**IEEE P802.24**

**Vertical Applications Technical Advisory Group**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.24 Vertical Applications Technical Advisory Group | |
| Title | **IEEE 802 Networks for Alternative Fuel Vehicle (AFV) Fueling Infrastructure White Paper** | |
| Date Submitted | 2022-03-12 | |
| Source | Craig Rodine, Jin Seek Choi, Hyeong Ho Lee, Young Kyu Ko, Adedamola Adesokan, Sheryl Drake |  |
| Re: | Additional content | |
| Abstract | < to be added > | |
| Purpose | < to be added > | |
| Notice | This document has been prepared to assist the IEEE P802.24. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.24. | |

# Introduction

The growing adoption of vehicles powered by electricity and hydrogen, instead of traditional fossil fuels like gasoline and diesel, creates the opportunity and need to re-consider fueling processes and infrastructure. The ‘user experience’ of fueling a traditional Internal Combustion Engine (ICE) powered vehicle is very familiar throughout the world. Everything from station locations and hours of operation, to safety precautions and ergonomics; the resources (time and money) required; how to use the dispenser; the units of measure and method of sale, including financial transaction and receipt; are well-known and effectively taken for granted by the driving public. However, many aspects of the fueling experience can and will likely be quite different for the new, non-ICE vehicles.

Throughout this report, the term Alternative Fuel Vehicle (abbreviated AFV) designates Electric Vehicles (EVs) and Hydrogen Surface Vehicles (HSVs), the two leading types of AFVs coming into use.

One significant difference is that AFV vehicles connect to their fueling infrastructure via a coupler that enables analog signaling and/or digital communication between the devices. (By way of wires in the cables used for EV charging, and an infrared link for HSV fueling.) This capability currently supports control protocols that manage the transfer of electrical energy or gaseous hydrogen; in principle, it could be used for other purposes as well.

This whitepaper presents some use cases, requirements, and integration oppor­tunities for AFV fueling that take advantage of mainstream communications capabilities and networking standards, across a range of scenarios and sites.

# Overview of AFV Fueling

This section describes common aspects and characteristics of AFV fueling processes, which may provide orientation to the AFV application domain and enhance understanding of the use cases presented in Section N.

## AFV – Fuel Dispenser Mechanical Connection

Every fueling process requires a means for fuel (liquid gas/petrol, electricity, liquid or gaseous hydrogen) to flow between the dispenser and a vehicle. It’s helpful to refer to this mechanism as a *coupler* with two mating components, an *inlet* (on the vehicle) and a *connector* or *nozzle* (on the dispenser).

The familiar “gas pump handle” used to fuel an ICE can be understood as a simple coupler, with the critical mating feature being the diameter of the nozzle spout and fuel filler neck. (This prevents a diesel fuel nozzle from being inserted into a petrol inlet.) Its control and safety features are mechanical: fuel-tank shutoff, attitude shut-off, a no-pressure-no-flow device, etc. There is no communication – not even a mechanical linkage – between fueling infrastructure and vehicle.

A gaseous hydrogen fuel coupler is similar to the ICE design but more complex, requiring a mating collar with magnet for dispenser activation and a sealing/locking feature for safety, since the gas is under pressure. The HSV specifies its fueling pressure (H35 or H70 service) via one-way infrared communication and can send an ‘emergency stop’ message if the vehicle detects an unsafe condition. (The dispenser can also detect an anomaly and shut down, but it can’t communicate this to the vehicle.)

For *conductive* charging of EVs, there are multiple standards-based couplers designed for manual, ergonomic insertion; almost all use mating pin-and-sleeve (or pin and contact-tube) electrical contacts following the practice and standards for high-voltage electrical plugs and sockets. All DC couplers support mechanical or magnetic locking to prevent arc flash on separation of connector from inlet with high voltage on the contacts. Some AC coupler designs include a locking feature, primarily for physical security (to prevent a charging cord from being stolen) not electrical safety.

EVs can also be charged in a “wireless” manner via induction. For inductive charging, electrical energy is passed over an air gap between coils in the infrastructure and the vehicle. In a typical prototype implementation, the dispenser coil is embedded in the floor or in a moveable pad or platform, and the mating coil is mounted on the underside of the E as shown in Figure X1 [s1]. Mating is done by positioning the vehicle over the pad for optimal energy flow between the coils; this positioning could use automatic vehicle control (e.g. EV autonomous driving capabilities). Naturally the communications used to control inductive charging is also wireless. One system sends control signals on the energy transfer frequency (~25 kHz or 85 kHz), while one prototype used JSON messages over IEEE 802.11/Wi-Fi® for coil geometry compatibility and positioning.

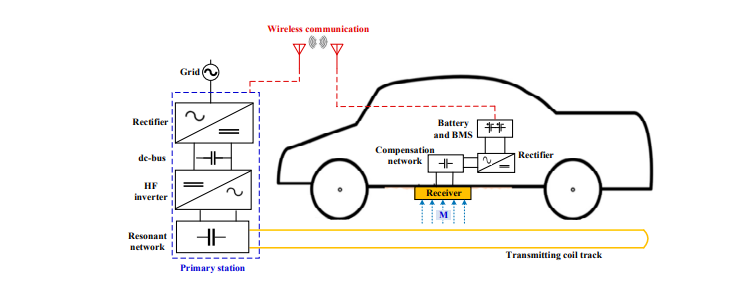


Figure X. EV Inductive Power Transfer Components

There are standards and technologies for robotic control of EV-infrastructure charging using pantograph mechanisms to connect rails or other, multi-pole contact systems to charge e.g. electrific buses as shown in Figure X2 [s2] Such a system can deliver power at high levels, up to 1 MW for 30 seconds or 400 kW for 15 minutes. As for wireless charging, the communications used to engage and disengage the pantograph, do electrical connectivity safety checks, and control the energy flow is some form of wireless, including IEEE 802.11n.



Figure X2. Pantograph charging.

## Energy Requirements and Supply

In conductive based charging, power is supplied to EV battery packs from either AC or DC based charging systems. AC charging uses ubiquitous utility service to power conversion devices (AC-DC converters) on board the EV. In North America, utility service is 117 VAC or 208-240 VAC, both single phase; these are called Level 1 (L1) and Level 2 (L2) AC charging levels, respectively. In Europe the coupler has five pins for power, enabling it to support both single-phase and three-phase AC charging; nominal service voltage is 230 VAC, and most homes and commercial buildings have single-phase service.

DC charging stations are typically powered through the electrical grid distribution devices which supply AC power, thus the DC charging stations must convert the supplied AC power into direct current. Called Level 3 or fast charging, DC chargers are able to supply power directly to the EV battery systems. The AC input power is converted to DC power through multiple steps including AC-to-DC rectification, DC power smoothing and DC-DC conversion which boosts the DC power to the required voltage with parameters specified in standards such as IEC 61851 and IEC 61980. However, there are emerging standards such Charin Megawatt Charging System (MCS) defined in standards including IEC 63379 and SAE 3271. MCS supports higher charging voltage levels up to 1250 DC with the ability to deliver 3000 A of current allowing charging in the megawatt range. With the higher charging rate associated with DC chargers, significant heat can be generated especially at voltages above 200 kW. Fluid (water or specialized coolants) cooled cables are used for DC charges to dissipate heat and provide heat management throughout the cable and charging pin assembly. The coolant is circulated through dedicated coolant channels integrated within the cable and pin housing and recycled though a heat exchanger to remove thermal energy from the system.

As there is energy lost to the conversion of AC-to-DC and the secondary DC power conditioning and boosting, there is interest in using DC power directly as EV charging system input, avoiding this loss. Sources that generate DC voltage natively include Photovoltaic arrays, stationary fuel cells and battery energy storage systems. In such an environment, IEEE 802 communications could be leveraged to offer a communications fabric for the integration, coordination, and control of energy and AFV fueling systems.

## Fueling Session Frequency and Duration

The charging method used impacts time duration necessary, or dwell time to reach the desired battery charge. DC voltage charging is generally considered short dwell, as opposed to AC charging which is longer in duration or long dwell. While dwell time is affected by many variables such as battery chemistry and capacity, start of charge, etc., AC charge time is affected primarily by the voltage of the charger outlet, with Level 1 chargers (120V at 1kW) and Level 2 chargers (240V at 7 – 19 kW) taking 40+ hours and 4-10 hours, respectively. DC chargers (400 – 1000 V at 50 – 350kW) charge time is typically much less, with EV reaching 80% of charge capacity within 20 minutes to an hour, again based on starting charge, battery capacity, temperature, etc.

Use cases and business needs are the primary drivers which determine the method of vehicle charging. Some EV charging equipment is lightly used, delivering one or two charging sessions per day, e.g. 3.5-11 kW AC charging in a residence or workplace. However, others will be used with higher frequency, up to 24-30 sessions per day such as a publicly available charging station or in a heavy-duty vehicle charging site.

## Charging Infrastructure Environments

With the refinement of EV technology and the associated proliferation of EV vehicles in commercial, industrials and consumer areas, there is a variety of EV charging system architectures based upon the specific application requirements. When evaluating network architecture and design for an EV charging implementation, care to numerous factors such as the number and type of chargers needed with the associated power system connectivity and density requirements, as well as, deploying a physical and logical architecture which is robust, secure and scalable. Site assessments include determining site accessibility, physical security, greenfield (new) or brownfield (integrating legacy infrastructure with new charging infrastructure) installation characteristics.

While there are numerous implementation architectures, some common scenarios include:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Location/Use Case** | **Charger Type and Quantity** | **Power**  **Level** | **Cable Length** | **Security** | **Installation Type** | **Wi-Fi Access** |
| Single and Multi-family Residences | Level 2 AC stations | 3-11 kW (240V) each | 5 ± 2 m | Medium | Mostly retrofit, some greenfield | Covered by a single Wi-Fi AP or more |
| Workplaces and High-User-Density Charging Sites | Level 2 AC stations | Tens to a thousand, mostly 6.6 kW (240V), future more DC stations (11 kW) | 5 ± 1 m | - | - | Requires one to many Wi-Fi APs |
| Publicly Accessible Facilities (Urban/Suburban Fueling Stations, Parking Structures, Highway Rest Stops) | DC Charging, multiple stations, short dwell | High-power delivery | - | - | - | - |
| Fleet Vehicle Depots (Privately and Publicly Owned) | Long-dwell L2 AC for overnight services (fleet, postal, school district); Short-dwell DC for taxi pools, etc. | - | - | Higher physical and logical | - | - |
| Highway-side Fueling Facilities for Long-Haul Trucks | High capacity, High-voltage DC Charging | Extremely high-power delivery | - | - | - | - |

## EV Charging Infrastructure Communications

Initiating a charging cycle from an EV to a charging station involves the exchange of information between multiple car systems components and the charging infrastructure to provide both the monitoring and control of the charging session and the authentication and billing for the charging service provided. During a charging cycle, once an EV is connected to a charge cable or is in physical proximity to an inductive charger, several authentication steps must be performed prior to the transfer of electric energy to the car. For public charging, the station may require authentication of the EV vehicle and/or driver to process payments and allow for the charging service to commence. Once authorization has been approved, the communications and handshaking begin between both the EV and the charging station to negotiate the charging level based upon both the capabilities of them both. After the session and power negotiations are complete, the charging of the EV batteries can begin where an on-board converter within the EV converts the charging station from AC (L1/L2) power to DC power which is required for battery energy storage. In the case of L3, or fast charging, the DC power supplied by the charging station can be directly stored in the battery without conversion. Throughout the charging session, charging status, battery health and energy usage are monitored and when the charging is complete, final handshaking between the EV and the charging station is completed regarding the session with billing and payment information shared between the customer and the charging system operator if applicable.

To accommodate this process there are several communications protocols which control various aspects of each of the charging session stages. Within the EV itself there are several communications system in place which control the powertrain and charging systems with many manufacturers using the CAN bus (Controller Area Network) protocol or vendor specific variations for communication between these various electronic control systems. Upon connection from the EV to the charging station, the IEC 61851 protocol is used to exchange data regarding charger and EV capabilities, the authentication and authorization processes, power negotiation and charging control. ISO 15118 provides similar functions including the frameworks for plug-and-charge (PnG) functionality and billing data communications. From the EV charger station to the charging operator and management system, Open Charge Point Protocol (OCPP) gives an interoperability standard used to manage and monitory the charging session including user identification, authorization and billing information. The various protocols required to manage the charging sessions rely upon a reliable layer 2/3 transport utilizing IEEE 802.3, 802.11 and 802.15 protocols to communicate data dependent upon the specific implementation. Additionally, 802.1X can be used to augment the security aspects of IEC 61851 and ISO 15118, providing an additional layer of user authentication control.

Historically, EV charging communications methods were created by auto and electrical infrastructure engineers to be ad-hoc ‘point’ solutions without knowledge of or regard for communications/network orientation or expertise. Typically, EV-EVSE interactions are not inherently communications intensive and could remain isolated however, many additional e-mobility service applications would require a more robust communication infrastructure.

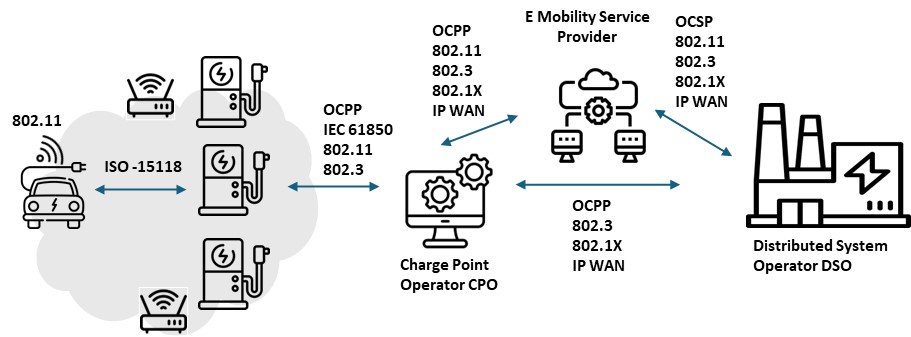


Figure X. EV Fueling Communications

# AFV Fueling Use Cases

With the increasing adoption of EVs, there are numerous opportunities to leverage technological advancement to enhance charging session efficiency and user satisfaction. Section 3 highlights various use cases that demonstrate potential improvements to the EV charging session experience for both consumer and commercial applications. IEEE 802 standards play a pivotal role in enabling more advanced connective options which would be necessary to support more advanced communications requirements between the various system elements.

## Public Parking with Advanced Charging Services

Public parking areas present an opportunity to integrate advanced charging services, allowing for vehicle charging while owners are occupied in other activities. These advanced services can include high-speed charging options, smart charging capabilities, payment integration, and real-time availability information, however, it is essential that these additional services are delivered reliably and secure manner.

To illustrate, an EV could be equipped with an IEEE 802.11 Station (STA), which enables it to establish a secure wireless network connection. Upon entering the range of the parking structure's Wi-Fi network (e.g. an Access Point), the EV's onboard communication system scans, identifies and initiates a connection process with an infrastructure Access Point (AP) broadcasting it’s SSID.

The STA and AP undergo an IEEE 802.1X authentication process with the EV STA acting as the Supplicant and the AP serving as the Authenticator. This authentication process could then be managed and coordinated by a back-end Authentication Server, utilizing an application like FreeRADIUS, and hosted in the cloud to facilitate centralized control, surveillance, and authentication services for the EVs remotely.

When the EV then initiates a charging session request, it presents its credentials to the AP which employs Extensible Authentication Protocol (EAP) over LAN (Local Area Network) (EAPOL) for the authentication dialogue between the EV(supplicant) and itself (Authenticator)/ The AP then verifies the EV’s credentials with the cloud hosted FreeRADIUS server within the CSMS via the internet. The EV presents its credentials in the form of a digital certificate and upon successful authentication, the network applies dynamic encryption keys, ensuring a secure IEEE 802.11i/WPA2 or WPA3 encrypted connection between the EV and the network. This connection is secured using IEEE 802.1X, a network access control protocol, ensuring a secure and encrypted communication channel between the EV and the network,

The dynamic encryption keys are derived from a complex process initiated during the IEEE 802.1X authentication. Initially, keying material is generated based on a shared secret established between the EV (Supplicant) and the Authentication Server through the EAP exchange. A Master Session Key (MSK) is derived from this process and shared between the Authentication Server and the Supplicant. This MSK, or a portion of it, becomes the Pairwise Master Key (PMK), which is used in generating session-specific keys that encrypt data frames between the EV and the AP, through protocols such as TKIP or CCMP for WPA2, and enhanced versions of CCMP for WPA3. These keys are dynamic, changing with each session, and ensure that even if a key from one session is compromised, other sessions remain secure due to their session-specific nature. This setup allows for scalable, flexible, and accessible management of charging sessions, user accounts, and payment processing, taking advantage of the cloud's high availability, redundancy, and disaster recovery capabilities. Simultaneously, an application-level connection through protocols such as Message Queuing Telemetry Transport (MQQT), Open Charge Point Protocol (OCPP), ISO 15118 or JSON over HTTPS could be exchanged between the EV and the EV Charging Services Management System (CSMS) enabling the transmission of data necessary for charging services.

Following the establishment of a secure connection, the EV and EVSP would commence a negotiation process to determine the specific parameters of the charging service. This negotiation might include determining the type of charging service needed, such as conductive (plug-in) or inductive (wireless) charging, and whether the power flow will be uni-directional (only charging the EV) or bi-directional (allowing for energy sharing between the EV and the grid – Vehicle-to-Grid, V2G capabilities). Additionally, the EV could communicate its specific needs, such as the amount of energy in kilowatt-hours (kWh) or additional range (in miles or kilometers) required; the desired duration of the charging session; and the pricing terms acceptable to the driver based on dynamic pricing models or pre-negotiated rates. This information exchange is crucial for tailoring the charging service to the individual needs of the EV and its driver, and also for matching energy supply available at the site with overall EV energy demand.

The EVSP would then process this information and make the best match between the EV's request and the capabilities of the Electric Vehicle Charging Infrastructure (EVCI) available at the parking structure. This determination involves several key considerations:

* Account Verification: The EVSP checks if the driver has an existing account or subscription with the service, usually through a query to a Charging Station/Services Management Server (CSMS).
* Charging Station Availability: The EVSP assesses the availability of a charging station that can deliver the power level needed to provide the requested amount of energy or range within the desired session duration. This involves checking the current occupancy and operational status of the charging stations.
* Other Considerations: Additional factors such as compatibility with the EV's charging system, current grid conditions, and any special requirements or preferences set by the driver may also be considered.

Similarly, the use of an Automated Valet feature for EV Parking could be used to increase charger utilization efficiency and improve the customer experience. Utilizing autonomous driving capabilities present in many EV models, these vehicles can independently navigate to designated charging stations within parking facilities, ensuring a seamless integration of charging services into the parking process.

Here, an Electric Vehicle (EV) could utilize the IEEE 802.11bd standard for secure, high-bandwidth vehicle-to-infrastructure communication to enable automated valet parking and efficient charging within a parking structure, leveraging autonomous navigation and smart charging technologies. Upon approaching the parking structure, the EV initiates communication using IEEE 802.11bd standard. This protocol is part of the enhanced Wireless Access in Vehicular Environments (WAVE) suite, specifically designed to facilitate direct vehicle-to-infrastructure (V2I), vehicle -to-vehicle (V2V) and other V2X communications, allowing the EV to securely connect to the parking structure’s communication network. The adoption of IEEE 802.11bd ensures enhanced reliability, lower latency, and increased bandwidth across these diverse communication channels, significantly improving the support for complex vehicular communications. Leveraging IEEE 802.1X for authentication, the EV establishes a secure communication link with the parking structure’s network, ensuring encrypted data exchange. Through this secure link, the EV communicates with the Electric Vehicle charging services platform (EVSP) to negotiate charging service parameters, as in the case above.

Once the charging service parameters are agreed upon, including type of charging, energy requirements, and session duration, the parking structure's management system activates the automated valet service for the EV. The EV could utilize standards under the IEEE P2040 family, which are related to road vehicle automation, to safely navigate within the parking structure. This involves real-time data exchange between the EV and infrastructure to guide the vehicle to the designated parking spot with the appropriate charging station. The EV's Advanced Driver-Assistance Systems (ADAS), enhanced for autonomous navigation in confined spaces then takes control. Using a combination of onboard sensors, cameras, and V2I communication, the EV autonomously navigates to the assigned parking spot, avoiding obstacles and adhering to the parking structure's traffic flow guidelines.

Upon reaching the designated parking spot, the EV aligns itself with the charging station and depending on the charging technology (conductive or inductive), the vehicle either automatically connects to the charging station through a robotic arm mechanism (for conductive charging) or positions itself accurately over an inductive charging pad. This process is facilitated by the Automatic Connection Device (ACD) feature set included in ISO 15118-20, which specifies advanced communication protocols for automated charging, ensuring a seamless and efficient connection between the EV and the charging infrastructure. With the physical connection established, the EV and the charging station commence the charging session based on the pre-negotiated parameters, ensuring the charging only begins after automatic authentication and authorization have been successfully completed. The EVSP monitors the session, adjusting as necessary to ensure optimal charging.

Throughout the charging session, the EV maintains a conductive or wireless communication link with the EVSP, providing updates on charging progress and any adjustments required due to changes in the EV's energy needs or the parking structure's power availability. Once the charging session is complete, or if the vehicle needs to be moved (e.g., to optimize parking space usage or for load balancing on the power grid), the EV can be autonomously navigated to a different spot or made ready for the driver to take over.

Similarly, for Hydrogen Surface Fueling (HSV) processes, there is a growing interest to apply comparable secure wireless technologies. Currently, HSV fueling often relies on a one-way infrared (IR) communication link, which, while functional for basic data transmission, lacks the interactivity and security afforded by more advanced communication methods. Recognizing this limitation, there could be a clear need for transitioning to a two-way communication system, which would significantly enhance the fueling process by enabling dynamic data exchange between the vehicle and the fueling station.

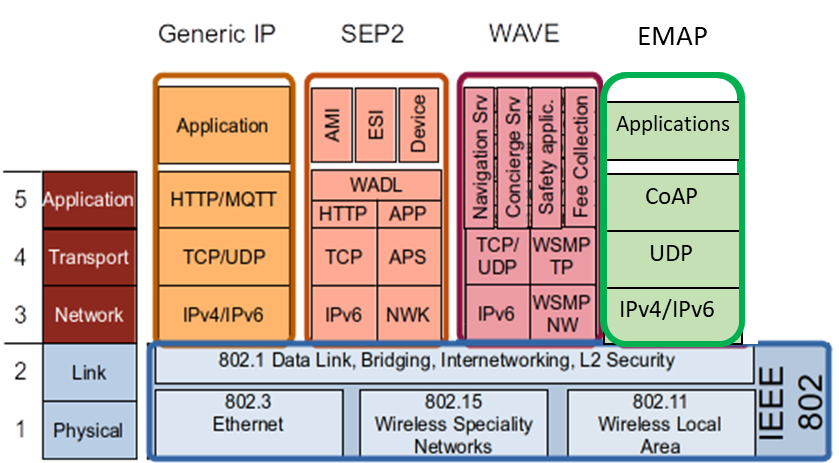
The potential shift towards utilizing secure, enterprise-level Wi-Fi, possibly by extending the existing Public Key Infrastructure (PKI) used in EV scenarios could be closely examined to push for a more robust and flexible communication infrastructure that can support not only the current needs but also the future developments in HSV fueling technology. By adopting a two-way communication protocol, based on secure Wi-Fi technologies, HSVs could engage in a secure authentication process with the fueling station's infrastructure, like the IEEE 802.1X network access control used in EV charging. This would facilitate many advanced functionalities, such as real-time negotiation of fueling parameters, secure transaction processing, and enhanced compatibility checks, thereby ensuring a safe, efficient, and user-friendly fueling experience. Additionally, this approach would allow for the integration of smart grid capabilities, optimizing energy usage and contributing to overall grid stability.

Further information on these use cases can be referenced in 24-22-0020-01-0000-afv-fueling-vertical-update.pptx.

## 3.2 Charging in Cooperative Energy and Smart Home Management

EV users who frequently commute between their workplace and home rely on an accessible charging infrastructure at both locations. Often employees work in small to medium-sized office buildings, while their residence could be a small multi-family residence or a single-family dwelling, both needing EV charging connections. As these vehicles can remain parked for several hours, L2 AC charging systems are most often used. At the most basic level, L2 AC charging is controlled by analog circuits within the charging device, operating standalone, with limited communications interface necessary apart from the vehicle battery management system negotiation for the charging session.

However, the integration of business power management with EV charging requirements is beneficial for small commercial building managers to maximize the utilization of charging resources, Similarly, homes or small multi-family dwellings with multiple charging stations can find a comprehensive approach to energy management to be advantageous, As such,



*Figure N: Examples of Smart Home platforms that can be deployed on IEEE 802 networks*

## Low-power, long-dwell EV Fleet Charging

- For a number of use cases, communications beween AC charging stations and a site-based or remote Charging Service Management System (CSMS) is required. Examples include vehicle and/or driver authentication; matching E-Van energy needs to charging station capabilities and availability; tracking and managing energy supply among charging stations; and providing firmware upgrade services to EV charging stations.

- Looking at the second example above in more detail: the main fleet use case is for overnight E-Van charging, but there might also be a need to charge vans between delivery runs. E-Van range with a full battery pack is typically 125 to 160 miles; charging requires the delivery of 68 kWh (Ford E-Transit) to 135 kWh (Rivian EDV/ECV). Depending on the initial state of charge (SoC, how much energy is in the battery when charging starts); and station power (7.6 kW to 22 kW), charging time to fully charge the E-Van battery can range between 3-18 hours. Fleets will have mix of shorter- and longer-range E-Vans; if every charging station must be able to charge any van overnight (say, between midnight and 6am) there will also be a mix of lower and high-power stations. To match stations to charging requirements, an E-Van could connect to a secure site Wi-Fi service when entering the depot and report its energy needs to the CSMS, which would make the match with an appropriate parking/charging bay. (Using the same process described in the Public Parking use case, Section 3.1, with perhaps additional service parameters exchanged in support of fleet logistics – see below.)

As more organizations electrify their fleet vehicles, the need for secure communications to support evolving EV charging technology. For EV fleet vehicles, maintaining a reliable and secure charging session is essential for both business needs and to protect sensitive organizational data. With the use of wireless technologies and other communication connectivity through the EV charging port, there is opportunities to leverage information gathered by the vehicle to optimize charging and other telematic logistical data within the fleet. Additionally, other opportunities though an 802 connected interface will allow for vehicle firmware updates for various systems such the Battery Management System (BMS), the Vehicle Control Unit (VCU), telematic and logistics management software or any required system security upgrades.

Since EV fleet vehicles are typically used in a time-bound manner allowing for overnight charging (long-dwell) sessions in depot settings the availability of numerous of medium-power L2 AC charging stations is required. AC charging can be simple, using only analog controls (see Appendix 1), and thus less expensive to deploy, with first-generation fleet vehicles charging stations being “standalone”, with minimal or no integration requirements, or external communications interfaces beyond RFID readers and Bluetooth capabilities for configuration. However, more advanced communications infrastructure would be required to support future applications in this area such as the integration of advanced technology and smart management to address the specific needs of electric vehicle (EV) fleets such as the optimization of charging based on operational patterns and predictive analysis, grid load balancing, and dynamic charging based upon time-of-day charging rates, grid condition and energy supply.

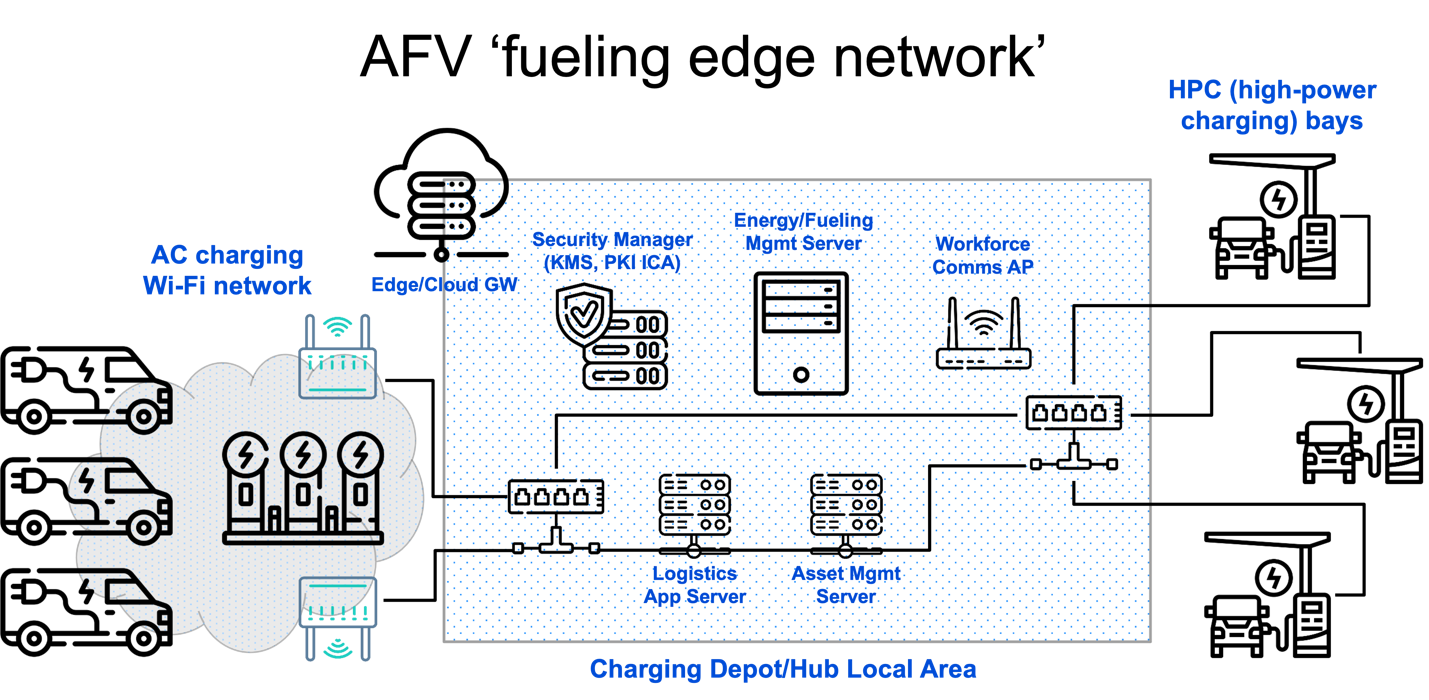
To illustrate, consider a package distribution or postal service operator employing electrified vans (E-Vans) within its fleet, multiple medium-power (Level 2, L2) AC charging stations would need to be installed at the operator’s depot. Upon arrival at the depot, each E-Van automatically initiates a secure wireless connection to the facility's network via its onboard IEEE 802.11 Station (STA) capability. This process involves the vehicle scanning for and establishing a connection with an infrastructure Access Point (AP), subsequently undergoing an authentication process managed by a back-end Authentication Server. This server is an integral component of the Charging Station/Services Management Server (CSMS), which leverages cloud technology for enhanced scalability and reliability, overseeing the authentication, monitoring, and management of EV charging sessions across the fleet.

Prior to the initiation of a specific charging session, authentication of the E-Van or driver could be implemented as exchanges over the secure Wi-Fi network. Here, When the E-Van arrives at the designated parking/charging bay, an EVSE with cable and connector (conductive charging service) might be plugged in to the EV by a robot arm that uses a camera and positioning sensors that all communicate via Wi-Fi. If the EVSE charges wirelessly, using inductive power transfer, Wi-Fi could be used to align the coil on the E-Van with the charging station coil embedded in the floor or mounted on a pillar. In both inductive and conductive charging cases, energy transfer can be managed by Wi-Fi messages between the EV and the charging station.

The Wi-Fi infrastructure required to support fleet charging should be based upon specific organizational requirements. Considerations as to the AP placement in regard to coverage and redundancy, security and back-haul architecture are contingent upon specific vendor capabilities and business case needs.

As part of the EV fleet charging infrastructure, the Charging Management System (CMS) can utilize advanced intelligence to schedule charging for each vehicle based on several factors such as the vehicle's current battery level, its anticipated energy needs for the upcoming day, and the depot's total energy capacity. This scheduling is dynamically adjusted in real-time to take advantage of fluctuating electricity prices, ensuring charging occurs during off-peak hours to maximize cost efficiency. Additionally, the system manages the depot's energy demand meticulously to prevent exceeding capacity limits. A pivotal feature of this system is the incorporation of Vehicle-to-Grid (V2G) capabilities, enabling not only the charging of the EVs but also allowing these vehicles to supply energy back to the grid during peak demand times. This bi-directional energy exchange is not just a potential source of additional revenue but also contributes to significant cost savings and promotes sustainable energy utilization.

Further information on these use cases can be referenced in: 24-22-0020-01-0000-afv-fueling-vertical-update.pptx



## High-power Medium/Heavy-duty Vehicle Charging

Medium to heavy duty vehicles are those who typically weigh greater than 10,000 pounds (4500 Kg) and can include freight delivery trucks, buses, construction or utility vehicles, etc. As such the charging requirements differ for heavy and medium duty vehicles than from those of light vehicles (cars, small delivery vans, etc.). Due to the high levels of DC power required to charge the larger battery packs at rates of 80kw or higher, specialized charging technology and standards have evolved for this application for various aspects of the power delivery systems.

Next-generation couplers for high-power EV charging (ChaoJi/CHAdeMO 3.0, SAE J3271 Megawatt Charging System [“MCS”]) include two pins for EV-charging station communications. Mechanical aspects (size, spacing, contact, etc.) were chosen to meet the high mating cycle requirements of the automotive industry (10,000). Signaling over the pins and conductors of these cable systems is still being defined, and there is interest in using IEEE 802.3 PHYs, specifically Single Pair Ethernet e.g. MultiGBase-T1 (IEEE 802.3ch), 1000Base-T1 (IEEE 802.3bp), 100Base-T1 (IEEE 802.3bw), 10Base-T1S (IEEE 802.cg), and 10Base-T1L (IEEE802.3cg) 802.3 to support additional charging and logistics applications for fleet management and operation. Through the incorporation of the vehicle as a peer station on an Ethernet LAN increased digital trust and cyber security can be achieved through leveraging aspects of 802.1X, as well as trusted metering and energy management for uni- and bi-directional power flows. The capacity to utilize secure high-speed communications from the vehicle to the fleet operations sites allows for the transfer of detailed data on battery health to and from the battery management system, enhanced diagnostics and firmware/software update options, and the transfer of critical data such as map updates, fleet logistics data, and payload tracking, etc.

1. Drill down on security aspects  
   - endpoint authentication using IEEE 802.1X  
   - other L2 security features (e.g. MACSEC)  
   - security for BPT transactions, e.g. trusted pricing, metering; non-repudiation  
   - support for higher-layer application security - (app/user authentication, MFA, ZTA)  
   - potential for using ML to track normal and anomalous EV charging behaviors
2. Drill down on energy management aspects  
   - waveforms for power transfers e.g. BPT and integration with on-site battery storage  
   - proof of conformance/performance to managed energy programs/signals  
   - backhaul for wireless WBMS

For further information regarding this use case can be referenced in: 24-22-0016-01-0000-ev-charging-vertical-overview.pptx

## Wireless Communication for EV Battery Management (WBMS)

< use case introduced in the March 2024 802 Plenary Session by Hyeong Hon LEE and Jin Seek CHOI, DCN 24-24-0005-00-0000) >

# Distributed Energy System Support for EV Charging

EV charging systems rely on a complex and robust systems to generate, deliver and manage the charging processes. Energy generation edge devices can include renewable energy sources such as photovoltaic (PV) panels, wind storage system or other edge systems such as microgrids. Complimenting the energy generation processes, energy management systems rely upon smart meters and sensors to enable localized data processing, analysis, and decision-making at the energy edge, allowing for real-time optimization, predictive maintenance, and intelligent energy management.

As vehicle fleet operators, such as mail/package delivery services and long-haul freight carriers, embrace electrification depots and fueling facilities will have to deliver high levels of electrical power and energy. Some sites may be adequately served by an electric utility, while others might be constrained by utility limitations regarding energy supply capacity or reliability, engineering project timelines, capital or operating costs, or other factors. Site- or region-scale solutions for energy generation, storage, management, and distribution – collectively, Distributed Energy Resources (DERs)– might become attractive alternatives.

We propose the term ‘energy edge’ to describe the use of DERs to manage energy production, distribution, and delivery close to electrical loads and to manage energy flows to and from ‘core’ electrical energy systems, e.g. the traditional electric utility. ‘Energy edge’ is thus a concept analogous to the ‘network edge’ and ‘edge computing’ in the IT world. We would qualify *microgrids* as exemplary but elementary or basic energy edge systems, due to their limited communications, control, and computing capabilities and the resulting ‘loose coupling’ so far between microgrids and the larger utility grid.

Indeed, microgrids were initially designed to work independently and separately from the utility grid. They were ‘energy islands’ by design for safety reasons: power generated by DERs might energize a segment of the grid that the utility had de-energized, thereby putting personnel at potential risk of electrocution. There was no way to integrate early DERs with the utility’s distribution system to ensure safety. Within a microgrid, each element relied on a self-contained controller and sensors to maintain its operation within acceptable bounds – there were no communications interfaces or networks connecting DERs.

As DERs and microgrids evolved, a degree of coordination enabling auto-islanding (disconnection) and reconnection of microgrids, was introduced based on a combination of energy sensing and some basic digital communications capabilities, which were introduced primarily to support remote monitoring and configuration – effectively, energy system ‘management plane’ functionality. That is, communications within currently deployed microgrids are not designed to support fine-grained coordination of energy flows, which still relies on ‘local’ (to the DER) sensing and control.

We use the term ‘converged energy edge’ to designate distributed energy systems, including microgrids, that embrace the aggressive, forward-looking use of digital communications to manage and control energy flows, safety, cybersecurity, reliability, efficiency, and all aspects of the energy edge. The capabilities of modern LAN/MAN standards and technologies have not yet been leveraged for energy edge applications. We believe that IEEE 802 standards and technologies can provide a coherent, secure, and extensible platform supporting next-generation, fine-grained sensing and control of EV charging stations, DERs, and microgrids. Along with edge computing, IEEE 802 networking will enable more reliable, resilient, and secure microgrid systems, including and especially those supporting electrified and other alternative vehicle fueling.

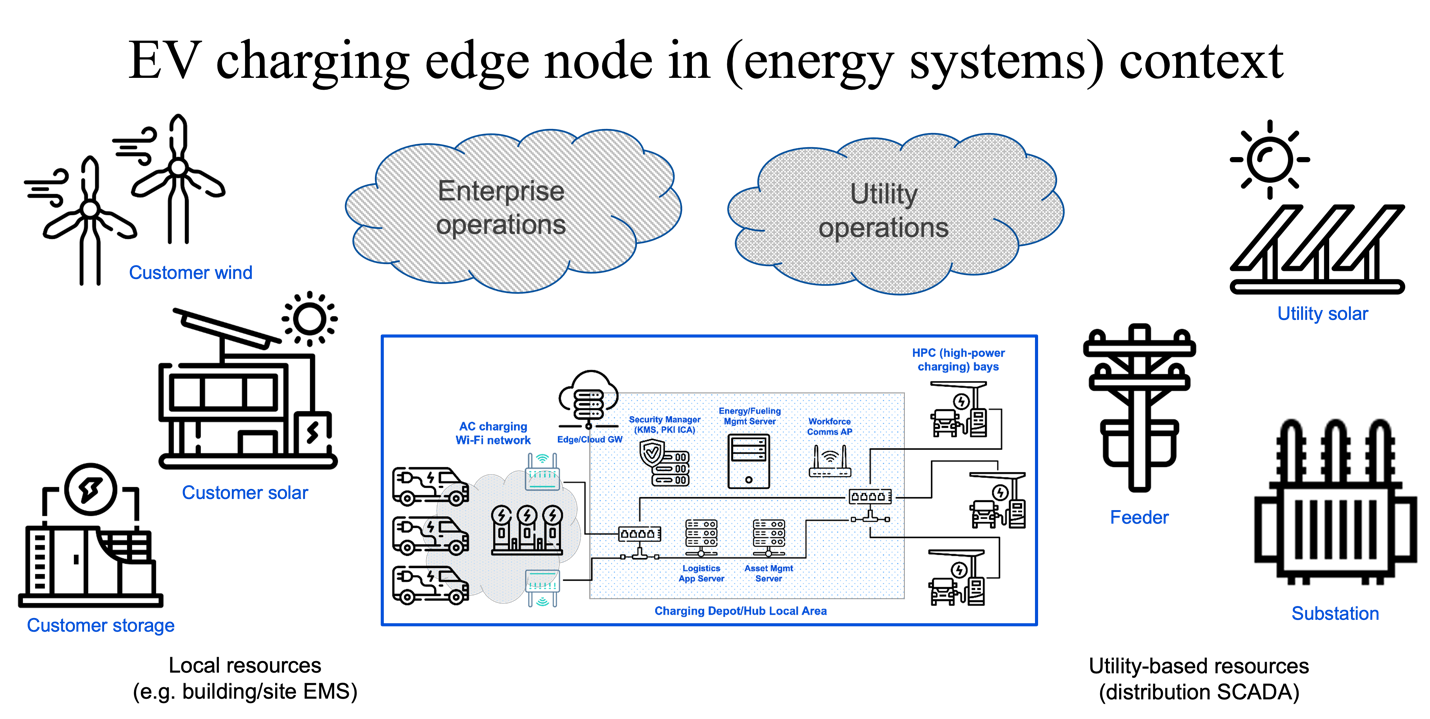
We can illustrate this by sketching a few integration scenarios based on high-level requirements.

1. Site-based energy storage: *<e.g. for energy security through utility supply outages; optimizing energy costs; fine-grained management of V2B. Mostly site-contained LAN-based communications, local edge computing for energy modeling and optimization, potential connection to cloud e.g. a centralize enterprise-wise asset/operations management system. >*

2. Connecting a fleet operator’s depots in a metropolitan area: *<e.g. regional network connections between US Post Office or Amazon depots; the analogy is with data CDNs. >*

3. Integration with offsite DERs*: < e.g. communication with a local or regional wind generation site. LAN-based or (more likely?) MAN-based communications, depending on distance and data comms requirements; tighter integration possible for fleet-owned DERs. >*

4. Integration with the serving utility’s distribution system: *< e.g. connection with the serving substation for the exchange of control signals, analytical data, energy management e.g. DR Program signasl, etc. >*



# Communications and Networks supporting AFV Fueling

*< Indicate that this is the technical essence of our whitepaper, providing details on the topics in the subsections below.>*

## Communications Requirements

*< Speeds and feeds, both minimal and aspirational. This can be the kind of table shown in other 802.24 whitepapers, with use cases/scenarios as rows and metrics as columns. This is a common way to show ‘speeds and feeds’ requirements over common span distances / in or across network domains; I’ll try to find some other examples. >*

## Network Architectures

*< Expanding on the diagrams above from 24-23-0007-00-0000-draft-afv-whitepaper.docx. At a basic level, perhaps show the next level of detail for the first diagram above: clarify the wireless and wired LAN endpoints, add access points, switches and routers, 802.1X AAA servers, etc. Then, supplement this LAN-only architecture (with a site-level connection to enterprise network or cloud) with a depiction of LANs connected via MAN interfaces, and other MAN nodes: ‘sister’ depots, energy supply partner sites, utility sites e.g. a substation. >*

## Device and Network Cybersecurity and Management \* EV Charging System Cybersecurity and Management?

*< Survey the applicable IEEE 802 standards relevant and applicable to this concern.*

*I think the approach here would be to describe what kinds and levels of cybersecurity provisions would be required on various, well-chosen links, e.g. between AC EVs using Wi-Fi and APs; between APs and network management elements [authentication server]; between LAN switches and routers; etc. We should draw on and reference well-established practices and guidelines for configuring ‘enterprise-grade security for wireless and wired LANs’ – Damola has been researching these – keep it short and sweet, since we presume our reading audience is familiar with common 802 networking knowledge>*

*<Let’s review what the draft IEC/IEEE 60802 Industrial Automation and Control standard has in this regard – for example, it calls out cipher suites for device authentication and might require the use of mTLS (if memory serves, need to verify). We could note that the ICS (industrial control systems) community, which has traditionally relied on physical security and minimized cybersecurity provisions to keep costs and operational complexity low, are now stipulating more stringent cybersecurity requirements. This might be seen as setting a new ‘floor’ for cyber requirements for cost-constrained devices – we can draw some conclusions for energy edge and EV charging, etc. >*

# IEEE 802 Standards and Technologies supporting AFV Fueling and the Energy Edge

IEEE 802 protocols provide an OSI Layer 2 transport network supporting pure L2, IPv4 and IPv6 communications, which enable flexible, real-time capabilities necessary to facilitate the communications of industry specific higher-level protocols necessary to manage various EV charging scenarios. While the 802 standards have a rich protocol suite which can be used in a variety of purposes to foster robust, reliable and timely communications, the most relevant protocols for consideration within the AFV fueling environment include 802.1, 802.3, 802.11 and 802.15.

## IEEE 802.1 for AVF Bridging and Management Applications

While the 802.1 protocols themselves are not directly used for EV charging, they play a crucial role in providing network infrastructure and management capabilities that support EV charging systems. Here are a few ways in which the 802.1 protocols can be most applicable in EV charging:

* 802.1AB-802.1AB-2016 - IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery
  + Link Layer Discovery Protocol (LLDP) can be used for discovering and advertising network device information enabling EVs to discover and identify charging stations and for charging systems to be identified for integration into network management systems.
* 802.1AC-802.1AC-2016/Cor 1-2018 - IEEE Standard for Local and Metropolitan Area Networks--Media Access Control (MAC) Service Definition - Corrigendum 1: Logical Link Control (LLC) Encapsulation EtherType
  + - Ethernet encapsulation could be used in networks to transport other protocol data necessary to enable the charging process.
* 802.1AC-2016 – IEEE Standards for Local and metropolitan area networks – Media Access Control (MAC) Service Definition including MACsec.
* MACsec, as part of 802.1AC specifies protocols to improve data confidentiality, integrity and origin authentication supporting a secure exchange of information between AFV and the charging station infrastructure.
* 2018 - IEEE Standard for Local and metropolitan area networks -- Time-Sensitive Networking for Fronthaul802.1CS-2020 - IEEE Standard for Local and Metropolitan Area Networks--Link-local Registration Protocol
  + - Time sensitive Networking (TSN) can be relevant in EV charging systems that require precise timing and synchronization, such as for Vehicle-to-Grid (V2G) applications or coordination with grid management systems.
* 802.1Q-2018 - IEEE Standard for Local and Metropolitan Area Network--Bridges and Bridged Networks
  + - Virtual LAN (VLAN) tagging can be used to allow for the segmentation of network traffic into different virtual networks enabling the separation and prioritization of charging-related traffic, ensuring efficient and secure communication between charging stations, management systems, and other network components.
* 802.1X-2020 - IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control –
  + - Could be used within EV charging systems to authenticate and authorize EV access to charging infrastructure.

## IEEE 802.3 for AVF Ethernet Applications

Similar to 802.1 protocols, the IEEE 802.3 protocol suite provides necessary elements to a robust and reliable L2 transport. Again, IEEE 802.3 is a comprehensive suite of protocols which could be used to support various requirements of a AFV fuelling. These protocols are relevant to EV charging either due to their power delivery capabilities, speed characteristics or use within an automotive application.

* 802.3ch-2020 - IEEE Standard for Ethernet--Amendment 8: Physical Layer Specifications and Management Parameters for 2.5 Gb/s, 5 Gb/s, and 10 Gb/s Automotive Electrical Ethernet
  + - As this protocol addresses connectivity in automotive applications, it could be relevant to AFV fueling, although not directly used in EV charging.
* 802.3cg-802.3cg-2019 - IEEE Standard for Ethernet - Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors
  + - The use of single pair ethernet could be advantageous in some scenarios within an AFV fueling system allowing for a both 10 Mb/s data and power to be transmitted over 2 physical wires.
* 802.3cd-2018 - IEEE Standard for Ethernet - Amendment 3: Media Access Control Parameters for 50 Gb/s and Physical Layers and Management Parameters for 50 Gb/s, 100 Gb/s, and 200 Gb/s Operation
  + - * 50 Gb/s, 100 Gb/s, and 200 Gb/s operation can be used within aspects of a charging system, or the backend systems required for authentication, billing and authorization of services.
* 802.3bt-802.3bt-2018 - IEEE Standard for Ethernet Amendment 2: Physical Layer and Management Parameters for Power over Ethernet over 4 pairs
* Power over Ethernet (PoE) can be used within the context of EV charging to enable the transmission of power with data for various components or auxiliary devices.

## IEEE 802.11 for AVF Wireless Applications

Although 802.11 protocols are not typically involved with the direct management of the charging process, they are substantially used to facilitate other services required to support payment processing, monitoring and management, vehicle to grid integration, and advanced user services such as autonomous fueling in a secure and reliable manner. Possible use cases include the following:

* 802.11-2020 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
* Within an AFV fueling context, wireless technology can be used for various purposes such as authentication and authorization, billing and payment processing, remote monitoring and management, user communications and firmware updates.
* 802.11ax-2021 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN
  + - Wi-Fi 6 OFDMA, MU-MIMO enhance throughput, reducing latency which could be beneficial for EV charging in urban or densely populated areas.
* 802.11ay-802.11ay-2021 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Enhanced Throughput for Operation in License-exempt Bands above 45 GHz
  + - High data rates in 60 GHz band suitable for high data transfer rates over short distance such as software updates for EV fleet vehicles in charging depots.
* IEEE 802.11bd-2022 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Next Generation V2X.
  + - Specifies Vehicle-to-Everything (V2X) communications, specifically for dynamic conditions, applicable for autonomous vehicle connection to EV charging systems.

## IEEE 802.15 for AVF Specialty Applications

IEEE 802.15 protocols, focusing on Wireless Personal Area Networks (WPANs) facilitate short-range communication between devices, typically within a few meters or tens of meters, depending on the specific standard and application. 802.15 protocols are suitableto support Smart Home, Smart Metering applications and possible communications requirements for Vehicle to Grid energy transfers.

* 802.15.1-2005 – IEEE Standard for Local and metropolitan networks – Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN).
* Bluetooth connectivity is specified within this standard which allows for EV charging systems to interact both with users or smart home infrastructure usually in the context of setting up 802.11 connectivity.
* 802.15.4-2020 - IEEE Standard for Low-Rate Wireless Networks
* Specifies protocols for low-rate, low-power communications which is applicable for sensor networks or device controls within EV charging stations where low power consumption and reliability are required rather than high data rates.
* 802.15.4g-2012 – IEEE Standard for Local and metropolitan area networks: Low-Rate Wireless Personal Area Networks (LR-WPANs). Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks.
* Also known as Zigbee, used in many Smart Home applications, 802.15.4 enables EV charging stations to communicate within a home energy management system allowing for charging optimization based on rates and usage and provides opportunities for the integration of the charging function into an overall home management scheme.
* 802.15.4y-802.15.4y-2021 - IEEE Standard for Low-Rate Wireless Networks Amendment 3: Advanced Encryption Standard (AES)-256 Encryption and Security Extensions
* Specifies the use of AES-256 Encryptions and security extensions which enhances security communications of sensitive information such as consumer PII, positioning information, etc.
* 802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks--Amendment 1: Enhanced Ultra-Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques
* Utilizes UWB for precise ranging with increased data rates, applicable for automated wireless charging systems requiring precision positioning.
* 802.15.4g-2012 – IEEE Standard for Local and Metropolitan area networks: Low-Rate Wireless Personal Area Networks (LR-WPANs) – Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks
* Also known as Smart Utility Networks (SUN), used to support smart-metering and other smart-grid applications. Can be used in conjunction with other smart home protocols to support communications for V2G connectivity.

# Conclusions and Recommendations

The family of IEEE 802 standards provide a robust framework for the communications requirements of alternate vehicle fueling systems. Fueling systems integrated with advanced features such as fleet charging management, charging station reservations and queuing, “Smart” integration into home and beyond rely on reliable and secure Layer 2 transport of device, consumer or business data between the various systems. The architecture of IEEE 802 networks, characterized by modular and interchangeable components, ensures that these networks can adapt and grow with relative ease. While IEEE 802 standards predominantly underpin IP-based communication solutions, they also offer broad support for other network protocols required to support other protocols required in the operation and management of an EV charging infrastructure.

As both the IEEE 802 standards and the underlying technology of alternative vehicle fueling systems continue to evolve, there are continued opportunities to both explore current standards for this use case and for the development of new standards to support new communications requirements in this industry silo. Key focus areas include improving V2E security and latency reduction to continue to advance autonomous driving and fueling features, the integration of time sensitive networking and the use ultra-reliable low-latency communications (URLLC) where applicable.

# References

1. J. S. Choi, "Energy management agent frameworks: Scalable, flexible, and efficient architectures for 5G vertical industries," IEEE Industrial Electronics Magazine, vol. 15, no. 1, pp. 62-73, March 2021
2. ISO/IEC 15067-3:2012, Information technology – Home Electronic System (HES) application model – Part 3: Model of a demand-response energy management system for HES
3. ISO/IEC 15067-3-3:2019, Information technology – Home Electronic System (HES) application model – Part 3-3: Model of a system of interacting energy management agents (EMAs) for demand response energy management
4. ISO/IEC 15067-30:FIDS, Information technology – Home Electronic System (HES) application model – Part 30: EMA functional requirements and interfaces
5. ISO/IEC 15067-3-31:FDIS, Information technology – Home Electronic System (HES) application model – Part 3-31: Protocol of energy management agents for demand response energy management and interactions among these agents
6. J. S. Choi, "A hierarchical distributed energy management agent framework for smart homes, grids, and cities," IEEE Communications Magazine, Vol. 57, No. 7, pp. 113-119, 2019
7. T. Shimizu, T. Ono, W. Hirohashi, K. Kumita, and Y. Hayashi, “Experimental demonstration of smart charging and vehicle-to-home technologies for plugin electric vehicles coordinated with home energy management systems for automated demand response,” SAE International Journal of Passenger Cars-Electronic and Electrical Systems, vol. 9, no. 2016-01-0160, pp. 286–293, 2016.
8. IETF RFC 7252, The Constrained Application Protocol (CoAP), edited by Z. Shelby et al., June 2014, available at: <https://tools.ietf.org/rfc/rfc7252.txt> [viewed 2023-05-31]
9. IETF RFC 7159, The JavaScript Object Notation (JSON) Data Interchange Format, edited by T. Bray, March 2014, available at: https://tools.ietf.org/rfc/rfc7159.txt [viewed 2023-05-31]

A. A. S. Mohamed, A. A. Shaier, H. Metwally, and S. I. Selem, “An Overview of Dynamic Inductive Charging for Electric Vehicles,” *Energies*, vol. 15, no. 15, p. 5613, Aug. 2022, doi: <https://doi.org/10.3390/en15155613>.

[1]

“ROADMAP OF STANDARDS AND CODES FOR ELECTRIC VEHICLES AT SCALE ANSI Electric Vehicles Standards Panel (EVSP),” 2023. Accessed: Apr. 20, 2024. [Online]. Available: https://share.ansi.org/evsp/ANSI\_EVSP\_Roadmap\_June\_2023.pdf

‌

[1]

T. Basso and R. Deblasio, “IEEE Smart Grid Series of Standards IEEE 2030 (Interoperability) and IEEE 1547 (Interconnection) Status Preprint,” 2011. Accessed: Mar. 29, 2024. [Online]. Available: https://www.nrel.gov/docs/fy12osti/53028.pdf

‌ [1]

C. Ruth, “IEEE Standards in Everyday Life: Summer Vacation,” *IEEE Standards Association*, Jun. 30, 2022. https://standards.ieee.org/beyond-standards/industry/technology-industry/ieee-standards-in-everyday-life-summer-vacation/ (accessed Mar. 29, 2024).

‌

**Appendix 1: Electrical Characteristics of Residential and Small Building Charging**

Appendix 2: Smart Home Overview

In order to meet these goals, the devices and systems in a home need to have some degree or information processing and communication capability. Modern media devices, which are highly configurable and connected, provide a good example of how any subsystem within the home can be automated and integrated with others. For example, meshed Wi-Fi nodes – originally meant primarily to provide consumer devices with wireless access to the Internet –now incorporate microphones and speakers, allowing for natural-language interaction from almost anywhere in the home; can retrieve or relay data such as music playlists or television viewing preferences and activate services accordingly; and can report the status or change the settings of environmental controllers such as thermostats, skylights, and window shades. One can imagine such nodes soon incorporating sensors to gauge environmental factors (e.g. air quality, human/pet motion/activity, light or noise levels) as well.

**Appendix 3: DER Overview**

DER energy sources (such as solar energy and wind energy) have become important alternative sources of energy in the smart home. EVs are also becoming popular, because of their fuel efficiency and economic benefit, as compared to the conventional fuel-based vehicles. Energy management is an early target for similar verticals such as healthcare, agriculture, manufacturing, automotive, public transportation, utilities and energy, environmental, smart cities, and more. In energy vertical, it is crucial to find solutions to manage the peak demand while supporting substation automation of renewable energy systems such as DERs and EVs.

Appendix 4: Smart Energy Environmental Management Systems

EMAs enable the allocation of energy among appliances and switching energy sources from grid to local generation or storage according to consumer preferences [1]. EMAs also enable automated demand-response (DR) services in a house, a residential community or a building consisting of multiple apartments for coordinating and allocating energy consumption and generation among multiple EMAs in different locations [6]. DR programs are being offered to residential consumers for energy conservation and for energy management to align demand for power with available supplies for appliance usage and budget constraints. The co-ordination among EMAs offers improved energy management and overall efficiency according to customer preferences.

Typical smart energy services can include integrated energy management for efficient energy usage. The coordinative energy management is a combination of DR services and distributed energy sharing and trading within the community, energy information sharing among multiple energy systems for more efficient energy usage, etc. These cooperative energy services offer benefits in electrical energy management in a house, a residential community or a building consisting of multiple apartments by energy sharing and trading among EMAs, EVs, DERs and home appliances [6].

Appendix 5: Additional Use Cases:

An example of a service delivered to the charging device via Wi-Fi and the vendor’s cloud, is to allow the user to select their electricity pricing rate program from a list provided by the utility or utilities serving their location. Some utilities offer discounted rates for overnight consumption, encouraging EV charging at lower cost when electricity is not in high demand. If the user enrolls in such a program and selects that rate, their wallbox might be configured to block charging, or post a warning, if the EV is plugged in when rates are higher (e.g., during daytime). Given the rate program, the wallbox could calculate and display the cost of charging the EV. (Only after energy has been delivered, unless the EV’s battery capacity was set on the station and the EV sent its state of charge before charging, which is not currently possible using SAE and IEC L2 AC charging protocols).

A similar service that could be provided to EV drivers via the vendor cloud and Wi-Fi include charging power level regulation and/or incentive based on energy pricing or utility capacity constraints. Thus, an attempt to charge an SUV or pick-up truck with a 120 kWh battery pack at 14.4 kW (60 A) during hours of peak energy demand might result in the charging station being limited to delivering only 7.2 kW (30 A) and perhaps incentives – a price discount or confirmed reservation – to charge at a nearby public fast charging station that gets its energy from solar panels and energy storage, rather than the grid.