Pacific Northwest
NATIONAL LABORATORY

PNNL-34072

Electric Vehicle Infrastructure Consequence Assessment

February 2023

PR Maloney
J O'Brien
TE Carroll
RM Pratt
LR O'Neil
GB Dindlebeck

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-34072

Electric Vehicle Infrastructure Consequence Assessment

February 2023

PR Maloney
J O'Brien
TE Carroll
RM Pratt
LR O'Neil
GB Dindlebeck

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

With consumers' growing interest in electric vehicles, extreme fast charging stations are poised to provide high-power charging to rapidly recharge light-duty passenger vehicles. High-power charging requires high-level communication between vehicle and charger to govern the charging process. The coupling of power and communication increases the potential scale of cyberattacks. Using a full Western Electricity Coordinating Council planning model, load manipulation from high-power charging infrastructure is investigated. Two cases of load manipulation are studied: (i) a discrete, widespread system event and (ii) loads modulated near the Western Interconnect's resonant frequency. In (i) some generation trips and in (ii) oscillations are observed on the California Oregon Intertie. Neither scenario results in significant adverse effects to the grid.

Electric Vehicle Infrastructure Consequence Assessment

Patrick R. Maloney[a,*], James O'Brien[b], Thomas E. Carroll[a], Richard M. Pratt[a], Lori Ross O'Neil[a], Gregory B. Dindlebeck[a]

[a]*Pacific Northwest National Laboratory, Richland, Washington 99354, USA*
[b]*PSC Consulting, Kirkland, Washington 98033, USA*

Abstract

With consumers' growing interest in electric vehicles, extreme fast charging stations are poised to provide high-power charging to rapidly recharge light-duty passenger vehicles. High-power charging requires high-level communication between vehicle and charger to govern the charging process. The coupling of power and communication increases the potential scale of cyberattacks. Using a full Western Electricity Coordinating Council planning model, load manipulation from high-power charging infrastructure is investigated. Two cases of load manipulation are studied: (i) a discrete, widespread system event and (ii) loads modulated near the Western Interconnect's resonant frequency. In (i) some generation trips and in (ii) oscillations are observed on the California Oregon Intertie. Neither scenario results in significant adverse effects to the grid.

Keywords: , bulk electric system, cybersecurity, electric vehicle charging, extreme fast charging, load drop

*Corresponding author
Email addresses: Patrick.Maloney@pnnl.gov (Patrick R. Maloney), james.obrien@pscconsulting.com (James O'Brien), Thomas.Carroll@pnnl.gov (Thomas E. Carroll), rmpratt@pnnl.gov (Richard M. Pratt), lro@pnnl.gov (Lori Ross O'Neil), gregory.dindlebeck@pnnl.gov (Gregory B. Dindlebeck)

1. Introduction

A recent study [1] has projected significant adoption of electric vehicles (EVs) before the end of the decade. The case for significant EV adoption in the United States is further bolstered by federal and state investments in charging infrastructure, tax credits to incentivize EV purchases, and aggressive state-level zero-emission vehicle mandates. Extreme Fast Charging (XFC), which reduces the time necessary to charge a vehicle, advances adoption as EVs can travel faster and further. High-power charging, such as XFC, employ high-level communication between the vehicle and charger to govern the charger process. Moreover, high-level communication among vehicles, charging infrastructure, and the power grid underlie managed charging and grid services (e.g., smart charging and ancillary services) information and decision exchanges that mitigate adverse charging-at-scale effects and contribute to the stable operation of power grids. Economy-wide transportation system electrification will significantly increase electricity demand and create strong and substantial interdependence between the historically disparate electric supply and transportation systems. This transformation will expand the electric power system attack surface and potentially heightens the risks posed by cyberattacks as an event may bring wide-ranging consequences to vehicles, electric supply, and transportation systems. With these potentially dramatic changes to the electric power infrastructure, new evaluation methods such as [2] to fully consider the implications of these changes, and new IT architectures [3] for greater system awareness may be required to fully analyze and prepare for these new attack vectors.

The purpose of this paper is to explore and better understand potential system wide grid impacts of demand-side load manipulation. The events

in this study assume an attacker has control over all electric vehicle load in the WECC (Western Electric Coordinating Council) and can disconnect and re-connect it at will. The method or access to this load manipulation, however, is intentionally left unspecified so as not to artificially constrain the attack surface. Rather, the focus of the study is if an attacker could gain full control of the electric vehicles (likely as a result of increased network connections to EV infrastructure), what might be the impacts?

Using a Western Electricity Coordinating Council (WECC) planning model, two cases of load manipulations are considered that attempt to mirror the types of events grid operators actually study when evaluating grid reliability and stability. The first event is a single discrete EV load drop event where generation becomes temporarily imbalanced causing system frequency to drift from its nominal value of 60Hz. Typically, a grid operator would study a generation/load imbalance from the perspective of the loss of a single generator which would result in a drop in frequency. However, as the loss of single EV representing a fraction of a percent of system load would unlikely have any significant impact on system frequency for a system as large as the WECC, we evaluate a much more extreme system-wide load drop event in an effort to analyze worste case scenarios.

It is conceivable that a large XFC load loss event could trigger generator protective relaying and cause some generators to go offline. In fact a significant amount of bulk-grid generation resource protection is modeled within the WECC planning case. North American Electric Reliability Corporation (NERC) requirements for generators to stay online during transient events are only applicable to transmission components that meet the bulk electric system (BES) definition [4]. For this reason, only the protections on BES

elements are considered.

NERC Standard PRC-024-2 [5] defines generator frequency and voltage-protective-relay ride-through settings. However, ride-through settings only regulate when generation must stay online. Therefore, we do not assume additional or more restrictive voltage protective settings than what is contained in the original base case WECC planning model. Only BES generator bus frequency and voltage are monitored in this work.

In addition to the discrete, system-wide load drop event, a second case is considered, where the modulation of loads (i.e., alternatively switching loads off and on) targets the grid resonant frequencies. In this scenario, a single load, or potentially many loads at critical locations, are modulated with the purpose of exciting an existing inter-area oscillation mode. Inter-area oscillations on an electric power grid are typically characterized by one set of generators oscillating against a second set of generators through a weak electrical connection at relatively low frequency (0.15 Hz to 1.0 Hz) [6]. The generators oscillating against each other can in turn cause elevated powerflows on the tie lines connecting them.

Inter-area oscillations are of great interest to power system operators and there are examples of them occurring in both the Western Interconnection (WI) and Eastern Interconnection. Consequently there is a need to evaluate whether EV load manipulation could cause this type of event. In 2005, a failed control system at a power plant in Alberta, Canada resulted in a 20 MW peak-to-peak forced oscillation close to the WI's resonant frequency. This forced oscillation resulted in 200 MW of peak-to-peak oscillations on the California Oregon Intertie [7]. Similarly, in 2016, a 200 MW forced oscillation at Grand Gulf Nuclear Station in Mississippi caused a 40 MW

New York tie line oscillation approximately 1400 miles away [7].

With regard to the WI—the system simulated in this work—a variety of modes have been reported; however, the two dominant modes are typically labeled the North-South A (NSA) mode and North-South B (NSB) mode [8]. The NSA mode is a lower frequency mode that primarily involves generators in Alberta oscillating against generators in Southern California and the US Southwest. The NSB mode is higher frequency than the NSA mode and includes generators in British Columbia, the Pacific Northwest, Montana, and Northern California oscillating against generators in Southern California, the US Southwest, and Alberta [8]. A consequence of generators in the north oscillating against generators in the south is fluctuations in the power-flows along the lines connecting the generators. A good location to monitor the power fluctuations caused by the NSA and NSB is along the California Oregon Intertie (COI), a critical WECC path, which is approximately the midpoint of the affected generation. As described in [9], WECC paths are a simplified way of describing flows between regions of a power system; they consist of aggregations of transmission lines transferring power from one region to another. The COI, or path 66, consists of three 500 kV transmission lines that are largely responsible for connecting and transferring power between Southern Oregon and Northern California. Studies addressing forced load manipulation with the intent of adversely affecting the power grid tend to fall into several classifications [10]:

- Static vs. dynamic: Static load manipulation refers to discrete, one-time load modification events, whereas dynamic load manipulation [11, 12] may vary load magnitude through time.
- Single point vs. multipoint: Single-point studies [13] evaluate load ma-

nipulation at a single bus, while multipoint [12] studies allow load manipulation simultaneously at multiple buses.

- Open loop vs. closed loop: Closed-loop load manipulation [13] uses sensors to monitor some aspect of the system state when determining how to change system load, while open-loop [13] load manipulation does not.

Load manipulation studies tend to focus on some combination of design and demonstration of load manipulation methods [12–16] or extend these studies to detection of load manipulation [10] or even mitigation/protection from load manipulation [11, 17–19].

The work in this paper evaluates both static and dynamic load manipulation from both single and multipoint perspectives using an open loop control. The main contribution of this work, and how it differentiates itself from [10–19], is its demonstration of load manipulation on a full WECC planning model (a model actually used by generation and transmission system operators to plan and operate the WECC grid), rather than a test system in an effort to evaluate potential real world impacts. A full WECC planning model differs from the previously listed test models in the following ways:

- Model topology and size: Our studies are conducted on a full 20 000+ bus WECC planning model. The next largest system is in [12], which uses a 179-bus test system.
- Powerflow simulation: This study and [12, 16] use an AC powerflow; the others use a DC powerflow model.
- Standard machine controls: With the exception of [12, 16], [10, 11, 13–15, 17–19] only consider automatic generator control and governor control.

References [12, 16] use standard machine, governor, and exciter models, while this work uses standard machine, governor, exciter, and power system stabilizer models. Exciters are an important control system for maintaining power system stability in that they can be used to automatically control voltage at a generator's terminal [20]. Power system stabilizers (PSSs) also promote system stability, specifically by damping local and inter-area oscillations [21].

- System protection: The WECC planning model contains models for remedial action schemes and standard generation protections. We see no evidence of these models in the other work.

An additional contribution of this work is the proposal of a heuristic for discovering high-impact candidate buses for load manipulation based on frequency response and application of the heuristic to a 2028 EV forecast based on [1].

The primary objective of this work is to better understand the effects of load manipulation, especially due to high-power charging infrastructure, such as XFC, on a large-scale, high-fidelity, realistic representation of the WI. To achieve this, we simulate several load manipulation events on a full 20 000+ bus WECC planning model within transient stability studies that model both real and reactive power, as well as the critical components of a generator's dynamic model, such as governors, exciters, and PSSs. Furthermore, the model receives additional loading based on the EV forecasts developed in [1]. The work in this paper is adapted from [22] but improves simulations by moving simulations to a 2028 system instead of a 2018 system, updates the EV forecasting method to better represent regional differences in EV penetration, and tests both load drop and load modulation

simulations.

The rest of this work is organized as follows. Section 2 describes the model under study and the EV forecast added to the model. Section 3 presents and discusses the results for a discrete load loss event, while Section 4 and Section 5 describe the setup and give results for the load modulation events, respectively. Section 6 concludes.

2. Methods, WECC Model, and EV Forecast

A 2028 WECC planning model is used for both load drop and load modulation studies. The model contains generation and transmission dynamics, along with a high-fidelity composite load model that represents motors, lighting, electronic, and the associated distribution feeders from which they are fed. All major BES elements of transmission protection and remedial action schemes are modeled, including generation protection. For discrete load drop studies, the simulations are observed for 10 s to capture the main features of the initial dynamic response, which include inertia and governor response. Load modulation simulations are conducted over a 50-second interval to allow the effects of low-frequency oscillations to reach an approximately steady-state response.

An EV load forecast is adapted from [1], which projects for year 2028 the electrical demands of 23.6 million EVs distributed nationwide. The 2028 WECC case used in [1] divides load onto 41 different areas typically used in WECC's production cost model simulations. This work creates a mapping to translate the EV load in those 41 different load areas into a new set of 22 load areas used by this work's transient simulations. After obtaining EV load by area for the transient simulations, we scale the size of

the total EV load to match the medium trend given by [1] of 10.8 million EVs nationwide forecasted for 2028. WECC's incremental evening peak load attributed to EV charging in [1] is 18 768 MW. Thus, we calculate our new WECC incremental peak EV load as $\frac{10.8}{23.6} \times 18\,768 \approx 8600$ MW. Thus the new area loads within the transient simulations are comprised of a base case load component and downsized cumulative EV area load component. New EV loads are added to the base case powerflow used by transient simulations by iteratively adding load and solving the new powerflow configuration.

The intent of the studies is to examine any cascading or resulting events that may occur during simulations. Because the size and severity of the scenarios that are studied are far beyond what any operational or planning study would consider, thermal limits and path ratings are not considered.

3. Load Drop Event Results and Discussion

The load drop event consists of dropping the approximately 8600 MW of EV load added to the system. The case is configured with several modifications to transformer tap ratios and automatic voltage regulation after adding the EV load to lower several system initial voltages to get them closer to their nominal values. This same effect might also be achieved with generator redispatch. Frequency and voltages from initial voltage and frequency values at buses containing BES generators (>20 MVA base values) with positive MW output are given in Fig. 1 and Fig. 2. As a result of the 8600 MW load drop, there are some relatively small generator (approximately 30 MW) and load losses (approximately 466 MW) due to their respective generator and load protective systems.

For the discrete load trip results, while we do observe some generation

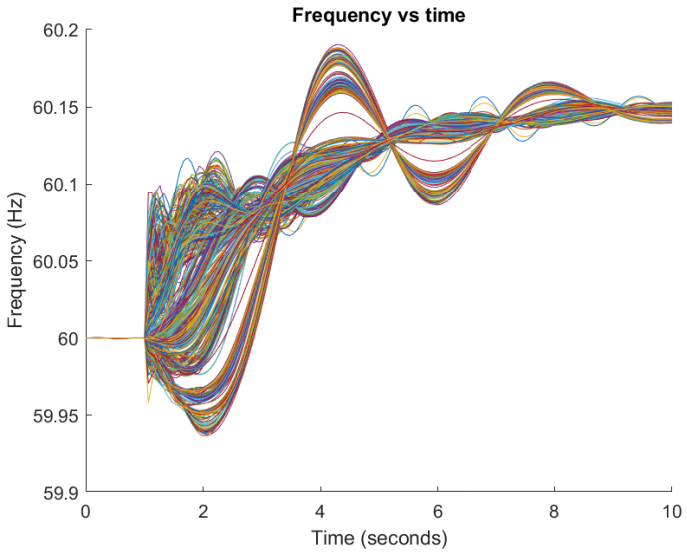

Figure 1: Frequency vs. time.

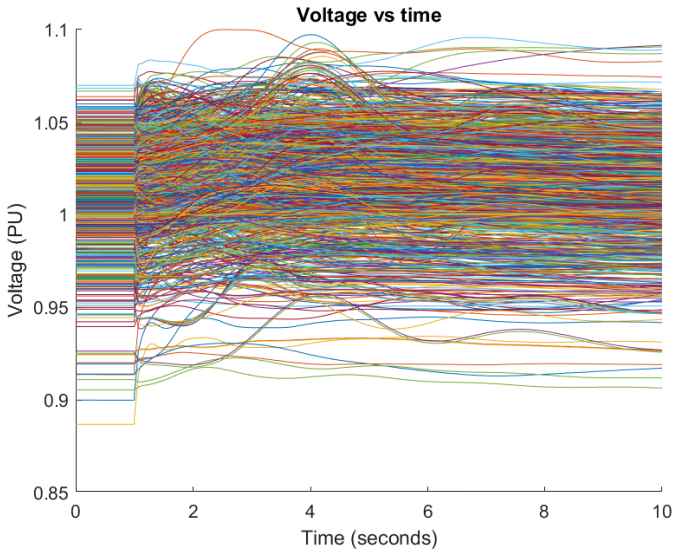

Figure 2: Per unit voltage vs. time.

trips, the generators are small (largest is less than 6 MW) and their absence has negligible effect on the security of the BES. Fig. 1 and Fig. 2 report the system's frequency and voltage response for the generator buses. In terms of frequency, at no point do any bus frequencies approach the BES's lowest over-frequency threshold of 60.6 Hz [5]. With regard to voltage, consider

that the starting case is a heavy summer case, where BES is already stressed. Some of the BES generator bus voltages near the fringe of 0.9 pu to 1.1 pu may be known issues that are allowed to run at higher or lower voltages under close surveillance during peak operating conditions. With regard to Fig. 2, a single voltage just under 0.9 pu actually gets pushed above 0.9 pu by the event.

4. Load Modulation Events Development

The following discussion describes the five-step process used in this work to construct a load modulation event (LME) on the electric power grid. A LME is an event that, instead of simply dropping load, has the ability to switch load on and off. The purpose of modulating load is that the frequency of the modulation can target one of the electric power grid's natural frequencies. This is analogous to pushing a person on a swing: if the pushes are timed just right, a small periodic force can drive the swing to significant deviations from its resting position. Similarly, if the load is modulated at the correct frequency, it may be possible to excite inter-area oscillations. However, there are advanced controls in BES generation known as PSS that will slightly modulate thecite power output of the generator out of phase with a sensed oscillation. In this way, the PSS makes the generator "resist" changes in the system causing a positive impact on system damping.

The process by which LMEs are generated in this work is illustrated in Fig. 3. The remainder of this section details how a distributed LME is developed for analysis in Section 5. By distributed LME, we mean an event where multiple loads are switched on and off simultaneously. Single-load LMEs are also analyzed in Section 5 and are created from a subset of the

steps illustrated in Fig. 3.

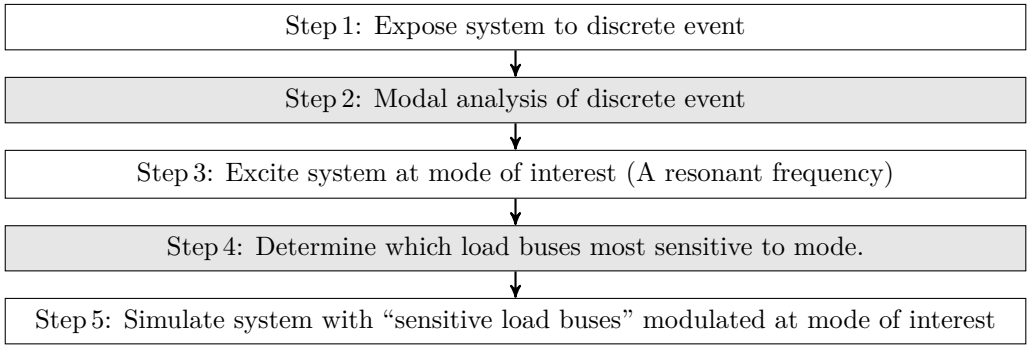

Figure 3: The five-step methodology that is used to construct a load modulation event. Unshaded boxes indicate simulations, while shaded boxes indicate analysis.

Step 1 exposes the system to a discrete event. For this work, a 1000 MW braking resistor is used as the discrete event. The purpose of this discrete event is to create a disturbance that can be further analyzed with modal analysis in Step 2. In Step 2, system modes are determined using PowerWorld's modal analysis tool by analyzing 500 kV bus voltage angle profiles generated in Step 1. Key outputs of the modal analysis include estimates of damping percent, frequency, and the magnitude of the mode's real portion of its eigenvalue. These parameters are used to select a single mode for study in Steps 3–5.

Step 3 exposes the system to a forced 500 MW oscillation. This is accomplished by adding a load to the system and oscillating at one of the discovered modal frequencies. Given the well-known NSA and NSB modes of the WI, we chose a bus in Southern California as this area contains one of the oscillating sets of generators for both modes and has potentially high EV adoption. This initial location is chosen using engineering judgment for an area known to participate in the system modes. However, the intent of

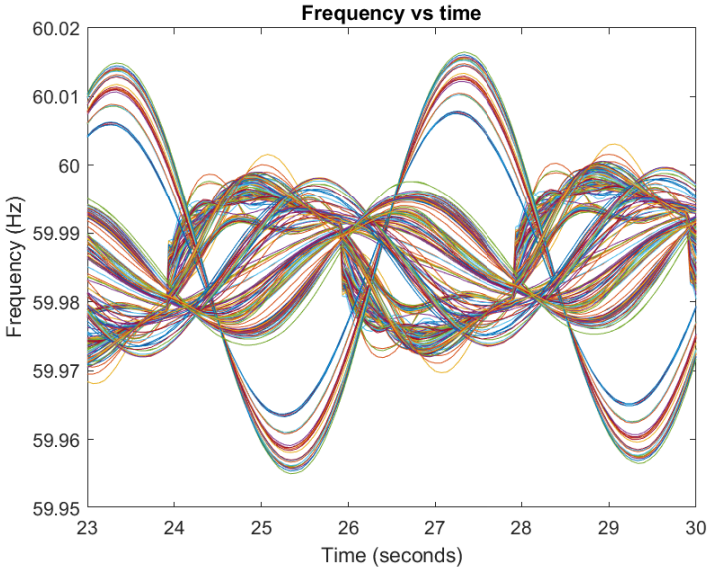

Figure 4: Actual frequency vs. time from Step 3 for load buses >50 MW.

the methodology is to develop a process for selecting candidate buses that best excite the NSA and NSB modes.

Next, in Step 4, the results of modulating a single load are analyzed and load buses for the LME are selected that appear to be most affected by the modulated 500 kV load selected in Step 3. As previously mentioned, Steps 1–3 use engineering judgment to determine where to place the brake and the initial oscillating load. Step 4, however, looks at the frequency response of load buses system wide and ranks them according to the magnitude of their frequency deviations. The buses with largest frequency response to load modulation according to this metric are in Canada. Step 4 also determines the phase angles of the frequency deviations with respect to each other which is useful for determining which groups of generators are oscillating against each other. A plot of Step 3's bus frequency vs. time for load buses is displayed in Fig. 4. In effect, Fig. 4 shows each load bus's response to the oscillating load, where larger frequency excursions indicate that the

bus may be more susceptible to excursions when forced oscillations occur at the resonant frequency. Furthermore, there are approximately 2–4 sets of sinusoids, each oscillating at a different phase angle. We hypothesize that the buses with greatest frequency excursions will also make the best candidates for affecting the grid when modulated at resonant frequency.

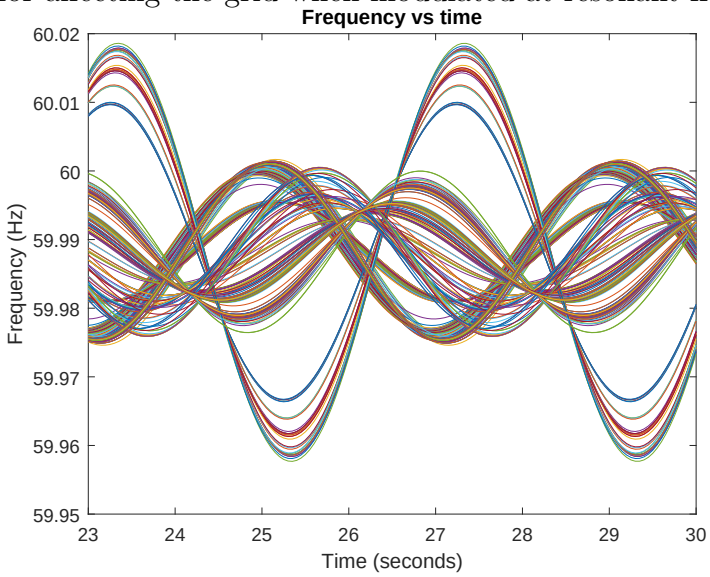

Figure 5: Fit frequency vs. time from Step 4 for load buses >50 MW.

Thus, to construct an LME, it is desirable to select the buses from Fig. 4 that exhibit the largest frequency response from each set of sinusoids. To facilitate this, the raw data of each bus's frequency response in Fig. 4 is fit to the model $y(t) = A\sin(2\pi f_0 t + \theta) + \beta$ using MATLAB's least squares fit algorithm. The estimated parameters of θ and A for each curve can then be used to determine which sinusoidal packet the raw curve belongs to (θ) and the buses with the largest frequency excursions (A). The estimated values of f_0 and β represent the offset and frequency of the curves, but are not used beyond fitting curves to the raw data. The fit curves for a sample time period of approximately 2 cycles are displayed in Fig. 5.

After fitting the raw data to the model, curves are sorted by phase angle.

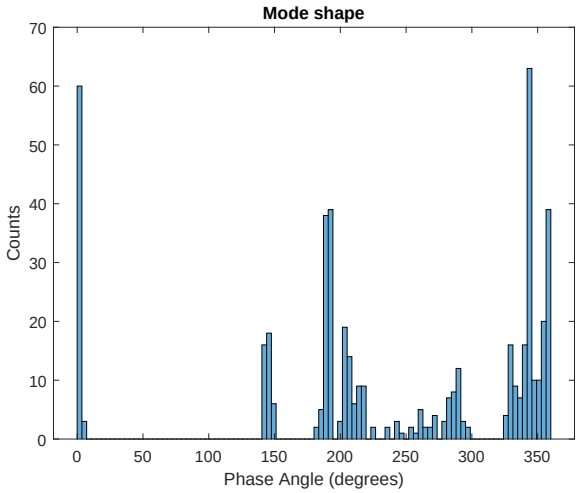

Figure 6: Distribution of phase angles.

As seen in Fig. 6, much of the data is consolidated into two separate groups approximately 180 degrees out of phase with each other. Specifically, Fig. 6 shows that there is a cluster of buses with phase between 340 and 5 degrees and a second cluster of loads between 150 and 210 degrees. Candidate buses to construct the LME are selected by choosing the N loads from each phase group with the largest frequency response.

Finally, the LME is constructed in Step 5 by identifying the loads with greatest fit amplitudes A in each of the two phase groups shown in Fig. 6. The LME is then composed of load at the 10 locations with largest A in each phase group (i.e., 20 total–10 on each end) which are modulated at the resonant frequency determined in Step 2. Each phase group's loads are then modulated 180 degrees out of phase with each other. The results that follow are the Step 5 simulations constructed using this process.

5. Load Modulation Event Results and Discussion

Two different sets of results, with each set composed of three simulations, are described and analyzed below with regard to oscillating load. The simu-

lations in Set 1 correspond to the full WI system using forced oscillations at the same frequency as the NSA mode that, as previously discussed, tends to cause power fluctuations along the COI. The simulations in Set 2 correspond to the WI system with the Alberta system disconnected. This topology modification is selected because it has been reported that removal of the Alberta system tends to simplify the system by consolidating its two dominant modes into a single system mode and decreasing system damping [7, 9]. Furthermore, there is history of Alberta either disconnecting entirely from the WI [7, 9] as occurred in 2000, or being weakly connected to the WI because of tie line outages [9]. The expected location of observation for this mode is again along the COI. The descriptions of the six simulations evaluated in this work are:

1. Simulations on full WI: NS Mode A
   - 1-SLSC (Single-Load Southern California): 500 MW oscillating load at a single Southern California bus.
   - 1-SLFR (Single-Load Frequency Response): 500 MW oscillating load at bus with largest frequency response. This bus is located in Alberta, Canada.
   - 1-DLFR (Distributed-Load Frequency Response): 500 MW of oscillating load at 20 buses, each of size 25 MW. Phase groups in the ranges $140 < \theta < 150$ and $330 < \theta < 350$ were chosen based on several tests.
2. Simulations on WI: Alberta disconnected (combined mode)
   - 2-SLSC: 500 MW oscillating load at a single Southern California bus.
   - 2-SLFR: 500 MW oscillating load at the bus with largest frequency response. The bus is located in British Columbia, Canada.

- 2-DLFR: 500 MW of oscillating load at 20 buses, each of size 25 MW. Phase groups in the ranges $170 < \theta < 190$ and $340 < \theta < 360$ were chosen based on several tests.

A prefix of 1 or 2 in the simulation abbreviations indicate which simulation set it belongs to (for example, 1-SLSC refers to simulation set 1); no prefix means that its general and not specific to either set. While simulation sets 1 and 2 implement the EV loading described in Section 2 to stress the existing system, they relax the requirement of placing the oscillating loads on buses with EV loads. In doing so, the simulations evaluate additional buses for potential issues. In other words, the studies are more conservative than if oscillating load were only allowed at the same location and magnitude as the EV loads described in Section 2.

Both SLSC simulations are developed in Step 3, while the DLFR simulations are developed by the process outlined in Section 4. Fig. 4, Fig. 5, and Fig. 6 correspond specifically to the development of simulation 1-DLFR. While neither of the SLFR simulations is explicitly described in Section 4, Steps 1–4 are used to select the bus that appears most sensitive to force oscillations. In the case of 1-SLFR, the bus most sensitive to forced oscillations could not support an additional 500 MW load, so we placed the load at an adjacent bus capable of supporting it.

The results of simulations 1 and 2 are shown in Fig. 7. *Impact Factor*, defined as $IF = \frac{\text{Peak-to-peak path flow}}{\text{Controllable load}}$, is used to measure the relative increase in power flows along the COI given a specific amount of modulated load. The peak-to-peak path flow is the maximum observed flow minus the minimum observed flow over a 10-second window on the COI, where the system response to the forced oscillation appears to have reached a steady-state

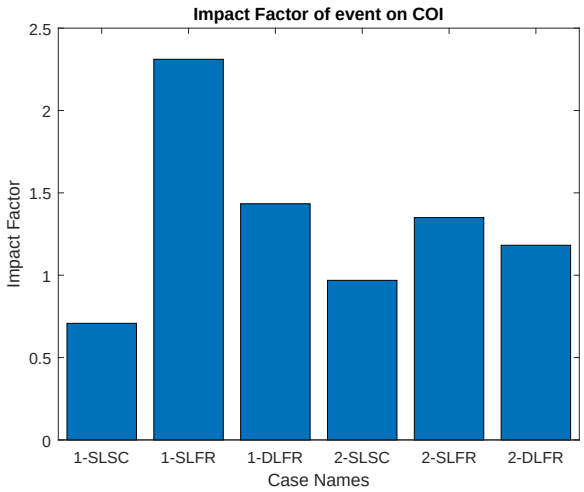

Figure 7: Impact factors by case.

magnitude. Thus, an impact factor of 2 would correspond to a 1000 MW oscillation on the COI given 500 MW of modulated load, while an impact factor of 0 would correspond to a 0 MW oscillation.

SLSC and SLFR add a new 500 MW load at the appropriate system bus. This is done because very few loads in the system are greater than 500 MW. On the other hand, distributed-load simulations and DLFR are modeled by adjusting the load levels of existing loads greater than 50 MW in the system (base loading plus additional EV loads). Additionally, when modulating loads, the desired set points are programmed into the transient stability software but because of the voltage and frequency dependence of load, there are deviations from these set points and sometimes shifts in the range for which the set points are originally programmed. Our work ignore these factors as the simulations are based on the intended load set points.

Generation and load tripped in the distribution-load simulations are tracked in Tab. 1. We observe in 1-SLSC an impact factor of slightly less than 0.75 when choosing a bus in Southern California on which to place the modulated load. However, in 1-SLFR and 1-DLFR, where loads are

Table 1: Summary of generation and load tripped as a result of load modulation.

	1-SLC	1-SLFR	1-DLFR	2-SLSC	2-SLFR	2-DLFR
Generation Tripped	0	0	0	0	0	0
Load Tripped	0	0	22.24 MW	0	0	19.9 MW

selected by the Section 4 frequency analysis method, elevated COI flows are observed. 1-SLFR has the largest impact factor of almost 2.5, while 1-DLFR has an impact factor of almost 1.5. These results support the use of the Section 4 methodology for identifying potentially problematic buses for EV attacks. The methodology is further bolstered when considering that, by just choosing a bus (1-SLSC) that might appear to be a good candidate based on engineering judgment, it is possible to get impact factors less than 1. These results indicate that modulating relatively low levels of load can significantly affect system flows. It should also be noted that, while the focus of this work is to demonstrate that modulating loads can produce significant impact factors on the COI, it was observed that other critical WECC paths had oscillating power flows; however, the COI oscillations were more pronounced.

In simulation Set 2, slightly elevated impact factors are observed in 2-SLFR and 2-DLFR, but they are significantly smaller than those of 1-SLFR and 1-DLFR. In 2-SLSC, an impact factor of slightly less than 1 is observed on the COI when choosing a bus in Southern California on which to place the modulated load. However, in 2-SLFR and 2-DLFR, where loads are selected by the frequency analysis method described in Section 4, impact factors greater than 1 are observed. For 2-DLFR and 2-SLFR, the impact factors are approximately 1.15 and almost 1.4, respectively. This again

lends support to identifying potentially problematic buses for demand-side EV attacks using the Section 4 methodology.

In both simulation sets, placing all 500 MW of modulated load on a single bus has the largest impact factor (SLFR) when choosing buses with the largest frequency response. However, both distributed-load modulation events (DLFR) had a greater impact than choosing a single bus for the placement of the 500 MW of modulated load based on engineering judgment (SLSC) and also resulted in minor load shedding because of the composite load model's internal protection. This lends credibility to being able to adversely affect the grid by coordinating many smaller loads rather than by using a large single load. A distributed event with many smaller loads instead of a single large load is also likely easier to map to real EV loads on the power system.

6. Conclusion

This work evaluates the effect of manipulating forecasted EV loads on a realistic representation of the WI. Two different types of events are explored: a single, large, discrete, simultaneous load drop occurring across the WI and load modulation events using much smaller amounts of load. The second simulation set involving modulating load was tested both with and without Alberta connected to the grid. In both, a forced load oscillation using load is applied to the WI with the intention of inducing inter-area oscillations. Inter-area oscillations are of concern because they put the grid in an elevated state of risk during system events, may foreshadow protective actions [23], and can make it difficult to achieve ideal transfer capacities and optimal power flows [24].

This paper does not find significant adverse effects caused by the scenario events. While there is some generation and distributed-load tripping in the static load drop event and impact factors of ~2.5 on the COI in the dynamic single-point LME, these events do not independently cause significant system-wide cascading outages. The authors recognize that the full space of potential power system events due to controlling load is larger than the study scope. Future work will focus on better understanding the full space of LMEs with respect to EV infrastructure and characterizing the extent of their impact on bulk electric power grids.

References

[1] M. Kinter-Meyer, S. Davis, S. Sridhar, D. Bhatnagar, S. Mahserejian, M. Ghosal, Electric Vehicles at Scale—Phase I Analysis: High EV Adoption Impacts on the Western U.S. Power Grid, Tech. Rep. PNNL-29894, Pacific Northwest National Laboratory (Jul. 2020).

[2] G. Fotis, C. Dikeakos, E. Zafeiropoulos, S. Pappas, V. Vita, Scalability and replicability for smart grid innovation projects and the improvement of renewable energy sources exploitation: The flexitranstore case, Energies 15 (13) (2022). Available from: https://www.mdpi.com/1996-1073/15/13/4519, doi:10.3390/en15134519.
URL https://www.mdpi.com/1996-1073/15/13/4519

[3] M. Zafeiropoulou, I. Mentis, N. Sijakovic, A. Terzic, G. Fotis, T. I. Maris, V. Vita, E. Zoulias, V. Ristic, L. Ekonomou, Forecasting transmission and distribution system flexibility needs for severe weather condition resilience and outage management, Applied Sciences 12 (14) (2022). Available from: https://www.mdpi.com/2076-3417/12/14/7334, doi:10.3390/app12147334.
URL https://www.mdpi.com/2076-3417/12/14/7334

[4] North American Electric Reliability Corporation, Bulk Electric System Definition Reference Document, Version 2 (Apr. 2014).

[5] North American Electric Reliability Corporation, Standard PRC-024-2—generator frequency and voltage protective relay settings (May 2015).

[6] North American Electric Reliability Corporation, Reliability guideline—forced oscillation monitoring and mitigation (Sep. 2017).

[7] North American Electric Reliability Corporation, Interconnection oscillation analysis—reliability assessment (Jul. 2019).

[8] D. Trudnowski, E. Paull, U. Agrawal, R. Elliott, J. Follum, R. Lott, J. Pierre, Modes of inter-area power oscillations in the Western Interconnection (2021). Available from: https://www.wecc.org/Reliability/Modes%20of%20Inter-Area%20Power%20Oscillations%20in%20the%20WI.pdf.

[9] Western Electric Coordinating Council Joint Synchronized Information Subcommittee, Modes of inter-area power oscillations in western interconnection (Nov. 2013).

[10] S. Amini, F. Pasqualetti, H. Mohsenian-Rad, Detecting dynamic load altering attacks: A data-driven time-frequency analysis, in: 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2015, pp. 503–508.

[11] S. Amini, F. Pasqualetti, H. Mohsenian-Rad, Dynamic load altering attacks against power system stability: Attack models and protection schemes, IEEE Transactions on Smart Grid 9 (4) (2018) 2862–2872.

[12] H. E. Brown, C. L. Demarco, Risk of cyber-physical attack via load with emulated inertia control, IEEE Transactions on Smart Grid 9 (6) (2018) 5854–5866.

[13] S. Amini, H. Mohsenian-Rad, F. Pasqualetti, Dynamic load altering attacks in smart grid, in: 2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2015, pp. 1–5.

[14] S. Acharya, Y. Dvorkin, R. Karri, Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?, IEEE Transactions on Smart Grid 11 (6) (2020) 5099–5113.

[15] A. Patel, S. Purwar, Destabilizing smart grid by dynamic load altering attack using pi controller, in: 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2017, pp. 354–359.

[16] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, C. Assi, Power jacking your station: In-depth security analysis of electric vehicle charging station man-

agement systems, Computers & Security 112 (2022) 102511. Available from: https://www.sciencedirect.com/science/article/pii/S0167404821003357, doi:https://doi.org/10.1016/j.cose.2021.102511.
URL https://www.sciencedirect.com/science/article/pii/S0167404821003357

[17] S. Yankson, M. Ghamkhari, Transactive energy to thwart load altering attacks on power distribution systems, Future Internet 12 (4) (2020).

[18] R. Germanà, A. Giuseppi, A. Di Giorgio, Ensuring the stability of power systems against dynamic load altering attacks: A robust control scheme using energy storage systems, in: 2020 European Control Conference (ECC), 2020, pp. 1330–1335.

[19] A.-H. Mohsenian-Rad, A. Leon-Garcia, Distributed internet-based load altering attacks against smart power grids, IEEE Transactions on Smart Grid 2 (4) (2011) 667–674.

[20] T. Wildi, Electrical Machines, Drives and Power Systems, 6th Edition, Pearson, 2006.

[21] P. S. Kundur, Power System Stability and Control, McGraw-Hill, 1994.

[22] J. O'Brien, P. Maloney, U. Agrawal, T. E. Carroll, R. Pratt, Electric vehicle infrastructure consequence assessment–revision 2, Tech. Rep. PNNL-29514, Pacific Northwest National Laboratory (2020).

[23] D. Kosterev, C. Taylor, W. Mittelstadt, Model validation for the august 10, 1996 wscc system outage, IEEE Transactions on Power Systems 14 (3) (1999) 967–979.

[24] J. Lian, S. Wang, M. Elizondo, J. Hansen, R. Huang, R. Fan, H. Kirkham, L. Marinovici, D. Schoenwald, F. Wilches-Bernal, Universal wide-area damping control for mitigating inter-area oscillations in power systems, Tech. Rep. PNNL-27351, Pacific Northwest National Laboratory (2017).

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov