P_{MIN} case). Clearly, other sources of flexibility were available to help the system maintain balance. As it turns out, two of the primary drivers are curtailment and net imports.

[46] Recall the $LOLE_{MULT-HOUR}$ metric detects any multi-hour ramping insufficiency, which is the renewable integration challenge most commonly illustrated by CAISO's "duck chart."

Curtailment Results

Figure 4.5 below shows the level of curtailment by case. Results show a sharp increase in curtailment as system P_{MIN} is increased; and conversely, a drop in curtailment as system P_{MIN} is decreased.

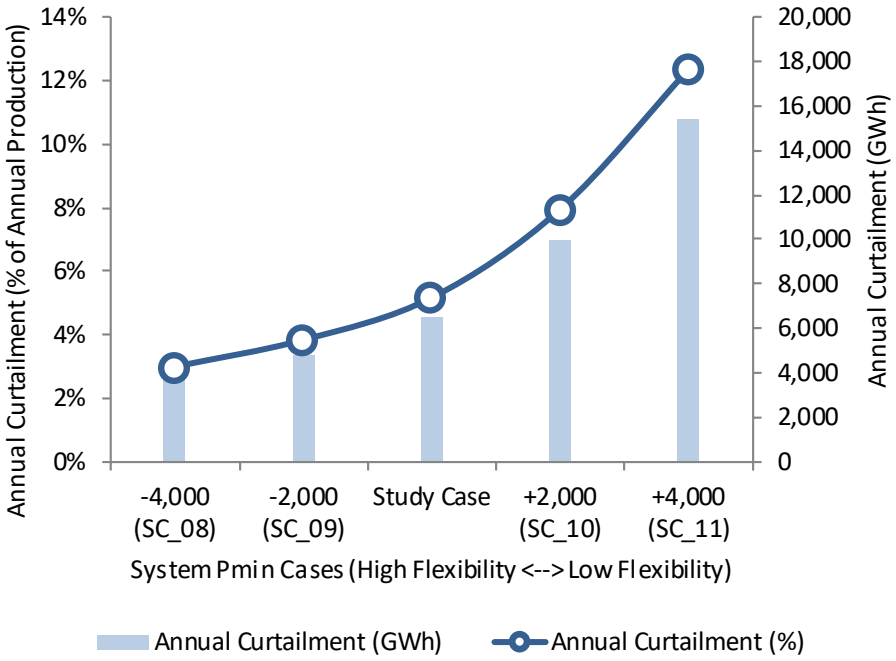


Figure 4.5 Impact of System P_{MIN} on Curtailment

These results revealed a relationship between two flexibility solutions: curtailment and system P_{MIN}. This relationship – incremental reduction in curtailment with reduction in system P_{MIN} – is shown in **Table 4.7** below. These results suggest the marginal curtailment benefit may be a function of the flexibility or inflexibility of the underlying system. In these cases, an additional MW of decrease in system P_{MIN} resulted in much higher curtailment benefit for an inflexible system than a flexible one. For instance, the marginal curtailment benefit of 1 MW of P_{MIN} reduction is 2.8 GWh at the highest level of P_{MIN} studied. This indicates that having lower P_{MIN} would benefit the system 2,800 hours per year when the system is at such a high P_{MIN} baseline. However at lower P_{MIN} baselines, the benefit is much lower. Between -4,000 MW and -2,000 MW P_{MIN}, the marginal curtailment reduction is only 0.5 GWh per MW of P_{MIN} reduction, suggesting only 500 hours per year of benefit.

Table 4.7 Curtailment Benefits from decreasing System P_{MIN}

Cases	Annual Curtailment (GWh)	Incremental Curtailment Reduction between cases (GWh)	Marginal Curtailment Reduction (GWh per incremental MW of P_{MIN} Reduction)

P_{MIN} +4,000 MW (SC_11)	15,447	**5,507**[47]	**2.8**
Reference Case (SC_01)	6,466	**1,664**	**0.8**
P_{MIN} -4,000 MW (SC_08)	3,751	**N/A**	N/A

Net Import Results

In addition to curtailment, net import is another source of flexibility available to the system. **Figure 4.6** below shows the hourly mileage for the +4,000 P_{MIN} case.[48] These results show that the the projected CAISO system is consistently using net import to help balance the daily morning and evening net load ramps, across all seasons of the year.

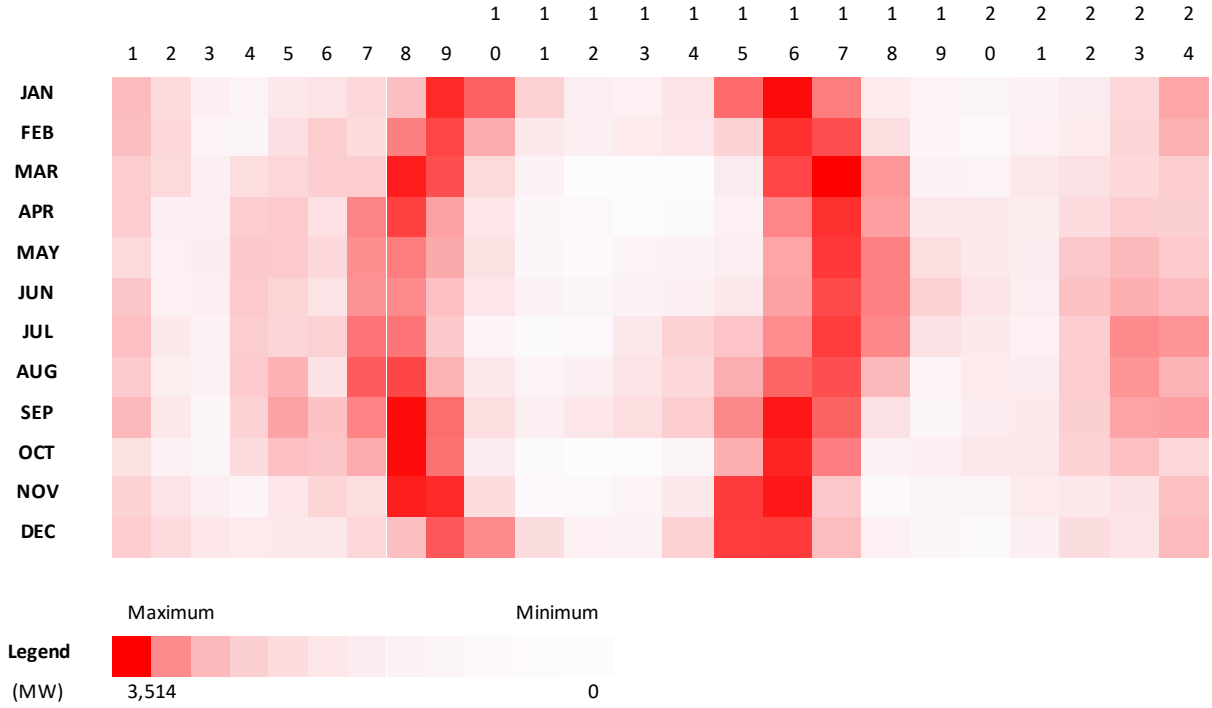


Figure 4.6 Average Hourly Net Import Mileage by Season and Hour (System P_{MIN} Cases)

Whereas curtailment and net import data reflects specific aspects of system operations, total production costs and emissions captures holistic, system level impacts. These results are shown in **Figure 4.7** below.

[47] Here, the incremental reduction between cases SC_10 and SC_11 is 15,447 – 9,940 = 5,507 GWh; and the marginal curtailment reduction is 5,507 GWh / 2,000 MW of P_{MIN} = 2.8

[48] Hourly mileage is calculated as the absolute hourly difference between CAISO net import levels

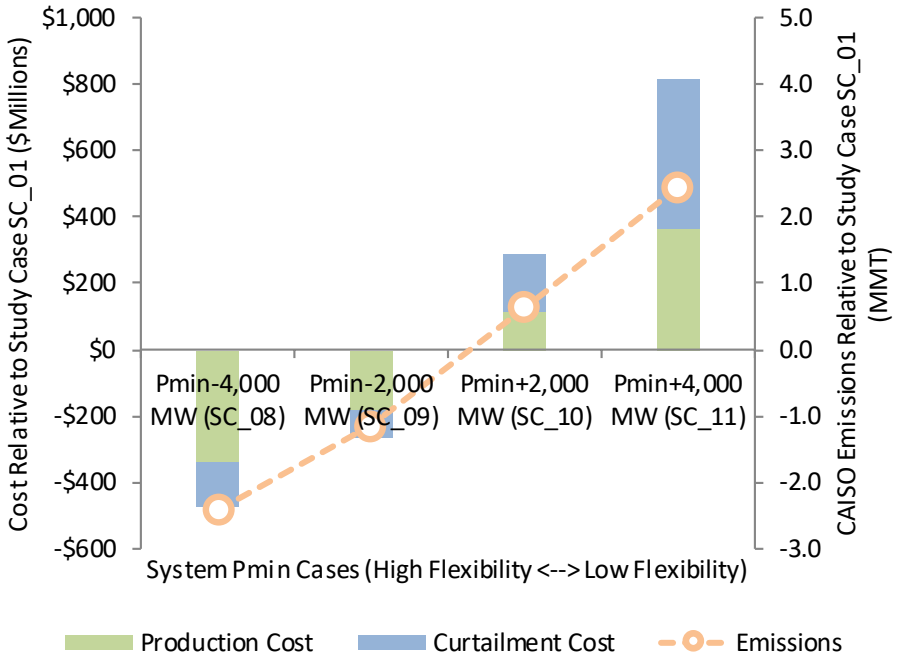


Figure 4.7 Impact of System P_{MIN} on Costs and Emissions

Here, the results confirm that in addition to more curtailments, inflexible systems also incur more production costs (due to inefficient dispatch and commitment of resources) and also produce more emissions.

4.3.2 Interchange 3-Hour Ramp Cases

Relative to the reference study case, these study cases limited the system's 3-hour ramping capability from net imports; thus, decreasing the flexibility of the system.

Similar to the P_{MIN} cases, these results showed a consistent trend between system flexibility, curtailment and system costs. Specifically, as system flexibility is decreased by further reducing the 3-hour ramping capability in each case, curtailments and production costs increased.

For these cases, results also showed the amount of 3-hour ramp from net imports that the CAISO could benefit from under a 50% RPS world. **Figure 4.8** below shows the largest one thousand instances of CAISO 3-hour ramp modeled for the projected 2026 year, for each of the study cases. Also shown in the chart, for comparison purposes, is the historical actual data for the years 2014 through 2016.[49]

As shown by the 9,000 MW and 6,000 MW study cases, these results indicate that under a 50% RPS scenario, the CAISO can benefit from having access to

[49] Actuals are based on CAISO's daily Renewables Watch data

more than 4,000 MW of 3-Hour net import capability for approximately a thousand hours of a year. Restricting that access, as shown by the 3,000 MW study case, severely limits a source of flexibility that the CAISO is already and increasingly relying upon as more renewables are integrated onto the grid.

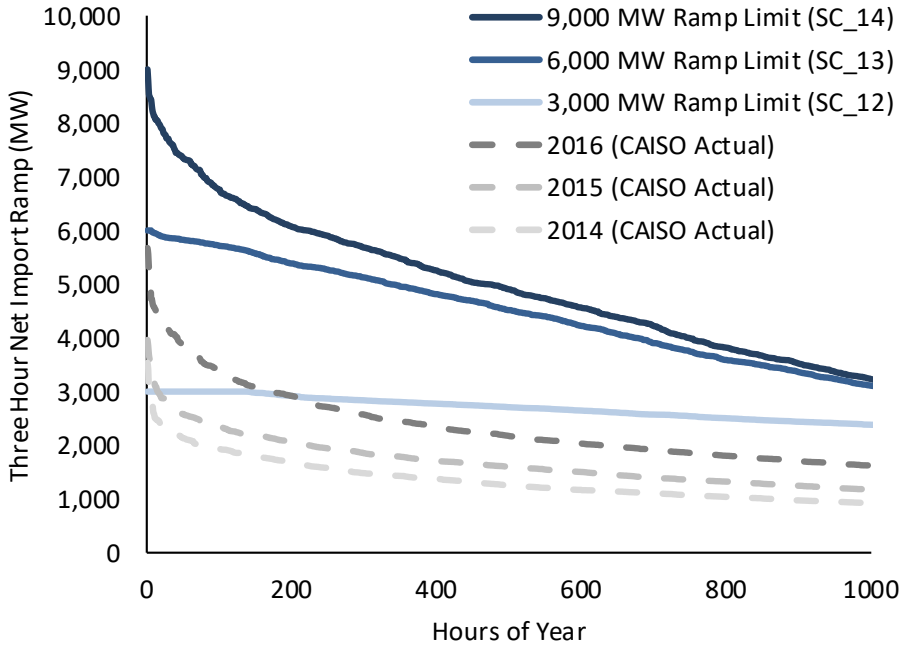


Figure 4.8 CAISO 3-Hour Net Import Ramp (Modeled Results vs. Historical Actuals)

4.3.3 Net Export Cases

Relative to the reference study case, the Net Export cases expanded the CAISO system's ability to export power in over-supply conditions, hence, increasing the flexibility of the system.

Similar to the P_{MIN} cases, results in **Figure 4.9** showed a clear relationship between flexibility and curtailment.

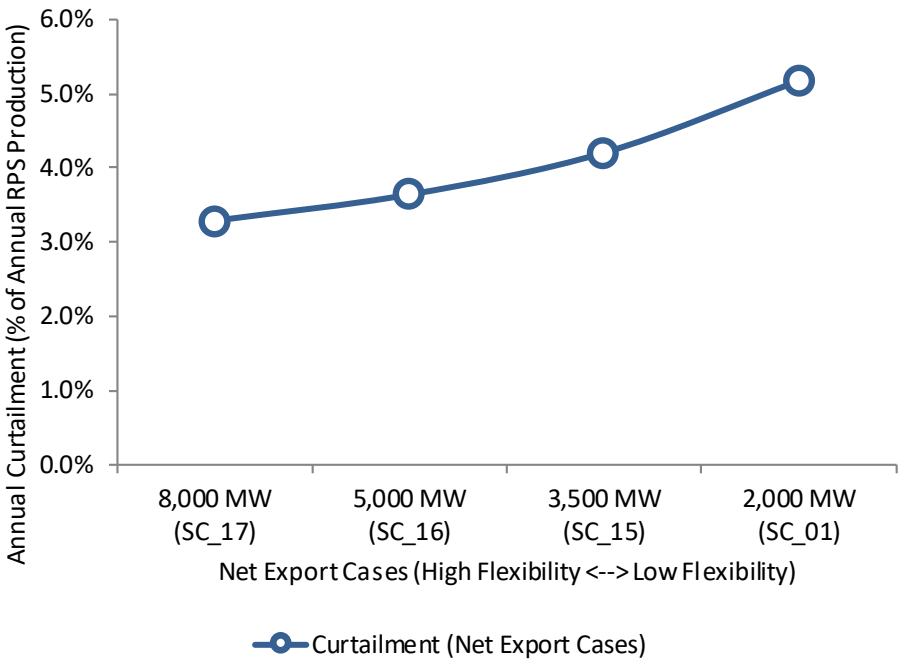


Figure 4.9 Impact of Net Export on Curtailment

Furthermore, **Table 4.8** below shows the magnitude of curtailment reduction as a function of the net export capability.

Table 4.8 Curtailment Benefits from Increasing Net Export

Net Export Cases	Annual Curtailment (GWh)	Incremental Curtailment Reduction between cases (GWh)	Marginal Curtailment Reduction (GWh per incremental MW of Net Export)
2,000 MW (SC_01)	6,470	**1,211**	**0.6**
3,500 MW (SC_15)	5,259	**706**	**0.4**
5,000 MW (SC_16)	4,553	**440**	**0.2**
8,000 MW (SC_17)	4,113	**N/A**	**N/A**

Similar to the P_{MIN} cases, these results indicate a diminishing gain in curtailment reduction as the system becomes more flexible (i.e., further expanding its net export capability). Part of this is due to the observation that the hours when the CAISO is experiencing extreme over-supply conditions at least partially coincides with similar situations in neighboring areas, thus limiting the CAISO's ability to export, regardless of modeled net export limit setting. Again, the marginal curtailment column indicates the utilization of the increased net export capability. Between the highest levels of net export capabilities, the marginal

curtailment benefit is only 0.2 GWh per incremental MW of net export capability. This indicates the increased capability is only utilized approximately 200 hours per year.

4.3.4 Additional Storage Sensitivities

As described in the study case section, two sets of storage sensitivity cases were run.

Capacity Value

The first set of cases focused on understanding the capacity value of storage as more storage is added to the system.

Figure 4.10 below shows the average ELCC value for the entire class of 4-Hour storage as the project team added 3,000 MW, 6,000 MW and 10,000 MW of 4-Hour storage to the CES-21 Reference Study Case (SC_01).

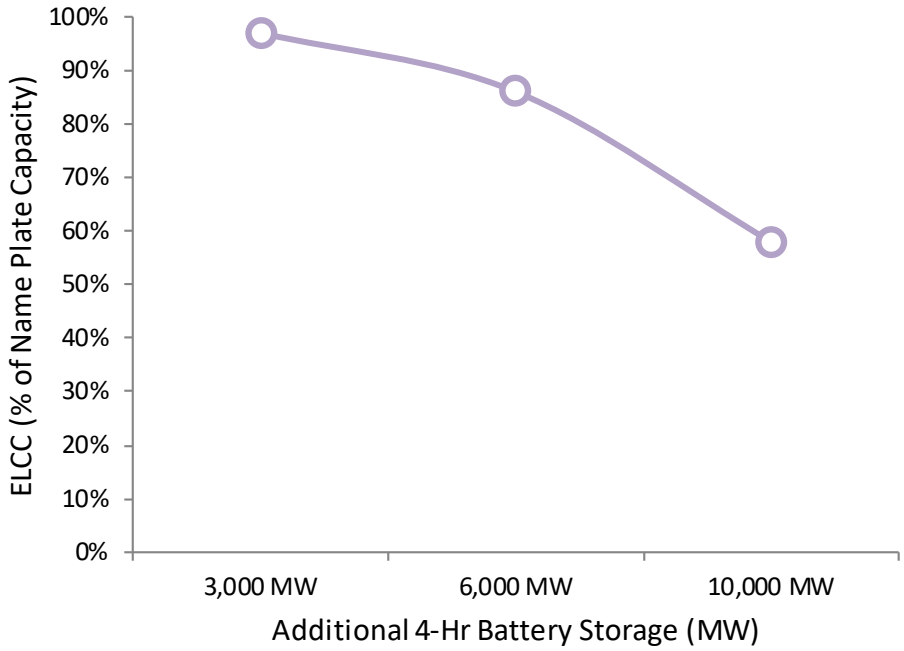


Figure 4.10 Average ELCC vs. Amount of Storage

These ELCC results indicate that adding 3,000 MWM of 4-Hour storage does not affect storage's capacity value. However, as more storage is added to the system, ELCC value for the entire class of storage resources decreases, and in the case of adding 10,000 MW of storage, this class average ELCC can drop below 60%. This is mainly driven by changes in the shape of the peak net load. Storage charges during off-peak hours in order to discharges during peak hours, flattens the peak net load in the process. These results show that if 10,000 MW of storage is added to a 50% RPS system, they will flatten the peak net load so much that a 4-hour battery device can only cover a portion of the peak.

Economic and Curtailment Benefits

The second set of storage cases focuses on understanding the economic and curtailment benefits from storage products of different durations. The economic and curtailment benefits of adding 1,000 MW of storage devices (of various durations) to the 50% RPS reference case are shown below in **Table 4.9** and **Table 4.10**, respectively. These results show a similar trend: for the studied 50% RPS reference system, the marginal economic and curtailment benefit is highest for a shorter duration storage device.

These cases presume that the storage resources can be used to serve ancillary services which do not require significant shifts in the real-time storage level of the resource. This means that a 2-hour storage product can likely serve ancillary service requirements all 24 hours of the day. In comparison, these results show the incremental load-shifting value of increasing the storage capability to 4-hours per day is relatively small (as shown by the more limited opportunity to provide curtailment benefits)

Table 4.9 Economic Benefits of Energy Storage

Cases	Total Benefit ($/kW-year) [50]	Incremental Benefit between cases ($/kW-year) [51]	Marginal Benefit ($/kW-year per incremental hour of storage capacity) [52]
Add 1,000 MW of 2 HR Storage	48	48	**24**
Add 1,000 MW of 4 HR Storage	80	32	**16**
Add 1,000 MW of 6 HR Storage	96	16	**8**
Add 1,000 MW of 8 HR Storage	100	4	**2**

Table 4.10 Curtailment Benefits of Energy Storage

[50] Includes CAISO production cost benefits, net purchase cost benefits, and the economic scarcity rent; does not capture any resource costs.

[51] Represents the incremental benefit from an additional two hour chunk of storage capacity (e.g., the incremental benefit going from a 2-Hour to a 4-Hour storage device is 80 – 48 = 32 ($/kW-year)

[52] Taking the incremental value and dividing it by the two hour block of storage capacity

Cases	Total Benefit (MWh of Curtailment Reduction / MW of Storage)	Incremental Benefit between cases ((MWh of Curtailment Reduction / MW of Storage)	Marginal Benefit (MWh of Curtailment / MW of Storage per incremental hour of storage capacity)
Add 1,000 MW of 2 HR Storage	266	266	**133**
Add 1,000 MW of 4 HR Storage	472	206	**103**
Add 1,000 MW of 6 HR Storage	588	116	**58**
Add 1,000 MW of 8 HR Storage	601	12	**6**

5 FINDINGS AND RECOMMENDATIONS

5.1 Overview

As discussed earlier in the report the main goal of this project was to determine whether there is a need to revise planning standards to reflect the changing conditions of the electric grid. Due to high levels of variable energy resources, there are concerns about whether there is sufficient operational flexibility in the system to manage the increased variability and uncertainty associated with wind and solar power. A well-designed standard is expected to provide a relatively easy to calculate metric that shows whether a system has a sufficient resource mix to reliably meet load, within certain tolerances. While the relative economics are considered when setting criteria for the standard (e.g. whether to set desired reserve margin at 15% or 20%), the calculation on how resources contribute to reliability does not consider the economics of doing so. The economics related to operating the system, and other operational practices, are not usually robustly considered when assessing the system's ability to meet reliability standards since dispatch decisions to ensure reliability will trump normal operational practices or economic concerns. However, this ignores any potential interaction between economic concerns, operational concerns, and reliability. In many conventional systems with predominantly dispatchable resources this approach may be reasonable, but the significant projected changes to the resource mix in California compel a realistic simulation of system operations to determine whether standards should consider operational flexibility explicitly.

Resource adequacy has traditionally been assessed by calculating the risk of not meeting demand, using metrics such as Loss of Load Expectation (LOLE), which determines the expected number of intervals during a given time horizon in which load will not be met.

While this provides a detailed risk-based calculation, this method can be very time consuming and is not easily done especially if multiple load serving entities are making simultaneous planning decisions that impact the overall reliability of an electrical system. To address this other methods have developed around resource needs, with planning reserve margin (PRM) as a common approach. This is calculated as the additional capacity above expected peak demand divided by peak demand, and is required to cover the uncertainty in peak demand forecasting and generator availability in the future year. This can be done using a simple, transparent calculation. Calculated properly, PRM allows for easy comparison across different candidate portfolios, while also being easier to allocate procurement responsibility across different entities, such as the various load serving entities in California. This allocation would be challenging using a LOLE-type approach, so planners need to have a simpler metric to use for this. As computational power increases, solution algorithms improve and data availability improves, even more detailed studies are now possible, as were carried out using the SERVM tool in this project, where LOLE can be calculated explicitly while considering operational flexibility issues. Therefore, when and how PRM can still provide value, especially in light of increased renewable penetration, was a key consideration in this project.

The SERVM results described earlier clearly show that the assumed resource mix studied, up to 50% RPS, has sufficient capacity and flexibility to meet demand in a reliable manner. This finding is subject to several important assumptions as discussed later, including the assumption that operating practices, represented in detail here, will be adjusted to reflect the increased uncertainty in the system at higher RPS penetrations. In terms of planning standards, this suggests there is no need to add additional flexibility-related standards for addressing reliability-related issues. This is not to say that additional metrics cannot be useful indicators, or that economic or market related issues may not result in the need for new metrics; it also does not mean that planning processes used in the past always guarantee sufficient flexibility. Indeed, the introduction of $LOLE_{INTRA\text{-}HOUR}$ and $LOLE_{MULTI\text{-}HOUR}$ show that operational assumptions can affect the calculation of typical reliability metrics and thus there is a need to better consider flexibility issues in reliability studies. However, the study did demonstrate how the continued use of the PRM requires robust calculations of the Equivalent Load Carrying Capability (ELCC) of resources to indicate a reliable system.

Results also investigated the main drivers of the overall reliability of the system, as discussed in the various sensitivities shown. These showed that minimum stable levels of dispatchable generation can have a significant impact on results, while assumptions about how much flexibility can be obtained from the rest of the interconnection can also have a significant impact on the ability to meet load and manage variability and uncertainty in California. The ability to curtail renewable resources was shown to be crucial, while the assumed load following requirements, which drive commitment of generation, can be very important.

These results are mainly focused on the long term needs of the system. However, similar concerns will occur when looking several months to years in advance, as shown by the recently developed Flexible Resource Adequacy Criteria Must Offer Obligation (FRAC-MOO) construct in the CAISO market.[53] Investigating the need for such a construct was somewhat outside the scope of this project, as FRAC-MOO is not just focused on whether the resource mix can provide sufficient reliability, but also on procuring those resources and ensuring they offer flexibility into the CAISO market. However, results here do show that, if the market can access the flexibility available, there is no shortfall in ability to provide flexibility up to 50% renewable penetration.

In general, it was shown that existing planning standards can still ensure reliability, assuming the relevant components are calculated sufficiently. The project's analysis does show a need to consider intra-hour and multi-hour ramps more explicitly in long term planning, but the Planning Reserve Margin techniques developed and used previously can still provide useful indicators of resource adequacy.

5.2 Capacity Adequacy

In the past, PRM was calculated based on adding up nameplate capacity of the dispatchable generation on the system plus the dependable output of variable energy resources, and ensuring they have a specific margin over the expected demand. This study showed that for PRM to continue to serve as a reasonable reliability standard, the process for calculating PRM will need to account for the Effective Load Carrying Capability (ELCC) of all resources with any dispatchability constraint. Therefore, it is recommended that ELCC is calculated based on studies like the ones completed in this project, and revisited when significant changes to the resource mix occur. Results can then be used to inform the PRM, which allows for quick comparison of different plant portfolios. Results would need to be revisited if the portfolio of wind and solar resources changes sufficiently from the portfolio assumptions used in the calculations; this may also be true for demand side resources and energy storage. If the ELCC is calculated as such, then this project found a PRM of 17% appears to provide sufficient reliability to meet the LOLE standard as described above (subject to operational assumptions described later). This study did not explicitly look at how much the wind and solar resource penetration (or any other resource mix changes) would need to change before revisiting the ELCC calculations. Given the rate of change in California's power system, a two to three-year cycle for calculating ELCC contributions of new resources seems reasonable.

In the IRP process, PRM could therefore still be used as a metric to assess resource adequacy, with the ELCC being based on outcomes of detailed studies. The results section shows the results calculated for this system including sensitivities on issues like energy storage; this type of analysis would need to be repeated for any future analysis with

[53] https://www.caiso.com/informed/Pages/StakeholderProcesses/FlexibleResourceAdequacyCriteria-MustOfferObligations.aspx

different underlying system assumptions. There may also be value in the IRP process to determine an ELCC for both existing resources and marginal or new resources since the IRP process is likely to be looking for the best resource to add to the existing system and these ELCC values can vary based on the underlying system and assumptions about operations.

Recommendation #1: PRM is still a useful metric to assess adequacy, but the ELCC of all resources needs to be accurately calculated and used in the calculation.

5.3 Intra-Hour Ramping

As shown in the results, assumptions about the amount of load following reserves required can have a significant impact on the likelihood of having sufficient flexibility available to meet intra-hour load changes. As such, load following requirements need to be carefully understood for future studies. Traditionally, sufficient load following was made available through the day ahead hourly market, and then economic dispatch at time resolutions closer to real time (fifteen-minute market and real time dispatch). Aspects like adding a look ahead in the dispatch and forecasting wind and solar in the real time and fifteen-minute markets also helps increase the amount of available capacity. However, with increasing levels of renewable penetration, explicit load following is often carried in planning studies focused on renewable integration.

With increasing renewable penetration, **Figure 5.1** below shows that there is a significant increase in ramping, particularly when moving from 33% to 43% penetration. Here, the solid lines show the absolute ramping on a daily basis for four different time series – load only, and net load for the three cases. This is calculated by adding up the absolute value of 5 minute ramps in a given day (e.g. if the net load ramped up 20 MW in one period and down 5 MW in the next, the absolute ramping mileage would be 25 MW). The numbers here are less important than the relative changes, as absolute ramping does not impact operations, but does show how much overall additional ramping is required. As shown, renewables add ramping throughout the year. The dotted lines show cumulative ramping – compared to load only ramping, 33% renewables increases ramping by 172%, 43% renewables increases it by 237%, and 50% renewables increases ramping by 259%.

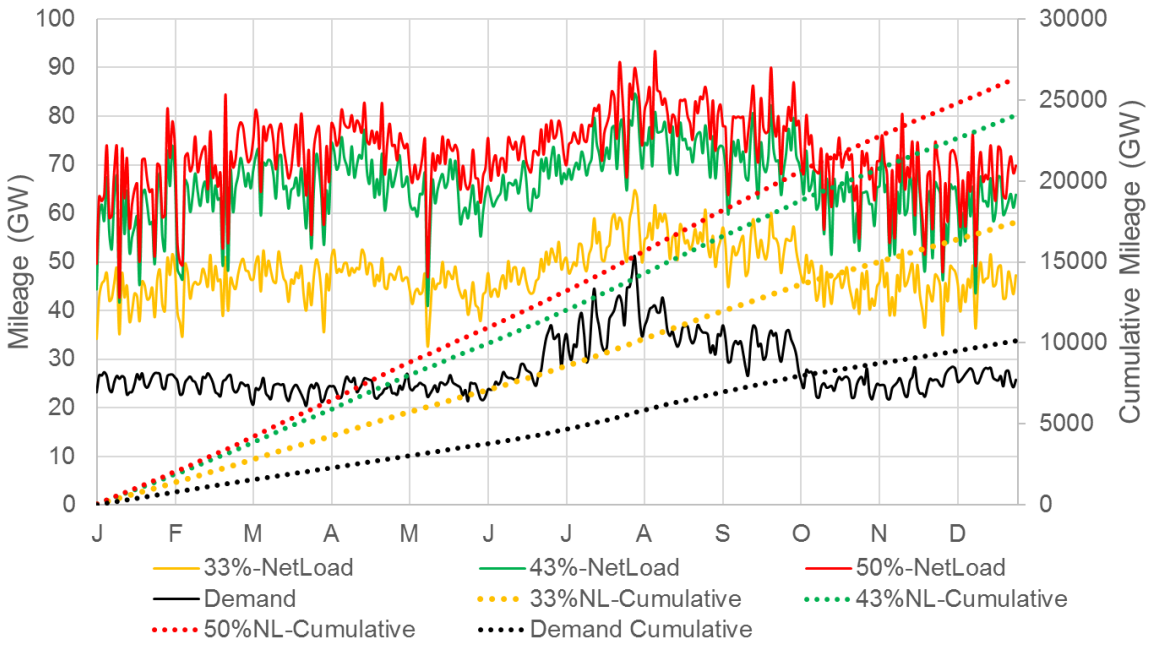


Figure 5.1 Daily and Cumulative Absolute Ramping Mileage for Different RPS Cases

This increase in ramping would be expected to put increased strain on intra-hour load following, and a noteworthy outcome of the studies performed here was that the $LOLE_{INTRA\text{-}HOUR}$ metric was shown to be heavily influenced by the amount of load following carried. This type of LOLE hasn't traditionally been included in reliability studies in the past – as such, it can be thought of as a somewhat new metric, or at least subset of existing metrics, that have been introduced here. The purpose of this, as well as the $LOLE_{MULTI\text{-}HOUR}$ is to look at the ability of the system to meet intra-hour (or multi-hour) ramps. Here, it was decided to continue to use a 1 day in 10 years total LOLE as the standard; however, there may be a need to further consider what the appropriate requirements for the new LOLE standard, or at least these new indicators, should be. Hence, when presenting results, the project team has tended to show both capacity and intra-hour/multi-hour ramping, and then ensure that total LOLE is less than 1 day in 10 years. One could also consider separating out these metrics from $LOLE_{CAPACITY}$, where that metric is still focused on the 1 day in 10 years standard, whereas the new metrics may be assessed against a different standard. Due to the close relationship between $LOLE_{INTRA\text{-}HOUR}$ and operational decisions, this metric can be significantly altered by changing operational decisions, and thus may not be as important as a planning reliability standard. For the purposes of this study, though, it was decided to use the total LOLE as the standard – the assumption being that there is a need to ensure reliability metrics can be met using the planned resource mix.

In actual operations, the operator may decide on some relaxation of the intra-hour flexibility requirements as a trade-off between small Area Control Error deviations (while still maintaining NERC and WECC standards) and lower costs. For example, the

Net Load Observed method used here, while showing a very large $LOLE_{INTRA\text{-}HOUR}$ in comparison to the percentage of load-based load following requirement, is still relatively low in terms of how it compares with NERC and WECC operational standards, where frequency deviation due to small supply-demand imbalances is allowed on a relatively frequent basis. Here, the project team wanted to determine whether the system could meet all variability and uncertainty as well as capacity requirements within the 1-day-in-10 standard. In operations, it will be up to the policy of system operators to determine the appropriate requirements. A final point to note on the introduction of these new indicators is that the current baseline is not known; for example, it may be that while the $LOLE_{CAPACITY}$ of the current system is significantly lower than 1 day in 10 years, when the other LOLE indicators are also included, the current system may already be significantly greater than the 1-in-10 standard. The project team has taken the conservative assumption here that, even with new ways to consider loss of load, the system should still be planned for a 0.1 total LOLE.

The results of the study related to Load Following are shown in **Figure 5.2** below for the 50% penetration cases. The blue dots, and right hand axis show the $LOLE_{INTRA\text{-}HOUR}$, while the orange dots and left hand axis show the costs in billions of dollars. Based on the study results shown in **Table 4.6**, at 50% penetration, calculating load following using the NL Observed method – where short term variability of wind, solar and load variability is considered in calculating the required amounts – is insufficient to ensure that intra-hour variability and uncertainty can be met. Using a percentage of load, and significantly increasing beyond current requirements to 9% of load, can ensure sufficient intra-hour ramp capability is always available. Clearly, there is a cost to this, which needs to be understood more before it comes to operating the system, but these results at least show the future resources on the system (including interchanges) can be operated to nearly always meet load, as well as ramps in load (or net load) levels. The system operators may determine a more optimal method to determine reserve requirements, but results here show the potential cost and reliability implications of varying this target reserve level. Based on the figure, it would appear that there is a "sweet" spot for the modeled system where the $LOLE_{INTRA\text{-}HOUR}$ is sufficiently low, but costs are still kept relatively low, with 25 GWh, corresponding to 9% of load, the amount chosen for the CES-21 reference study case.

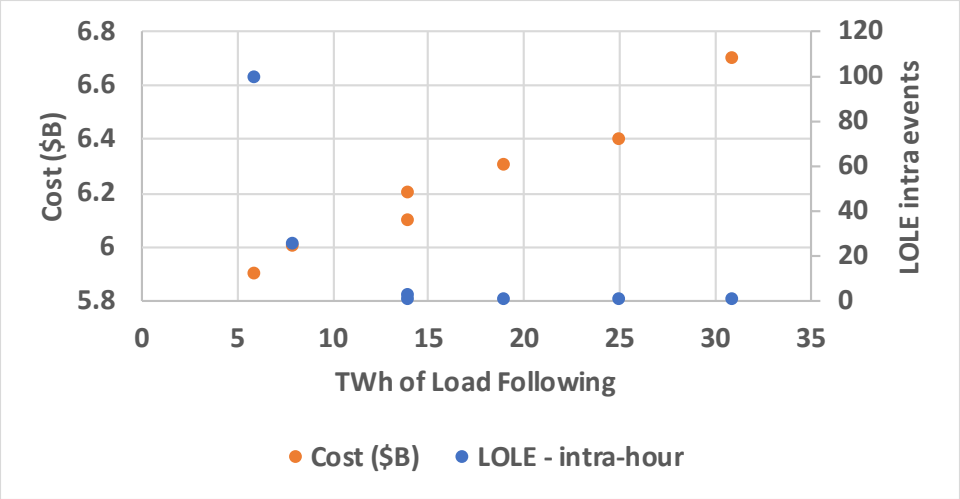


Figure 5.2 Cost and Load Following Impacts of Different Load Following Levels

For example, moving from 14 GWh (corresponding to 5% of load) to 25 GWh (9% of load) increases system operating costs by approximately $300m, but also reduces the intra-hour shortfalls and helps bring total Loss of Load Expectation under 1 event in 10 years. In comparison, using the 99th percentile of net load ramping observed in previous two months increases the intra-hour shortfalls to 25 events in 10 years, but saves an additional $100m beyond the 5% of load case. 25 events in 10 years appears to be a lot; however, the duration and magnitude may be short and small enough respectively to be acceptable as operators determine the actual requirements. As stated earlier, the conservative approach is taken here to ensure the system can meet load at (practically) all times. Another approach would be to study the LOLE of the current system, including intra-hour shortages, and then assume that the future systems being studied will have the same LOLE. Depending on what the actual LOLE may be, this could be either a more conservative or optimistic approach.

Recommendation #2: Sufficient load following capability must be carried in order to ensure intra-hour flexibility sufficiency – and there is a potential tradeoff between reliability and economics in calculating requirements

Recommendation #3: Use of new metrics – $LOLE_{INTRA\text{-}HOUR}$ and $LOLE_{MULTI\text{-}HOUR}$ allow for greater understanding of the flexibility needs and resources. How these relate to $LOLE_{CAPACITY}$ needs to be further considered.

5.4 Multi-Hour Ramping and Flexibility Options

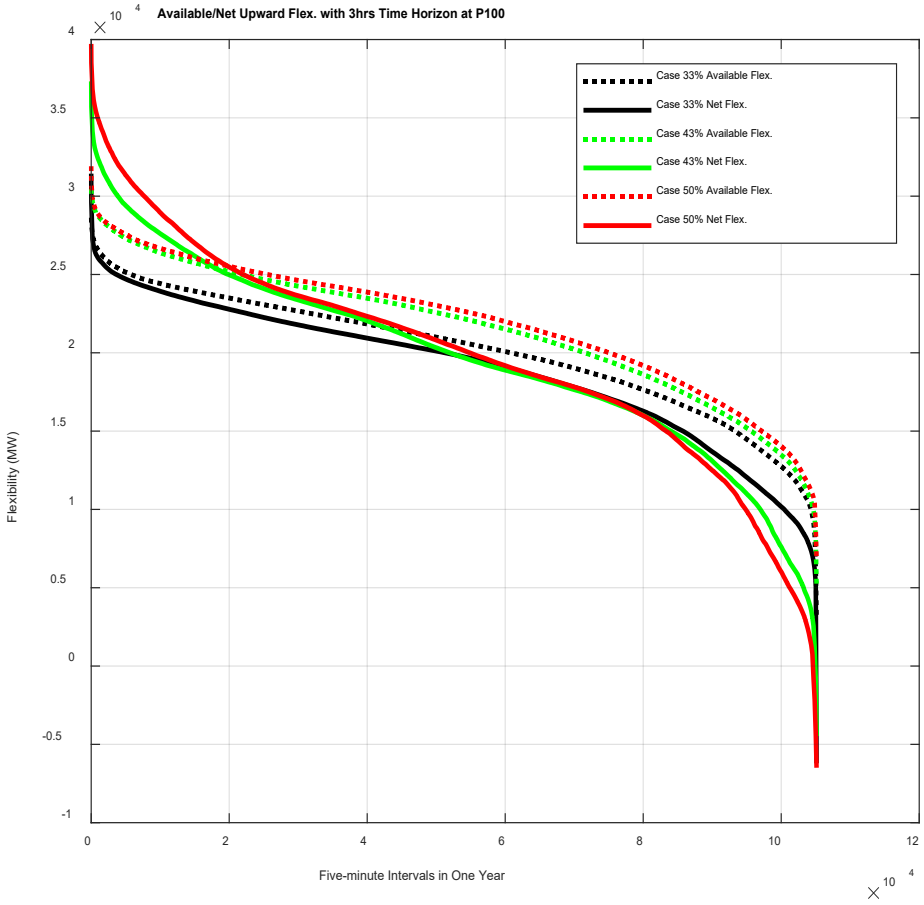
As shown in the results, multi-hour ramping constraints are not as frequently binding as capacity or intra-hour ramping constraints. It was shown that, if sufficient capacity exists, then intra-hour ramping is more frequently a binding constraint in terms of meeting load. No reliability deficiencies were found in most cases because the study assumed imports

and exports can vary hourly, and renewable generation can be economically dispatched[54] or curtailed, to make up the multi-hourly ramping up/down of net load. It was also shown that, in general, reduced multi-hour ramping flexibility has little or no negative reliability impact but a significant cost impact. Reducing flexibility from minimum generation levels, interchange ramping or export limits all have cost and emissions implications. Therefore, careful study of these issues is warranted in any future activities, particularly those related to economic build-out of the resource mix.

Longer duration ramps, from one hour to several hours, have been identified as a potential challenge, and are demonstrated in the well-known CAISO 'duck curve'. With increased renewable penetration, particularly solar, there is a need to ensure that longer ramps can be managed in a reliable fashion. The results here show that, assuming the system has access to renewable curtailment, interchange, and the ability to commit and dispatch all resources in an operational context, that the system can meet longer duration ramps.

The EPRI InFLEXion tool was used to analyze single years for several of the cases in more detail. Below, the amount of ramping available in that interval was calculated based on resource characteristics, with flexibility also available from interchanges based on the same assumptions described earlier; this is shown as available ramping. That was then compared with the potential requirements, which were based on calculating a certain percentile of the ramps observed during similar net load conditions; this is shown as net ramping. (note the actual flexibility available was compared with the largest potential ramp, rather than what actually occurred, such that this is a very conservative answer, and that the net flexibility may be greater than available when no upwards ramping is expected in the period). Even making the very conservative 100th percentile assumption, the number of periods when there were potential shortfalls in the three-hour time horizon were extremely low, with less than 1% of all intervals showing insufficient ramp capability in the 50% case, and even lower amounts in 43% and 33% cases.

54 Variable energy resources can be dispatched by curtailing in advance of upward ramps, then reducing curtailment to increase generation.



Since 2015, the CAISO has been procuring a flexible ramping capacity under the Flexible Resource Adequacy – Must Offer Obligation (FRAC-MOO) program. There, 3 hour ramps are analyzed to determine a requirement by time of day and year, and then resources are procured that must provide themselves as available to the market. It should be noted that the results in this study do not necessarily invalidate the need for that construct, but do show that it is not necessarily needed from a long-term planning perspective if by default all resources provide their respective flexibility to the market. So the construct could still be needed to ensure the market has access to the relevant resources, and that availability to ramp is adequately considered in the market and available to short term operations.

From a long-term planning perspective, the scenarios described in the Results section can provide insights into how different assumptions and potential flexibility options can impact costs, emissions and, in some cases, reliability. From a technical resource flexibility perspective, minimum stable generation levels are shown to be an important source of flexibility. Therefore, as more renewables are integrated into the system, there will be a need to ensure that conventional resources can operate over as wide a range as possible. It will be important not to lose any of the existing flexibility as a reduction in operating range can have a significant impact on results.

Other study cases related to multi-hour ramping provided greater insight into how operational practices and policies can impact outcomes. Curtailment of renewables is shown to be very important to provide flexibility, particularly when flexibility from other resources is reduced; for example, reducing operating range of the conventional resources by 4,000 MW (Case SC_11) from current assumed ranges results in increasing curtailment from under 5% to over 12 %. This system can still be operated reliably, but curtailment is extremely high. Therefore, planning studies should consider curtailment as an option, but need to ensure that it is not overly excessive.

Treatment of interchanges is also an important aspect. Here, the Energy Imbalance Market, and any expansion of the CAISO, are not considered explicitly, but flexibility from interchange is shown to be important. Net import is shown to help balance solar variability in particular; this is already happening in CAISO. As coordination between regions continues to increase in the Western Interconnection, planning studies should ensure that this is considered as a potential source of flexibility, but also that assumptions made are realistic. The results showed that 3-hour interchange ramps are typically higher than what has been observed in recent years, and that limiting ramping on the interchange does have significant cost (and small reliability) impacts. The most expensive system costs produced in this study are for the case where interchange ramp was limited to 3,000 MW in three hours (Case SC_12).

5.5 Use of the Analytical Framework for Further Studies

One important insight from this study was that it showed how detailed modeling, with high temporal resolution, representation of neighboring areas, modeling of the impact of uncertainty on operations and detailed representation of system operations, can provide additional insight beyond more simple models. Models with less of this type of operational detail can often be used to determine potential generation expansion activities, but cannot always provide the insight into both reliability and economics as shown here. One of the outcomes of this study was that it is clear that, on a regular basis, detailed studies informing planning decisions should be revisited. At the same time, there is likely no need to continually evaluate the large range of scenarios studied here, including things like load following, P_{MIN}, interchange ramps, etc. An obvious question is therefore when such studies should be performed, and when less detailed studies can be used.

The example of the storage studies performed here show how this detailed approach can be used to study resource options in the future. As shown there, capacity contribution of storage can be calculated using the modeling approach used, while also looking at aspects such as the economic and renewable curtailment benefits of different levels of energy storage. Duration of energy storage was shown to be important, particularly when moving from very short durations of less than two hours to several hours; beyond a few hours showed less benefit.

In terms of when the studies should be performed, the specific answer is subjective. However, the study provides several potential sufficient changes to require additional studies. An obvious reason would be that renewable penetration being considered has changed sufficiently from previous studies. For example, the difference between the 33% and 50% cases here were significant. Therefore, if moving from one of the scenarios studied here to a higher penetration, or a significantly different mix of wind and solar, one should redo the study. Similarly, if significant changes occur to CAISO operations, then there may be a need to revisit the study; in particular increasing the size of the ISO may be a reason to revisit the analysis as it can have an impact on flexibility available from interchanges. Other reasons to perform similar studies again would be if there are significant changes in underlying conventional resources, such as decreased flexibility from those resources, particularly in terms of operating range. However, with small changes to the resource mix, the need for studies such as this one would not be as great.

6 CONCLUSION

This project has shown a method to assess the costs and reliability impacts of increasing renewable penetrations. A large range of different sensitivities on operational assumptions and flexibility resources are used to understand future system operations. While no new standards are observed to be needed, the methods used here can inform future planning activities, including the IRP. The general recommendations and insights described in the previous section should be considered appropriately when moving forward with planning in California. By reporting on the studies done here, the project team hopes to show how one can study these issues using an appropriate set of tools and data. Further work is described next. It is clear that the detailed modeling performed here could be used in conjunction with the resource expansion models used in IRP. Selecting a subset of potential future cases and analyzing them using the detailed approach described here can provide significant insights into reliability, costs, emissions and what the system operator may need to do to operate the system for the future resource mixes in the IRP.

The study described here was intended as research, and therefore specific numbers for some inputs (e.g. on costs of DR or minimum stable level of generation resources) were based on imprecise data. However, this did not affect the ability of the study to meaningfully analyze, in a research framework, the need for flexibility metrics and standards. As such, the specific outcomes here are less important than the general directional findings. More specific studies on particular aspects would be required if making planning decisions; this project was about developing a framework that can be used to make such decisions in the future.

6.1 Future Work

A number of potential issues were identified that could be further examined, ranging from operational or market assumptions and policy, technical characteristics of the system and data used in these modeling exercises.

From an operational policy, the importance of curtailment to maintaining reliability was shown here, and should be further considered. For example, tranches of curtailment may need to be identified. In the results here, nearly all curtailment can be managed via wind and solar curtailment only, but a handful of hours indicate curtailment above the hourly output of all wind and solar resources. In those cases, there is a question of whether hydro/BTM-PV should be curtailed when RPS is exhausted. More generally, the costs of different levels of curtailment may need to be considered, e.g. curtailment up to a small amount may be relatively inexpensive, but will become progressively more expensive. The framework described here could be used.

Another operational issue is the need to ensure that merchant generation from other regions is available. In reality, long-term contracts and other potential markets may limit flexibility from other regions. While the model here analyzed the entire WECC system with significant detail, it may still need further analysis on the likelihood and potential impact if flexibility is not available.

As discussed earlier, load following requires further study in a number of aspects. The framework used here could be used to study more efficient methods to carry reserves while minimizing costs of doing so. Regardless of costs, there may be a need to consider the load following impact on LOLE, and therefore ELCC of new resources. For example, increasing load following can have an impact on capacity shortfalls; if this is the case, there may be a need to revisit ELCC of the resources causing the need for load following. On the other hand, more thought needs to be given to what the appropriate $LOLE_{INTRA-HOUR}$ should be; this is a new metric so assuming it gets rolled into an overall LOLE needs to be considered carefully.

In terms of technical flexibility, further work is likely needed, mainly to ensure that the assumptions about flexibility resources are accurate; this includes both cost and flexibility attributes. For example, minimum generation level has been shown to be capable of reduction, but at potential capital and operating costs. Similarly energy limited Demand Response resources also have economic parameters that should be more carefully studied.

From a data perspective, the data for intra-hour variability and day ahead and hour ahead uncertainty may need further investigation. Relatively simple methods were used to scale data here, such that the diversity benefits associated with increased renewable penetration (where per-unit variability often decreases due to increased geographic diversity) were not captured in a detailed statistical fashion. The forecast errors assumed

may also need further analysis, to ensure they are reflective of the uncertainty that would actually be seen in operations.

Through collaborative research between PG&E, SDG&E, LLNL, the project team, and the Advisory Group, this CES-21 project has successfully investigated the feasibility of maintaining operational flexibility as renewable generation increases, identified some economic tradeoffs for achieving that flexibility, and provided a valuable tool and framework for IRP stakeholders to quantitatively analyze new planning scenarios as California's electric grid continues to evolve.

Appendix F: Acronyms and Abbreviations

AL	Advice Letter
ATA	Automated Threat Assessment
CAISO	California Independent System Operator
CES-21	California Energy Systems for the 21st Century
COA	Course of Action
CONOPS	Concept of Operations
CPUC	California Public Utilities Commission
CRADA	Cooperative Research and Development Agreement
CTI	Cyber Threat Intelligence
DER	Distributed Energy Resources
DHS	Department of Homeland Security
DoS	Denial of Service
DOE	Department of Energy
DNP3	(ICS spec protocol)
ED	CPUC Energy Division
ELCC	Effective Load Carrying Capability
EMS	Energy Management System
EMV	Exploits, Malware, and Vulnerabilities
FLISR	Fault Location, Isolation, and Service Restoration
HPC	High Performance Computing
ICS	Industrial Control Systems
IKI	Industrial Key Infrastructure
INL	Idaho National Laboratory
IOU	Investor-Owned Utility
IP	Intellectual Property
IRL	Indication and Remediation Language

IRP	Integrated Resource Planning
LLNL	Lawrence Livermore National Laboratory
LOLE	Loss of Load Expectation
MMATR	Machine-to-Machine Automated Threat Response
NERC	North American Electric Reliability Corporation
NERC-CIP BES	North American Electric Reliability Corporation Critical Infrastructure Protection Bulk Electric System
NSA	National Security Agency
OT	Operational Technology
PG&E	Pacific Gas and Electric
PKI	Public Key Infrastructure
PLM	Planning Reserve Margin
PM	Program Manager
QKD	Quantum Key Distribution
R&D	Research and Development
RPS	Renewable Portfolio Standard
RTU	Remote Telemetry Unit
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDG&E	San Diego Gas and Electric
SEIM	Security Information and Event Management
SOC	Security Operations Center
SSP21	Secure SCADA Protocol for the 21st Century
STIG	Structured Threat Intelligence Graph
STIX	Structured Threat Information eXpression
STOTS	Structured Threat Observable Tool Set
T&D	Technology and Distribution
TAXII	Trusted Automated eXchange of Indicator Information
TEPPC	Transmission Expansion Planning Policy Committee
TMA	Threat Monitoring Appliance

TRL	Technology Readiness Level
TTP	Tactics, Techniques, and Procedures
US-CERT	United States Computer Emergency Readiness Team
VMAR	Validation and Measuring for Automated Response
WECC	Western Electricity Coordinating Council