comed℠ AN EXELON COMPANY | Smart Grid

Backup Power Capabilities: A Technical Study

Release Date: 02/25/2026

Prepared For

Commonwealth Edison Company

Prepared By

Argonne National Laboratory

Acknowledgments

This project was developed as part of the Smart Grid initiative within the ComEd Beneficial Electrification R&D Program under internal project number BEPILBKUP. Argonne National Laboratory produced this report for the Smart Grid Team with overall guidance and management from Simitrio Arellano, Rahul Jha, Akansha Jain, Sri Raghavan Kothandaraman, Querida Ellis, and Courtney Anderson. Alongside this, additional acknowledgements would like to be given to the Transportation Technology Office as well as the Smart Energy Plaza at Argonne National Laboratory for assistance in conducting the pilot, along with the Department of Energy for CRADA guidance and approval. For more information on this project, contact BEPilots@ComEd.com.

Legal Notice

The ComEd Beneficial Electrification R&D Program is funded in compliance with state law.

comed AN EXELON COMPANY | Smart Grid

Executive Summary

This project evaluates the potential role of residential, non-grid tied vehicle-to-home (V2H) systems as a resilience resource in ComEd's service territory, with a focus on how V2H backup power could reduce the customer burden of outage events and what technical, operational, and cybersecurity constraints must be addressed before broader deployment. The work combines system-level reliability and value analysis with laboratory testing of a representative V2H backup ecosystem to produce actionable findings for future pilot design and program planning.

Methodologically, the project integrates three complementary components. First, it uses feeder-level outage event data and simulated electric vehicle (EV) driving and charging profiles to estimate how V2H and vehicle-to-grid (V2G) adoption scenarios could change reliability outcomes and outage-related customer costs under a technoeconomic analysis (TEA). Second, it performs controlled laboratory V2H performance testing across multiple operating conditions and test suites to characterize backup transfer behavior, sustained power delivery, efficiency trends, and repeatable reliability limitations. Third, it conducts a cybersecurity assessment structured around National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 and International Standards Organization (ISO) and Society of Automotive Engineers (SAE) 21434 to identify interface-level risks, assess residual risk drivers, and propose program-relevant mitigations.

Results show that V2H can provide measurable resiliency value at the system level, but benefits depend strongly on outage patterns and the share of outages that are "V2H-applicable" for residential customers. Under location specific modeled scenarios, estimated system-wide V2H adoption can reduce system average interruption duration index (SAIDI) materially in high-applicability years and generate non-trivial reductions in outage-related customer interruption costs (including an estimated value on the order of dollars per kWh discharged from V2H during outages).

Laboratory testing finds that backup transfer behavior is typically on the order of minutes but includes rare edge cases where transfer can be substantially delayed. Cases that transition while the vehicle is already in a stable operating state (e.g., active charging) exhibit the most consistent and fastest transfer behavior, whereas non-active cases show wider variability, including a documented long-delay event with a pronounced oscillatory pre-transfer condition. Sustained high-power operation reveals that "nameplate" output is not always continuously deliverable, and that stable continuous output may require operating below peak ratings as well as managing thermal and installation constraints.

Additionally, distinct reliability modes were observed, including intermittent interruptions and a time-based shutdown/timeout behavior that can terminate backup power after a few minutes under some conditions.

The cybersecurity evaluation indicates that residential V2H ecosystems introduce a broad attack surface spanning local commissioning, home network dependencies, embedded web services, and cloud/over the air (OTA) pathways. The assessment identifies a mixture of architectural and procedural risk drivers—particularly around commissioning flows, software lifecycle management (e.g., patch cadence), and customer network hygiene—and provides program-oriented recommendations emphasizing disclosure, secure onboarding, signed updates, and coordinated vulnerability response processes.

Key Findings

1. Modeled system benefits are plausible but highly context dependent. The share of outage events and interruption duration that are "V2H-applicable" varies by year and drives the magnitude of achievable SAIDI reductions and interruption-cost savings.
2. Backup transfer is usually fast, but rare long-delay edge cases exist and matter. Typical transfer delays cluster around minutes, but at least one case required ~28 minutes and exhibited a distinct oscillatory pre-transfer behavior—suggesting that edge-case transfer performance should be treated as a reliability risk, not averaged away.
3. Peak-rated power is not the same as sustainable power. High-power tests show that operation near maximum output can be variable and may not be continuously sustained; improved stability was observed at slightly reduced output, with shutdown behavior consistent with thermal constraints and/or repeatable early interruptions.
4. Repeatable reliability limitations were observed. These include intermittent mid-test interruptions, a distinct time-based shutdown mode which occurred after ~25–30 minutes in an example case), and thermal-related shutdown behavior at high sustained output—each of which may require mitigation via operating envelopes, configuration, and installation guidance.
5. Cybersecurity readiness must be treated as a program prerequisite. The assessment (NIST CSF 2.0 / ISO/SAE 21434 aligned) highlights commissioning/onboarding exposure, software lifecycle/patching dependencies, and interface-level weaknesses that can affect availability, integrity, and customer confidence, motivating clear minimum controls for any scaled deployment.

Recommendations

Future work and any potential program-scale planning should begin by translating observed performance into enforceable minimum requirements: a V2H system must reliably progress to active backup within a defined transfer window under representative residential loads and must sustain operation within a demonstrated continuous-power envelope, not just a peak-rated capability.

Programs should require clear documentation of derating and shutdown conditions and should incorporate installation and configuration guidance that reduces avoidable interruptions and thermal-related trips. Given the observed presence of intermittent interruptions and time-based shutdown behavior, "no-surprises" persistence should be treated as a core requirement, including deterministic recovery steps, clear operating-state indicators, and defined strategies to prevent unintended shutdown during extended outages.

In parallel, cybersecurity should be treated as a gating criterion for any pilot expansion or program integration. At a minimum, scaled deployment should require secure commissioning practices, strong authentication and encryption for relevant interfaces, a robust software update process (including signed firmware and rollback protections), a defined patch cadence, and a coordinated vulnerability disclosure/incident response process. These controls should be articulated as program eligibility requirements and supported by minimal-but-sufficient telemetry/logging expectations to enable troubleshooting and incident triage without over-collecting customer data.