DOCKETED	
Docket Number:	18-MISC-04
Project Title:	Vehicle Grid Integration Roadmap Update
TN #:	224772
Document Title:	Dispersive Comments Docket #18-MISC-04, Vehicle Grid Integration Roadmap Update
Description:	N/A
Filer:	System
Organization:	Dispersive/Richard E. Harrison
Submitter Role:	Public
Submission Date:	9/21/2018 11:21:41 AM
Docketed Date:	9/21/2018

Comment Received From: Richard E. Harrison
Submitted On: 9/21/2018
Docket Number: 18-MISC-04

Dispersive Comments: Docket #18-MISC-04, Vehicle Grid Integration Roadmap Update

Additional submitted attachment is included below.

dispersive™

13560 Morris Road
Suite 3350
Alpharetta, GA 30004

Tel 1.844.403.5850
Support 1.844.403.5851

California Energy Commission
1516 Ninth Street
Sacramento, CA 95814-5512

Ref: Docket #18-MISC-04, Project Title: Vehicle Grid Integration Roadmap Update

Dispersive Technologies, Inc. commends the California Energy Commission (CEC); CA Air Resources Board (CARB); CA Public Utilities Commission (PUC) and CA Independent System Operator (CAISO) for coordinating under the leadership of the CEC to advance plans for integrating electric vehicles (EVs) with the power grid (18-MISC-04).

Introduction
We greatly appreciate the opportunity to offer comments in this docket. We believe the multiple California agencies' action in this manner is both timely and opportune, as growing EV sales and technological advancements will soon pave the way for vehicle to grid (V-G) models across the globe.

This urgency around policy may be more acute in California than in most states, but that is merely a matter of time. Utility commissions around the country will soon have to grapple with this issue, and what California decides is likely to pave the way for the rest of the country in developing the electric grids and transportations systems of the future.

In particular, we appreciate the specific focus on and investigation into:

1) Methods to improve related cyber-security practices to "ensure safe data transfers from malicious attacks" and;
2) Advanced communication and hardware technology standardization and interoperability for the various communications technologies and pathways that will enable successful V-G adoption at scale.

Indeed, the choice of communications solutions to be adopted is inextricably linked to the secure data transfer environment. Both are absolutely essential for promoting widespread and reliable V-G programs that enhance overall the goals of improving grid operations, reliability, and economic efficiency.

We are therefore grateful for the opportunity to offer our views on issues related to the cyber-security and communications protocols that will govern V-G interaction in California.

Dispersive Technologies provides a software platform that delivers ultra-resilient, hyper-secure connectivity for mission critical applications and services. Our

approach combines real-time network performance optimization, monitoring, dynamic adaptation to network conditions and unprecedented levels of data-in-motion security.

The company's experience extends to a broad range of organizations in the financial, military, and electric power sectors. Within the electric power industry, our solution provides asset visibility from bulk systems to grid edge with NERC CIP cybersecurity controls.

We currently provide service to secure SCADA transmissions between independent power producers and the Independent System Operator within California.

Our comments are as follows:

Best Practices
In developing a best-practices approach to cyber-security, several key points should be considered:

- Real-time (or near real-time) visibility to all grid-connected assets that are potentially capable of being hacked is a critical necessity to safe operation of the grid.
- It should be assumed from the outset that adversaries are continuously probing and reconnoitering the entire electric system in a constant search for weakest links. This activity includes both a search for possible points of intrusion and identification of potential capabilities to do harm.
- As demonstrated in the twelve-month interval between the December 2015 and December 2016 cyber assaults on the Ukrainian grid, 'blackhat' capabilities are constantly evolving and improving, creating increasingly leveraged attack capabilities that can assault multiple targets simultaneously.
- As the Department of Homeland Security warning of July 2018 indicated, hackers have likely penetrated multiple U.S. utility networks and are currently believed to be in a preparatory reconnaissance mode.
- Networks of connected EVs - lacking appropriate cyber safeguards - with ability to create bi-directional flows of energy, could create considerable harm to the grid if hacked. With some EVs now deploying battery packs of 100 kWh, and buses at three times that size, the risk of instability and disruption may extend beyond the distribution utility level to the bulk power system. This would especially be the case if an extensive automated attack were to be simultaneously targeted across multiple targets.

An electric vehicle is a means of advanced, cleaner, and more efficient transportation. It is also a mobile storage asset that serves as a potential resource to the grid. At the same time, it is connected to multiple networks.[1]

The critical issue to be resolved here is how to ensure security of a mobile physical asset that can traverse multiple utility service territories and conceivable carry with it enough electricity to power the average household for days (or weeks in the case of an electric bus or truck).

Specific Comments
In this area, we offer a number of observations and suggestions that we trust are helpful to the

[1] These networks may include, but in the future not be limited to: the charging capability; the entertainment system, which may include radio and television; GPS navigation systems; autonomous driving and associated safety systems, remote ignition systems; and functions such as remote-controlled parking app that can be operated by cellphone, and OEM upgradable software (currently offered by Tesla).

13560 Morris Road | Suite 3350 | Alpharetta, GA 30004 | dispersivegroup.com

process of establishing a safe, efficient, and secure means of facilitating V-G integration:

1) It is important to start the evaluation with the asset itself, at the system edge, and to evaluate the entire range of dynamic events to which that the asset may be exposed. These include valuable multiple use cases, as well as various scenarios for misuse that could de-stabilize the grid or damage the EV asset itself.

2) It is important to create a standardized 'fabric' of security regardless of where the asset is, what it is connected to, and the operating mode it is in.

3) One must be able to continuously guarantee the security, integrity, and timeliness of the data moving across any communications systems being employed. Systems must able to quickly identify data that has been corrupted and ensure replacement datasets within specified latencies.

4) It should be assumed that bad actors are constantly probing for vulnerabilities and looking for multiple surfaces to attack. There is sufficient evidence to assume that this is true, and consequently, protocols, systems and tools should be adopted that make assets invisible to those using traditional scanning and discovery tools. It should be assumed that wireless communications are not secure and systems should be designed accordingly.

5) The cyber-secure communications protocol should be as simple and cost-effective as possible, utilizing the network that has already been paid for. This approach also reduces the need for more computer memory (no specialized hardware is required, so you can install on any EV 'head unit.') Setting up a new network would be prohibitively expensive, and it is not necessary.

6) The cyber-security and communications system(s) adopted should be scalable in order to create efficiencies, and they should allow for network interoperability, so that they can work with any communications carrier and be accessed by any number of vendors or operators.

7) It is advantageous to utilize a communications protocol with the same type of security framework that you are bringing into your network control system in order to facilitate scalability and interoperability.

8) It is not necessary or beneficial to add additional communications systems to the electric vehicle. The cyber-secure capability should be added to existing communications networks rather than creating a new system.

9) Information flows for each unique purpose – whether for OEM software upgrades, GPS navigation, entertainment, vehicle-to-grid integration, or other purposes – should be kept pristine and separate. When EVs are connected to the grid, the particular interaction and related data flows should be virtually segmented and kept apart from other communications channels. Thus, for example, power management information would flow across one dedicated virtual network; autonomous driving data would move across another. This approach limits additional potential attack surfaces.

10) Zero trust perimeters, network micro-segmentation, and managed attribution should be mandatory. For example, it should be assumed that smartphones - that may be unprotected – are interacting with vehicle systems. Unless specific communications

13560 Morris Road | Suite 3350 | Alpharetta, GA 30004 | dispersivegroup.com

streams are locked down to an application level, and unless the device and user are authenticated before being given network access, an unprotected cell phone could become an attack vector to compromise the vehicle and the networks to which the vehicle systems connect. Similarly, the IP address of the server to which the EV connects should be protected and details about other connected devices controlled by the server should also be protected to help thwart cyberattacks before they start.

11) The electric distribution system needs to be dynamically segmented based on specific rules to limit potential damage from an adversary's potential attack. For example, a rule could be established that a specific substation will accommodate no more than a specific level of connected V-G capacity. At a given limit, no more EVs would be allowed to connect to the system. Furthermore, if specific segments are compromised, the compromised EVs can be isolated to limit damage and prevent further widespread harm.

12) The system should be able to identify compromised communications streams or aberrant behavior, and should also facilitate identification of compromised assets themselves.

13) The cyber and communications system should allow for interoperability across multiple utility service territories. Each independent network should be capable of incorporating the mobile EV assets into a network of aggregated vehicles up to a desired limit. Each system should have the ability to identify, authenticate, and approve the joining of any new asset to the network.2 By the same token, the system should be able to reject the new vehicle if necessary conditions are not met, segment limits have been reached, or other conditions are not suitable.

14) Given the empirical evidence from the cyber-security field, the system should also operated with the assumption that assets may be compromised all the way down to the chip level, which would create the ability to alter the code in the chip itself. This vulnerability can be mitigated with a call-out only approach that limits communications to trusted devices that are fully authenticated and authorized.

Conclusion

California finds itself in a unique position to lay the groundwork for the successful interaction of the transportation sector and the electric grid. V-G holds the promise for greatly enhancing the power grid of the future, bringing multiple and valuable services to the grid, while further accelerating the adoption of electric vehicles. Realizing this promise requires a robust and dynamic networking capability that meets wide-ranging security requirements, including:

1) Security must extend to all endpoints.
2) EV assets must be authenticated and authorized before they access the network
3) The network must be micro-segmented. Unauthorized flows or frames intended for the secure portion of the network must be discarded.
4) IP addresses of assets must be invisible/blocked. EV asset to server relationships must be hidden.
5) Endpoints (including EV assets and servers) should not be discoverable by the adversary. The detection of one asset should not enable the detection of other assets.
6) All communications should be secured with NIST-recommended cryptographic

[2] It's important to ensure that the connected asset is not a mobile hacking machine whose mission is specifically to compromise the system.

13560 Morris Road | Suite 3350 | Alpharetta, GA 30004 | dispersivegroup.com

algorithms only.

7) The network should implement an Authenticating Control Plane and an Authenticating Data Plane to minimize the attack surface and protect against DoS/DDoS, malware, and ransomware attacks.

At the same time, it is essential to ensure that the communications and cyber-security protocols are cost-effective, efficient and capable of protecting both the electric grid and the mobile assets connected to it. This will require the continued thoughtful and deliberate approach that has characterized these proceedings to date. We appreciate the opportunity to offer comments in this proceeding and we look forward to continued involvement as this process moves forward.

Sincerely yours,

Richard E. Harrison
President and CEO