V2X - Considerations & Conclusions

Version 1.1

08/01/2023

Document History

Version	Description	Date
0.1	Initial Version	06/30/2023
1.0	Final Engineering Version	07/10/2023
1.1	After Edits	08/01/2023

Kitu Systems, Inc
San Diego, California 92111

Table of Contents

1 Introduction

1.1 Purpose

Vehicle-to-Grid (V2G) aims to advance grid resilience and protect the climate by using EVs as "batteries on wheels," tapping their stored energy to balance electricity supply and demand rather than bringing high-polluting peak generators online. V2G is nascent, with a limited number of bidirectional-capable EVSEs and EVs on the market today and poorly defined standards. Unlocking the full promise of V2G will require significant cooperation and momentum across vehicle and equipment manufacturers, power utilities, standards bodies and regulators, EV charging providers, and other industry players.

This document is both an overview of the current state of the EV charging space and Kitu's assessment on what path forward the industry should take. Our stances and suggestions are based on the use of current technologies, minimal disruption of the current EV charging infrastructure, and a preference for market-based solutions where appropriate.

1.2 Executive Summary

Kitu takes the stance that EVs and EVSEs need to be interconnected with the grid for V2X to be safe and stable. This can be done with minimal disruption to current protocol use, and with a change to the default software included in EVSEs at manufacture time which will enable Utilities to ensure discharge occurs safely. The are many ways for discharge programs to be run and to be provided to the consumer, including through OEMs, CPOs, and companies working directly with Utilities. The market can decide which of these provides discharge opportunities to drivers.

1.3 Acronyms

EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
OCPP	Open Charge Point Protocol
OEM	Original Equipment Manufacturer (EV Manufacturer)
CPO	Charge Point Operator (OCPP term, refers to business entity operating EVSE's using OCPP clients)
V2G	Vehicle to Grid
V2X	Vehicle to Everything
CP	Charge Point
CS	Charging Station (same as Charge point)
CSIP	Common Smart Inverter Profile (of IEEE 2030.5)
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
SAE	Society of Automotive Engineers
CPUC	California Public Utilities Commission
CSMS	Charging Station Management System (OCPP term describing system EVSEs' clients connect to)
NIST	National Institute of Standards and Technology
DER	Distributed Energy Resources
DR	Demand Response

1.4 Use Cases

There are three basic use cases that discharge can occur in, although there are many possible variations within each use case:

1. Home: These scenarios are the simplest of the three. Session management and user authentication isn't necessary, proprietary solutions are more common, and remote management is more likely to come from an aggregator already affiliated with a Utility.
2. Private: These scenarios include fleet use cases and private lots such as condo complexes or office parking lots. While this may be very similar to the residential use case for some lots, others will require user authentication and session management making an OCPP solution more likely. Any CPO managing private charging lots that support V2G would act as an aggregator on behalf of the Utilities.
3. Public: These scenarios are generally paid parking and OCPP is common in these use cases. Public charging scenarios are less likely to support V2G charging in the near future.

All the stances and suggestions this document makes consider all three of these use cases.

1.5 Stakeholders

1.5.1 Vehicle OEMs

While most communications between EVs and EVSEs are standardized, every OEM maintains a proprietary telematics connection to the EV itself. Because an EV must agree to discharge, and because most OEMs have a relationship with their drivers, either directly or through telematics, OEMs will likely have an increasingly important role in this space.

EVs allow users to allow or disallow discharge either via their dashboard or through an app provided by their OEM. OEMs can give drivers the option to set preferences based on factors such as time or they may set those preferences remotely on a driver's behalf.

OEMs can send discharge commands to their vehicles, and some OEMs today have discharge or demand response programs already in place. Some OEMs manage these programs themselves, while others will work with telematics aggregators. Telematics aggregators work with many OEMs and provide a single source for remote management and data gathering from many vehicles from different OEMs.

1.5.2 Utilities & Energy Market

Utilities have a responsibility to ensure that the grids they manage are safe and reliable. This means making sure that DERs connected to the grid are consuming and producing energy responsibly, and that generation matches demand. Utilities work with a broad range of companies in the Energy Market, filling a variety of roles. Some companies manage DER assets on their behalf, some enable participation with DR programs on their own devices, and others provide consumers with opportunities to participate in TOU events or respond to power outages with alternate power sources.

Many charging sites today already participate in Demand Response programs provided by various utilities. As V2X discharge becomes more common, Utilities will need to stay involved to ensure that discharge is done safely.

1.5.3 EVSE Manufacturers

Today, EVSE manufacturers on the open market have overwhelmingly chosen OCPP to enable remote management of their devices. This matters because the capabilities of the EVSE are very important for ensuring safe discharge from EVs.

1.5.4 Charge Network Providers

Charge Network Providers, or Charge Point Operators (CPOs), are the groups that operate networks of EVSEs. This document generally uses the term CPO, which is the term used by OCPP. These may be public lots, or private lots, or even home EVSEs in some cases. Today, most large CPOs use OCPP and generally focus on serving drivers and site owners, with participation in the Energy Market being a secondary concern.

The needs of public and private lots, where a single EVSE may be used by many EVs and drivers, are different from most home charging scenarios. Session management, user identification, payment, and other features cease to be necessary in home scenarios. If remote management of home EVSEs is enabled, it can be done by CPOs, or it can be done with an aggregator or EMS who treats the EVSE as another DER.

2 Considerations

2.1 Grid Interconnection

Utilities have a responsibility to ensure grid stability, and end user owned energy resources are potential sources of instability in the grid. California and Hawaii have both codified the use of smart inverter function sets defined in IEEE 1547, providing a clear, tested set of requirements for how inverters should be integrated with utilities. Many other states and countries are in various stages of codifying similar rules.

The alternative to ensuring that smart inverters can execute these function sets based on input from local Utilities is to rely on safety measures built into the grid, meaning uncontrolled discharge could result in local outages or worse.

Beyond support for basic function sets, such as those defined in IEEE 1547, some states or utilities require inverters to consider their location in a topology defined by the utility or an agent working with the utility. Furthermore, effective balancing of the grid may require realtime comparison of data from and dispatching of commands to many different Distributed Energy Resources, such as battery banks, solar, and wind. While this document is primarily focused on the challenge of supporting V2X at the point where the EV meets the EVSE, considering the broader energy ecosystem will help all involved make more informed decisions.

2.2 V2X Security Concerns

2.2.1 Grid as Critical Infrastructure

Electric Grids in the U.S. are considered Critical Infrastructure, under potential threat from adversarial nation-state actors. While this document will not speak to security of the grid today, it should be noted that expanding V2G use cases in the U.S. provide many new potential vulnerabilities.

2.2.2 Potential Threats to Grid Stability in a V2X Environment

In an unregulated discharge environment, every EV and EVSE represents a point of vulnerability on the grid. Additionally, EVs will roam between private corporate networks when using public and private charging sites, giving malicious actors more opportunities to compromise them. If a malicious actor can control a significant enough portion of DERs capable of providing discharge to the grid, with no security put in place by local utilities and their agents, they can severely compromise local grid areas with coordinated timed discharging. The DERs can be compromised EVs or can be compromised EVSEs. If an EV is remotely managed by a CPO, and the CPO is compromised, then their entire network becomes compromised as well, with no additional layer of security to prevent this.

States like New York, California, and Hawaii have already taken steps to make sure this cannot happen by creating rules for all inverters providing energy back to the grid.

2.3 NIST Grid Interoperability Standards

The NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0 is concerned with ensuring that all communications regarding smart grid infrastructure are

managed by testable, certifiable, and well-managed protocols and standards. NIST defines Guiding Principles for Identifying Standards for Implementation, which include, but are not limited to:

- [Standards are] integrated and harmonized, or there is a plan to integrate and harmonize it with complementing standards across the utility enterprise through the use of an industry architecture that documents key points of interoperability and interfaces.
- [Standards are] supported by an SDO or standards- or specification-setting organization (SSO) such as a user's group to ensure that it is regularly revised and improved to meet changing requirements and that there is a strategy for continued relevance.
- [Standards have] associated conformance tests or a strategy for achieving them.
- [Standards] accommodate legacy implementations.

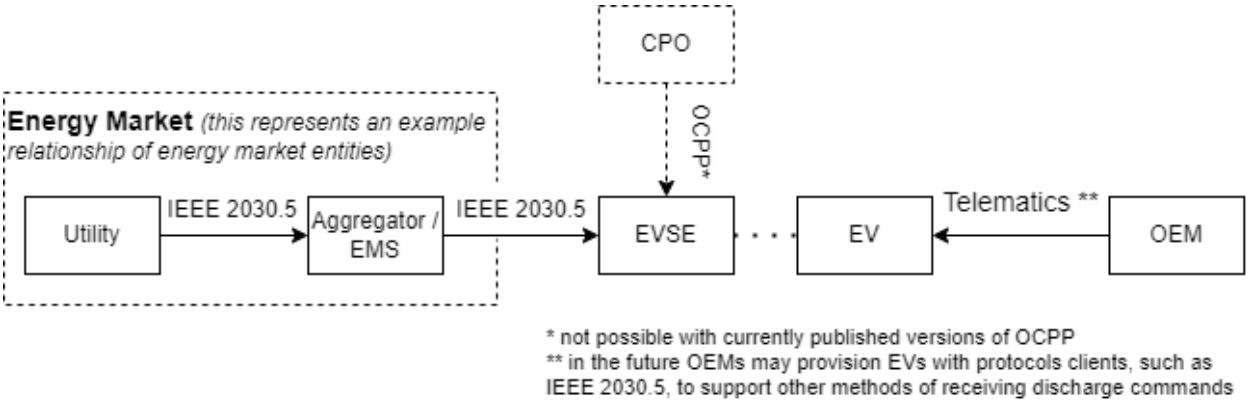
NIST names many ANSI, IEC, IEEE, NAESB, and SAE standards in its identified list of supported protocols. While the most recent publication of this document is from September of 2014, and as such is not completely current on V2X use cases, it does provide a strong framework for evaluating the robustness of standards relating to the grid.

2.4 AC vs DC

While much of the conversation around V2X affects both AC and DC vehicles equally, there is one critical difference between the two. AC vehicles have an inverter that enables charge and discharge in the EV itself while DC vehicles have EVSEs with inverters. This matters because grid interconnection means ensuring inverter compliance with specific function sets. Because specific commands go from the utility to the inverter, this means that there is an additional burden of ensuring communication of grid interconnection functions between the EVSE and the EV in the AC use case. Today, SAE J3072 and IEEE 2030.5 are the two primary mechanisms for accomplishing this.

2.5 Discharge Commands

Grid interconnection isn't strictly necessary in some cases, such as V2H, but discharge commands are. A discharge command tells the inverter in the EV (AC) or EVSE (DC) when to discharge, how much to discharge, and for how long. A discharge command may come from any number of sources such as aggregators, utilities, or OEMs. Please see the following diagram for examples of discharge command paths.



While specific protocols are listed above, discharge commands may come from proprietary sources as well. Unlike grid interconnection, simply enabling discharge is a relatively simple process, and aggregators or CPOs may have their own ways of transmitting commands. Additionally, EVs and EVSEs may have manual discharge controls for consumers to use, especially in V2H cases.

2.6 Agreement to Discharge

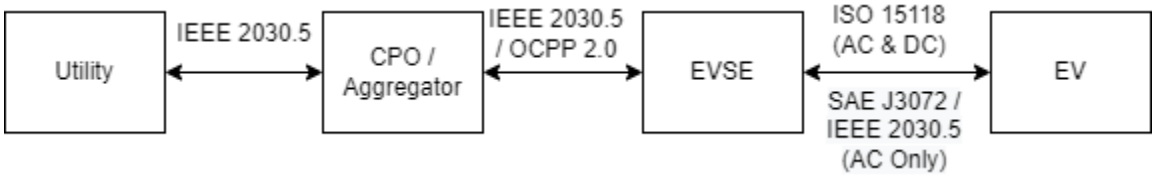
For discharge to occur both the EV and the EVSE must agree to discharge. Either may reject a discharge event, causing it not to occur. Here is some reasons why discharge events may not be agreed to.

- An EVSE may reject discharge if the EVSE isn't integrated with the grid.
- An EVSE may reject discharge if the site owner hasn't allowed discharge on their EVSEs.
- An AC EVSE may reject a discharge event if the EV isn't able to receive IEEE 1547 functions required to support grid interconnection.
- An EV may reject discharge if it's below a given charge percentage or may discontinue discharge if it drops below that percentage.
- An EV may reject discharge because it doesn't recognize connected EVSE.
- An EV may reject discharge because a driver has opted out of discharge through dashboard, or an OEM provided app.

While the above represent several reasons why discharge may be rejected, ultimately the driver needs to consent for discharge to occur. This may happen in the vehicle, through an app, or through an OEM that manages discharge on behalf of the driver.

2.7 Protocols

In this section, we will be discussing standards and protocols relevant to V2X charging concerns. Please refer to the following diagram which outlines where each protocol may be applicable in a simple V2X system. Please note, that this is a depiction of where each protocol could be used in such a system and is a superset of all use cases at once.



2.7.1 IEEE 1547

IEEE 1547 is not a communication protocol. It defines smart inverter functions requirements to support grid interconnection. Many jurisdictions like California's Rule 21 have adopted parts of IEEE 1547 as requirements for interconnection. An inverter compliant with IEEE 1547 must be capable of implementing all these functions. We are using IEEE 1547 as a guidepost for ensuring that any V2X solution can safely integrate with the grid. Please refer to the following table for IEEE 1547 compliance information.

Function Name	**Supported by IEEE 2030.5**	**Supported by OCPP 2.0 / ISO 15118-20**	**Required by CA Rule 21 Interconnection**
Limit Active Power	YES	YES	YES

Function Name	Supported by IEEE 2030.5	Supported by OCPP 2.0 / ISO 15118-20	Required by CA Rule 21 Interconnection
Constant Power Factor (PF)	YES	NO	YES
Voltage – Reactive Power (Volt-Var) Mode	YES	NO	YES
Voltage – Active Power (Volt-Watt) Mode	YES	NO	YES
Frequency Droop Mode	YES	NO	YES
Enter Service	YES	NO	YES
Cease to Energize	YES	NO	YES
Voltage High / Low Trip / Ride-Through / Momentary-Cessation	YES	NO	YES
Frequency High/Low Trip/Ride-Through	YES	NO	YES
Constant Reactive Power (Var)	YES	NO	NO
Active Power – Reactive Power (Watt-Var) Mode	YES	NO	NO

2.7.2 IEEE 2030.5

2.7.2.1 Overview

IEEE 2030.5, or Smart Energy Profile (SEP) Application Protocol, is designed to enable grid integration of the end user energy environment. This includes demand response, load control, time of day pricing, management of distributed generation, electric vehicles, etc. It is based on HTTP/XML and implements a RESTful architecture, defining a flexible client-server relationship.

IEEE 2030.5 supports Demand Response, Load Control, Metering, Flow Reservation, Pricing, and DER management functions, along with others. Additionally, it can support complex topologies of DER resources.

IEEE 2030.5 is part of the Catalog of Standards, which is maintained by the Smart Energy Power Alliance (SEPA) and is defined by the National Institute of Standards and Technology (NIST) as the set of standards relevant for a robust and interoperable smart grid.

2.7.2.2 Use in EV Charging

IEEE 2030.5 does not natively support many charging session management and driver support features commonly found in public EV charging use cases and many EVSE manufacturers don’t support IEEE 2030.5 today.

IEEE 2030.5 excels at DER management, making it especially useful for discharge use cases in charging scenarios. It fully supports IEEE 1547 function sets, which are important for grid stability in discharge scenarios.

2.7.2.3 Security

IEEE 2030.5 uses TLS 1.2 for communications security, and digital certificates for identification and authorization. The standard uses a single, highly secure cipher suite to guarantee interoperability. The cipher suite provides 128 bits of security strength and uses cipher algorithms that are consistent with the more stringent TLS 1.3 requirements.

2.7.2.4 CSIP

CSIP, or Common Smart Inverter Protocol, is a profile of IEEE 2030.5 that grew out of California's Rule 21 and supports "plug and play" communications-level interoperability between DER operators, system integrators, and DER aggregators. CSIP is the 2030.5 profile mandated by the CPUC that implements California Rule 21 interconnection requirements. Any distributed generators, including V2G DERs must comply with it. Even outside of California it provides a robust example of using IEEE 2030.5 to manage inverters across a wide number of actors.

2.7.3 OCPP

2.7.3.1 Overview

OCPP, or Open Charge Point Protocol, is a WebSocket based protocol that enables communication between a Charge Point Operator (CPO) and an EVSEs.

OCPP is primarily focused on charge session management and driver support. It offers user authentication methods including entering identification at device, scanning of RFID cards, and remote identification. OCPP devices also have robust offline user support features, such as offline authorization lists and user caching.

OCPP offers very basic energy management features in the form of its Smart Charging Profiles. While these do allow stacking and scheduling of controls at the device, these only manage active power limit today and can't support IEEE 1547 defined function sets. OCPP does not support discharge commands today.

2.7.3.2 OCPP Versions

OCPP 1.6 and OCPP 2.0 are the OCPP versions in use today. OCPP 2.0 makes significant security improvements to OCPP 1.6, but a widely distributed whitepaper outlines how to use OCPP 2.0 security profiles on OCPP 1.6 systems. OCPP 2.0 introduces support for ISO 15118 communications, which can be used to negotiate discharge and vehicle authentication. OCPP 2.0 does not include any way to initiate discharge today.

2.7.3.3 Security

OCPP 2.0 defines three security profiles, outlined here.

Profile	CS Authentication	CSMS Authentication	Communication Security
(1) Unsecured Transport with Basic Authentication	HTTP Basic Authentication	None	None
(2) TLS with Basic Authentication	HTTP Basic Authentication	TLS auth using certificate	Transport Layer Security (TLS)

(3) TLS with Client Side Certificated	TLS authentication using certificate	TLS auth using certificate	Transport Layer Security (TLS)

Charging Station identity is provisioned on the Charging Station before connection to the CSMS and is appended to the given connection URL to communicate Charge Point identity. No special uniqueness requirements are enforced on Charging Station identities.

2.7.4 ISO 15118

ISO 15118 is a communication interface that enables Plug and Charge between an EV & EVSE by enabling mutual identification and authorization. ISO 15118 defines use cases supporting both charging and discharging but does not support transit of grid codes from EVSE to EV. Because of the lack of ability to transmit needed controls to the EV, this protocol is not enough on its own to support V2X communication between the EV and EVSE.

2.7.5 SAE J3072

SAE J3072 defines how an EV and EVSE can exchange information and negotiate permission to discharge, as well as providing a mechanism by which the EVSE can provide the EV with IEEE 1547 defined controls.

Charge and discharge controls are outside the scope of SAE J3072, so another protocol is needed to send discharge controls to EV. This can be done through IEEE 2030.5 or can be done through the EV itself by driver action or through the OEM via telematics.

3 Conclusions

3.1 Stances

3.1.1 Cybersecurity & Protocol Stability

3.1.1.1 Consumer Safety, Privacy, & Choice is a Priority

It is Kitu's stance that consumer's concerns should be considered a priority in any proposed solutions regarding V2X. Any good solution in this space must speak to the consumers ability to determine if they agree to discharge and that their personal information is not accessible by any parties that they have not given access to.

3.1.1.2 V2G Use Cases May Pose Risks to Grid Security

Allowing private companies exclusive access to controlling discharge events from EVs and EVSEs across the country poses a security risk. Much of OCPP is customizable and does not have a standardized review process, meaning that changes to the spec can happen at any time. Telematics capabilities used by OEMs are mostly proprietary and speaking to their security is difficult. It is Kitu's stance that relying on the good will and vigilance of private companies is insufficient for ensuring grid security.

3.1.1.3 Proper Review and Management of Protocols Affecting Grid Security is Crucial

If the ability to control discharge to the grid is a security concern, then the mechanism of controlling that discharge becomes a potential area of vulnerability. It is important to ensure that any standard or protocol being used to manage communication around discharge goes through a rigorous vetting process. We believe the NIST Framework and Roadmap for Smart Grid Interoperability Standards provides a clear framework for approaching this challenge.

3.1.2 Grid Stability

3.1.2.1 Compliance to Local Grid Interoperability Functions Is a Requirement

Compliance with local grid codes in the U.S. is imperative. While some utilities and states haven't yet codified rules for dispatching to the grid, stability and consistency across a grid increasingly relying on energy from consumer owned sources will be a necessity in years to come.

IEEE 2030.5 is the best tool for communicating grid codes and controls described in IEEE 1547. While some states and utilities haven't yet declared it their standard, no better solutions exist.

3.1.2.2 Grid Interoperability Functions and Charge/Discharge Management Don't Conflict

When fulfilling the role of communicating grid codes to support permission to discharge, IEEE 2030.5 does nothing to impact normal operation of OCPP or ISO 15118. Charging and discharging commands, as well as active power limits, can be handled by other software running on the EVSE, be it OCPP or another solution.

3.2 Recommendations

3.2.1 Universal Adoption of Grid Interoperability Functions

3.2.1.1 Use IEEE 1547 as a Template

We believe that every power grid in the United States should make grid interoperability functions a pre-requisite for discharge to the grid, and that IEEE 1547 should be used as a template for how these functions should be defined.

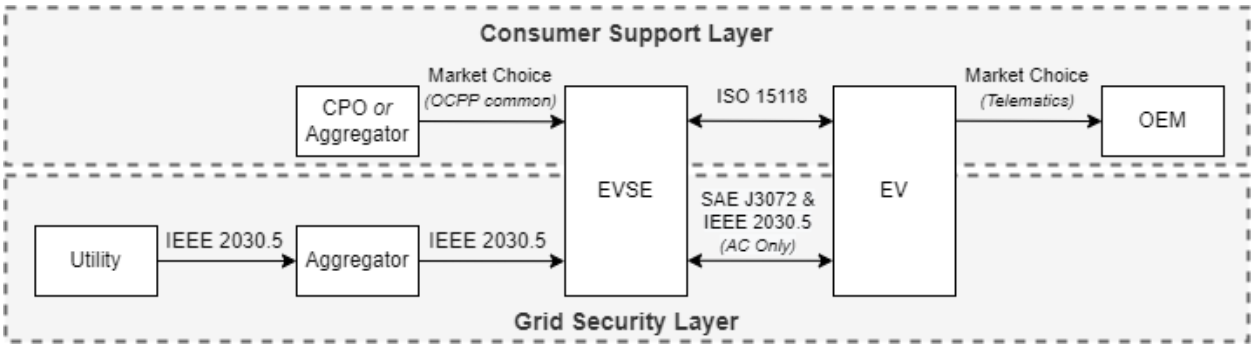
3.2.1.2 National Adoption vs. Individual Adoptions by States, Counties, and Utilities

Grid interoperability functions should be mandated at a national level with implementation left up to individual utilities, states, and counties. Each utility will need to set up its own mechanisms by which it determines how these functions should be dispersed across its service area. This requires the ability to distribute the functions across a complex topology of nodes and devices. IEEE 2030.5 natively supports such complex topology, and feature profiles of IEEE 2030.5 such as CSIP, give specific examples of how utilities can use a network of private entities to securely manage a complex topology of DERs such as this.

3.2.2 Separate V2X Layers of Concern

3.2.2.1 Overview

We are proposing that solutions in the V2X environment be split into two distinct layers, the Consumer Support Layer, and the Grid Security Layer. No changes to existing protocols are necessary to support this distinction, and it is primarily an abstraction to illustrate two separate areas of concern.



All the recommendations we make in the following sections are primarily concerned with securing the Grid Security Layer and enabling market flexibility and consumer safety in the Consumer Support Layer.

3.2.2.2 Consumer Support Layer

The Consumer Support Layer would be market driven, and consumer focused. Applicable regulatory requirements would be those focused on consumer protection, such as California Pricing Requirements for EV Charging Stations. The Consumer Support Layer would manage all the following:

- Permission to discharge given by consumer.

- Any personally identifiable information belonging to consumers.
- Any charge or discharge management performed by Aggregators, CPOs, or OEMs. This includes managing discharge programs themselves.
- Any plug and charge communication between EV and EVSE.
- Any exchange of payment for charging.
- Any exchange of payment for discharge.

3.2.2.3 Grid Security Layer

The Grid Security Layer would be primarily concerned with grid stability and security. No consumer data or interaction with the Grid Security Layer are possible. The Grid Security Layer would manage the following:

- Permission to discharge from Utility, or associated entity.
- Communication of grid interoperability functions to EVSE, and from EVSE to EV.

3.2.3 EVSE Owners Decide Whether to Enable Grid Security Layer on Their Devices

The owner of any EVSE, be they a homeowner with one charger or a business owning hundreds, would be able to configure their devices however they choose. This would mean they could hook their devices up to a local Utility, aggregator, or other source approved for providing grid codes to support discharging. They could then choose to connect their devices to any other entity for the purposes of charge and discharge management.

3.2.4 Mandate IEEE 2030.5 for Grid Security Layer Communication

3.2.4.1 EVSE Manufacturers to Include 2030.5 Clients in EVSEs for Grid Support Functions

IEEE 2030.5 should be provisioned on every EVSE during manufacturing, regardless of what else may be installed on the device. This would not affect any other software on the device, and the other software on the device would not be able to override grid interoperability functions. Only a subset of IEEE 2030.5 feature sets is necessary to accomplish this, and a specific feature profile of 2030.5 might be needed to inform manufacturer installation of these clients.

3.2.4.2 No Consumer Data Goes Through Grid Security Layer

Because the Grid Security Layer is only concerned with transmitting grid interoperability functions, no knowledge of consumer data is necessary.

3.2.4.3 Grid Security Layer Only Concerned with Setting Rules for Discharge to Ensure Grid Stability

The IEEE 2030.5 client installed at manufacturer time is, by design, only used for the purpose of setting grid interoperability functions on the device. This means that discharge still cannot occur if a discharge command hasn't been sent to the inverter, and the consumer has consented to discharge.

3.2.4.4 OEMs and CPOs Unaffected

The existing entities who manage communications to and between EVs and EVSEs would be unaffected by this change. ISO 15118, OCPP 2.0, and the general telematics landscape don't concern themselves with communicating IEEE 1547 style grid interoperability functions, and

these functions don't concern themselves with active power or any other capability already handled by these protocols.

3.2.4.5 Minimal Consumer Interactions in Grid Security Layer

The only interaction any consumer has with the Grid Security Layer is when a site owner decides to enable discharge on their EVSEs. In this case, they must connect their devices to an IEEE 2030.5 server operated by an entity approved by their local Utility. This is consumers only interaction with the Grid Security Layer.

3.2.5 Consumer Support Layer Owns All Other Functionality

3.2.5.1 Marketplace Decides Protocols

We are not making any recommendations about how charge and discharge commands should be communicated, how companies should communicate with consumers, or how EVs and EVSEs should communicate with each other. It is our view that that market has been working on these problems for years and has already started maturing existing solutions.

3.2.5.2 Discharge Programs Owned by Consumer Support Layer

Discharge Programs offer consumers a simple way to interact with discharge opportunities and can be offered by a variety of entities (please see Appendix B for a full examination of Discharge Programs in the V2X space). These programs exist entirely in the Consumer Support Layer as they are concerned with communicating discharge commands, not with communicating grid interoperability functions. This means that OEMs, CPOs, and any other entity interfacing with EVs and EVSEs can run Discharge Programs without hinderance.

3.2.5.3 EMSs and Aggregators in Consumer Support Layer

The terms EMS and Aggregator refer to entities managing DERs in the energy market. These are the same entities that may step in to provide Utilities with a way to distribute grid interoperability functions to various devices. In some cases, these same entities may also offer consumers access to Discharge Programs, TOU or DR programs, or other programs that are part of the Consumer Support Layer. While these entities may operate in both the Grid Security and Consumer Support Layers in some cases, the actions they take in each layer should be considered distinct.

3.2.6 A New V2X Profile

For the recommendations in this document to be actionable, a new profile should be created detailing the following:

- The differences between the Consumer Support Layer and the Grid Security Layer.
- An in-depth examination of role of all protocols and standards required for V2X use cases.
- An overview of the role of all protocols and standards that are common, but not required, for V2X use cases.
- The specifics of implementing IEEE 2030.5 in the Grid Security Layer, including specific instructions for manufacturers installing IEEE 2030.5 clients and Utilities or Aggregators interacting with EVSEs via the Grid Security Layer.
- An overview of the interactions between software in each layer running on a single device.

V2X – Considerations & Conclusions

This profile should comply with NIST grid interoperability standards and should only use published protocols already in use today.

Appendix A: Marketplace Options for Discharge Programs

A.1 Who Runs Discharge Program

A.1.1 OEM Provides Program

When an OEM runs a discharge program, no discharge management capabilities other than IEEE 2030.5 are necessary on the EVSE. If the EVSE is properly set up to discharge to the grid, the actual discharge commands can go straight to the EV. The EVSE may run any additional software it wants for charge and session management.

The communication path for the discharge command to get the EV may come from a variety of sources, depending on what Incentive Programs the OEM supports and what software they have in their vehicles. They may send the command directly to the EV via Telematics, or they may have IEEE 2030.5 client in the EV to receive controls, or they may have some other method of sending discharge commands.

OEMs may offer drivers programs from a variety of sources, such as Utilities, Aggregators, or other energy market entities. The communications pathway to the internet may come from EVSE bridging, Telematics bridging, mobile phone bridging, or any other pathway the OEM provides.

OEMs may choose to provide multiple V2G Programs to their drivers. Prioritization of these programs is ultimately up to the driver and OEM. Driver input is always necessary to allow discharge, but the OEM may choose to prioritize certain programs over others, such as always prioritizing a local utility-run emergency discharge program.

A.1.2 Utility Provides Program

If a Discharge Program is provided by a utility, they are likely to use IEEE 2030.5 to dispatch commands. However, they may be working with intermediaries that convert those commands to another public, or proprietary, communication mechanism before the command reaches the EVSE. The utility may work with CPOs or aggregators to send discharge commands to EVSEs or with OEMs or telematics aggregators to send controls to EVs.

A.1.3 CPO or Third Party Provides Program

Discharge Commands may originate with a CPO, Aggregator, or another entity working in the energy market. They may use any number of methods of transmitting discharge commands to the EVSE. While OCPP doesn’t support discharge commands today, future versions are likely to.

A.2 Where Is Discharge Program Executed

A.2.1 EVSE Executes Discharge Program

If the EVSE executes the discharge program, it means that the discharge command must come from an entity supporting the EVSE directly, such as a Utility, Aggregator, or CPO. The command may originate from a different source.

The EV still needs to agree to discharge. If the EV doesn't agree to discharge, then the command may be active in the EVSE but not being followed. It is the responsibility of the EVSE to determine whether an active command is being followed.

A.2.2 EV Executes Discharge Program

If the EV executes the discharge program, then the OEM is always going to be involved in enabling discharge in some way. They may simply provide a connection to another source of discharge commands natively in the device, or they may provide discharge commands over telematics.

The EVSE needs to be integrated with the grid and compliant with local grid codes for discharge to occur. If the EV receives a command but the EVSE can't support discharge, then the command won't be followed. It is the responsibility of the EV to determine whether an active command is being followed.

Additionally, some programs that OEMs implement may require discharge to specific EVSEs, or EVSEs within a specific area. This may require some way for the EV to verify EVSE identity before allowing discharge. There are several ways to accomplish this. IEEE 2030.5 and ISO 15118 both provide sufficiently unique identifiers that could be used for this purpose.