**IEEE P802.24**

**Vertical Applications Technical Advisory Group**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.24 Vertical Applications Technical Advisory Group | |
| Title | **White Paper: IEEE 802 Standards support for next-generation Alternative Vehicle Fueling/Charging Infrastructure** | |
| Date Submitted | 2025-07-29 | |
| Source | Craig Rodine, Adedamola Adesokan, Sheryl Drake, Jin Seek Choi, Hyeong Ho Lee, Young Kyu Ko |  |
| Re: | Draft with additional content | |
| Abstract | This white paper describes how IEEE 802 standards and technologies can help to enhance the features, performance, security, and convenience of Alternative Fuel (especially Electric) Vehicle refueling infrastructures. It provides examples of emerging advanced use cases and the networked integration of EV charging with other platforms and capabilities at the ‘energy edge’. | |
| Purpose | To encourage innovative thinking and proof-of-concept experiments using IEEE 802 standards and technologies to integrate the control and management of next-generation vehicle refueling and distributed power systems. | |
| 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 contributors acknowledge and accept 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, rather than fossil fuels, invites a reconsideration of fueling processes and infrastructure. The experience of fueling an Internal Combustion Engine (ICE) vehicle is familiar throughout the world. Aspects including availability (station locations, hours of operation); safety and ergonomics; resources (time and money) required; how to operate a dispenser; the methods of sale and units of measure (signage, payment methods, receipt, loyalty benefits, etc.) are well-known and taken for granted by the driving public. In contrast, many aspects of the fueling experience for non-ICE vehicles are new and different.

In this white paper, the term Alternative Fuel Vehicle (AFV) designates Electric Vehicles (EVs) and Hydrogen Surface Vehicles (HSVs), the two leading types of AFVs coming into widespread use. Since the vast majority of AFVs being adopted are (fully or hybrid) plug-in battery electric vehicles, our main focus in this whitepaper is on EVs and their charging infrastructure.

One significant difference between ICE and AFV fueling is that the couplers used for AFV fueling (cable/hose with attached plug/nozzle, and mating socket/inlet) support analog and/or digital communication between vehicle and dispenser. Control protocols exchange signals and data over this communications link to manage the transfer of the new, alternative types of motor vehicle fuel (electrical energy or gaseous hydrogen).

AFV fueling control schemes make limited or no use of mainstream communications standards and technologies, in particular at the Physical and Data Link layers of the ISO/OSI protocol stack model. Consequently, they don’t benefit from the proven security, performance, extensibility, and supply chain advantages of standards-based, mass-market communications solutions.

This whitepaper describes how IEEE 802 LAN/MAN standards and technologies can extend and enhance the communications capabilities and security posture of AFV fueling infrastructures. It includes some emerging use cases, high-level requirements, and integration oppor­tunities across a variety of scenarios and sites.

# AFV fueling communications and security

To understand how communications is used in the AFV vehicle fueling process, a comparison with ICE vehicle fueling can be useful.

Obviously, every vehicle fueling process requires a means for fuel (liquid gas/petrol, electricity, liquid or gaseous hydrogen) to be transferred from a dispenser to the vehicle. Such a *coupler* has two components, an *inlet* on the vehicle and a mating *connector* or *nozzle* on the dispenser.

The familiar “gas pump handle” used to fuel an ICE is a simple coupler whose critical mating feature is the dimensions of the nozzle spout (on the dispensing fuel pump) and fuel filler neck (in the vehicle’s fueling inlet). This “physical coding” prevents a diesel fuel nozzle from being inserted into a petrol inlet, or leaded petrol from being pumped into an ICE that requires unleaded fuel. An ICE coupler’s control and safety features are mechanical: operating lever, main valve, fuel-tank shutoff, attitude shut-off, no-pressure-no-flow device, etc.

Notably, there is no signaling or communication between ICE fueling infrastructure (a gas, petrol, or diesel dispenser) and the vehicles it serves.

A gaseous hydrogen fuel coupler is similar to the ICE design but with important mechanical differences, specifically a mating collar with a magnet for dispenser activation; and a sealing/locking feature for safety, since the gaseous fuel is under pressure.. Hydrogen fueling relies on a simple form of digital communications, as described below; in contrast, couplers used for EV charging have very different characteristics, e.g. electricity (vehicle ‘fuel’) is delivered over high-capacity conductors and pin-and-sleeve based couplers; smaller pins and conductors support two-way communication between the dispenser and EV to control the charging process.

## Electric Vehicle (EV) charging

The cells in an EV’s battery pack consume and dispense energy in the form of constant, “direct” electrical current (Direct Current [DC]). In contrast, the electrical energy delivered by utilities is Alternating Current (AC), which supports the transmission and distribution of energy over long distances. To benefit from ubiquitous AC infrastructure, EV fueling systems include a device to convert AC to DC current, i.e. a rectifier (also known as a converter). Since many EVs used AC motors for propulsion, a device that “inverts” DC energy stored in the traction battery to AC energy is also required; for reasons of economy and design, EVs some have a single device that functions as a two-way power converter.

The growth in EV adoption, market share, and volume helped drive the cost of on-board electric storage down, and battery packs grew in capacity to provide drivers with greater range between charging sessions. However, using a modest on-board AC-DC converter, larger battery packs would take longer to charge, adding hours to long-distance journeys. To speed up charging, higher power was called for, but on-board conversion doesn’t scale well: high-power converters would add unacceptable cost, weight, and heat to the EV. The solution is to move AC-to-DC power conversion off-vehicle to the fueling infrastructure – thus, “DC Fast Charging” (DCFC) was born. The split of power conversion control logic that’s internal to on-board converters requires fine-grained coordination between dispenser and vehicle, which involves the exchange of frequent and detailed control messages between dispenser and vehicle. Consequently, digital communications capabilities were added to charging cables, couplers, stations, and vehicles.

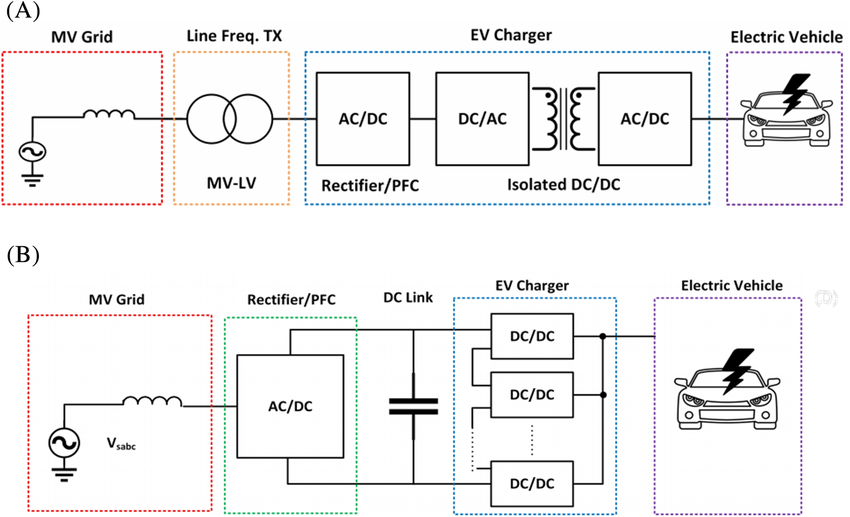


Figure (A) shows a DCFC that converts 400-480 VAC (three-phase) current to the DC power needed to charge an EV battery. Figure (B) shows a different topology, with upstream AC/DC conversion and multiple DC/DC stations using a shared DC link (bus). Other topologies are also used; in all cases, communication between EVs stations is the same.

### The foundation: pilot-wire control of AC charging

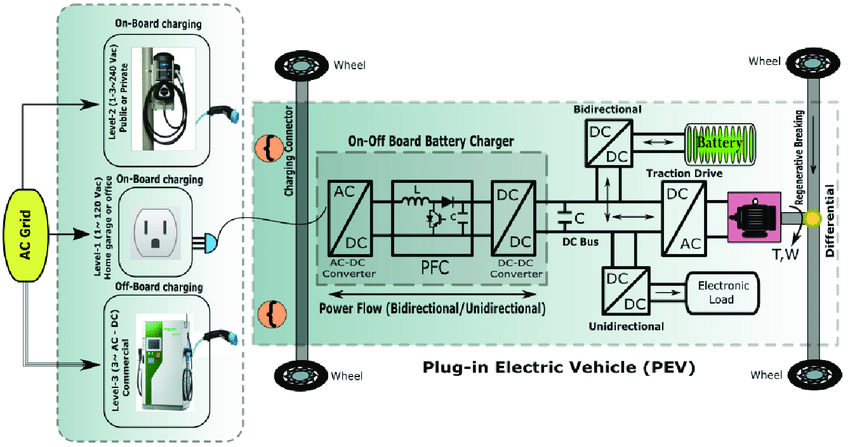
### In the case of AC charging, control of energy transfer between the charging station and an EV’s on-board converter is similar to HSV fueling: the associated communication is one-way, but with the difference in what’s being communicated. In HSV fueling, only a single, unchanging value – the vehicle’s fueling tank characteristics, an immutable physical property – are shared, whereas in AC EV charging the one critical datum – the current available from the dispenser, therefore the charging power – can be changed between or even during charging sessions.

### An AC charging station maintains an analogue Pulse Width Modulation (PWM) signal on a “pilot” conductor in the charging cable (1 KHz, ±12 VDC referenced to the Protective Earth conductor).[[1]](#footnote-2) By varying its voltage and duty cycle the dispenser, acting as charging process state machine master, coordinates changes in charging state, detects safety faults, and conveys the amount of current available to the EV. While it’s possible to change the current level during a charging session, as noted above, typically the value remains constant reflecting a steady energy supply level that’s a site design parameter (conforming to local and national electrical code requirements for circuit protection, among other factors). Occasionally the energy supply is constrained, for example due to temporary or periodic local constraints, load sharing, or a utility curtailment event. In such cases, the dispenser can be re-configured (via local or remote control) to decrease the PWM duty cycle and provide less energy than faceplate maximum.

### Technical specifications of AC charging state machines and control signaling are published as open standards (IEC 61851-1 and SAE J1772), which are harmonized and fully interoperable. After the publication of these standards (between 2001-2010) their implementation in EVs and AC stations became stable and provided a solid technical foundation for the first wave of EV market growth.

### Regarding security, AC charging signals are physically protected in the cable and coupler and emit very low levels of electromagnetic energy outside that envelope. The signaling ‘endpoints’ – microcontrollers implementing the charging state machines in the dispenser and EV – should be protected against unauthorized access and other attacks by utilizing physical and electronic tamper resistance. If an AC station is capable of network connectivity, means to secure its link to local and/or wide-area networks should be provided as well. Finally, AC charging state machines are designed for electrical safety and fairly robust against out-of-bounds parameter insertion.

Summarizing: AC charging communication is analogue not digital; there is no frame or packet formation or protocol stack involved. It is point-to-point and not connected to any network.[[2]](#footnote-3) Based on a low-voltage 1 KHz PWM signal, AC charging control is difficult to block, intercept, or modify, requiring expert knowledge and visible physical intervention. Attacks would require access to deeply embedded processors and the ability to override protections provided in firmware. Most threats and attack scenarios are low on the cost/benefit scale; the highest-value attack would seem to be on an OEM’s or supplier’s firmware installation process at manufacturing time, which is ostensibly high in effort and cost. Finally, even if the AC charging firmware of an entire fleet of EVs was compromised, due to the analog, disconnected nature of AC charging there would likely be very low if any impact on EV charging dispensers or other devices or actors in the ecosystem.



### DC charging using CAN communications (CN, JP)

To provide the communications needed for DC Fast Charging, Asian EV industry leaders chose the conventional automotive Control Area Network (CAN) vehicle bus standard, supported by a pair of conductors in the charging cable and pins with suitable properties for the physical layer in the coupler. Although CAN is a “multi-drop” bus standard, it is specified for DCFC as a point-to-point segment (two-port bus) between the charging station and the EV. The messages required for DC charging control are implemented as CAN Data Frames. Details of the physical coupler, the two (station and vehicle) charging state machines, and the control messages sent between them are specified in standards developed by a Japan-based international industry association (CHAdeMO Association); and working groups under the Chinese General Administration of Quality Supervision, Inspection and Quarantine (AQSIQ, 中华人民共和国国家质量监督检验检疫总局) and the Standardization Administration of China (中国国家标准化管理委员会).[[3]](#footnote-4)

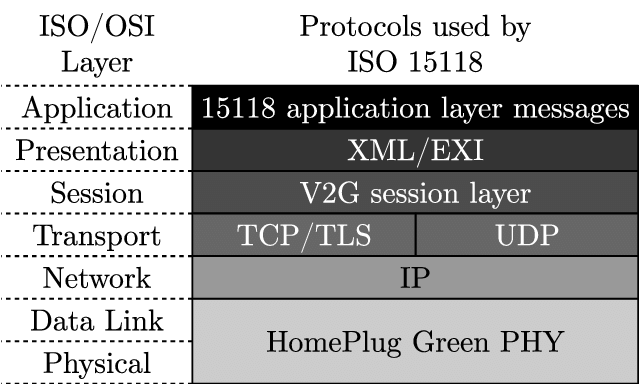
The use of CAN communications effectively adds an external component – the fuel dispenser – as a segment of the vehicle’s control network, thereby incorporating the EV fueling process and dispenser design into EV product/service definition. Advantages of this choice include technical familiarity; well established test equipment and procedures; supply chain leverage – multiple high-volume vendors offering components at low cost; and extensibility. The CAN approach has provided a solid foundation for the evolution of CHAdeMO and GB/T standards, starting with basic DCFC service and extending to advanced capabilities like much higher voltage and power, interoperability between CHAdeMO and GB/T (CHAdeMO 3.0), and Bi-directional Power Transfer. Notably, these standards ensure backward/forward compatibility between versions.

Regarding security, systems using CAN bus rely primarily on physical security, even in critical areas like Train Control and Monitoring Systems (TCMS), road vehicle Automatic Driver-Assistance Systems (ADAS), and robotic surgery, although there are means and methods for securing CAN messages if needed.[[4]](#footnote-5) CHAdeMO and GB/T applications are no exception, relying on the physical medium (a pair of 18 AWG conductors, not twisted, in the charging cable) and endpoints being challenging to access or tap, especially since they are proximate to high-voltage conductors within the cable, charging station, and vehicle; and CAN signal strength low enough to defy most efforts to intercept, interfere with, or inject CAN messages via inductive coupling.

### DC charging using a BPLC/IP/TCP protocol stack (EU, KR, NA)

The ISO 15118 series of DC charging standards mandated and/or being adopted in Europe, North America, and Korea utilize Broadband PowerLine Carrier (the HomePlug Green PHY industry standard [HP-GP][[5]](#footnote-6)) for EV-to-charging station communications. HP-GP uses carriers in the 2-30 MHz range on the single pilot wire in the charging cable, otherwise used for AC charging control (see Section 2.1 above). The OFDM symbols are formed at the MAC layer into IEEE 802.3 Ethernet frames, which constitute the Layer 2/3 interface.

Above the MAC, ISO 15118 uses Internet Standards IPv6 and TCP at layers 3-4, although the ‘network segment’ between charging station and EV endpoints is a point-to-point link (not connected to any other segments, switched, or routed. Thus, requirements for DHCP, etc. are limited to this topology. Between TCP and control messaging, a ‘communications session’ layer establishes the EV-station connection and provides a generic message data structure and basic service discovery for a charging session (from plug-in and authentication through billing and receipt). Control and service management messages are defined in an XML Schema and de/compressed using the Embedded XML Interface (EXI); what’s actually exchanged as TCP/IP payloads on the wire are binary EXI message representations (encodings).

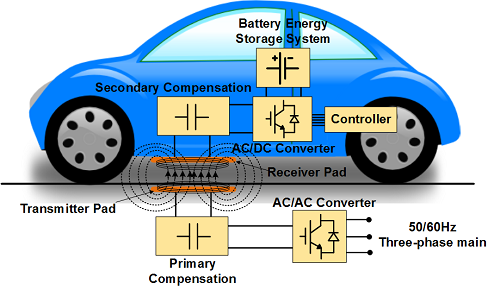


While there is a provision in ISO 15118 for protecting communications over this link with the IETF Proposed Standard for Transport Layer Security (TLS v1.2, v1.3) it is required only for a subset of messages that support an automatic, in-band payment feature called Plug-and-Charge (“PnC”).[[6]](#footnote-7) Since this is an optional feature and competes with widely-implemented RFID and mandated credit/debit-card payment methods, many EVs and DCFC stations have been deployed without support for TLS. As a result, the vast majority of ISO 15118-based charging sessions to date have used unprotected TCP/IP streams for charging control. The security consequences have not been dire, but the vulnerability is well known in the community and researchers have explored a range of obvious exploits.

ISO 15118 has another significant security vulnerability: even when TLS is used, the HomePlug Green PHY signal (and thus, the entire control messaging stream) is susceptible to interception, interference, and denial of service. The charging cable acts as an antenna, rendering the system an unintentional radiator and receiver; the endpoints therefore become susceptible to a preamble attack; other serious exploits of this vulnerability seem possible.[[7]](#footnote-8)

### Inductive (VLF, LF) charging using non-standard wireless communications

The AC and DC charging communications described so far control conductive charging over a cable. EVs can also be charged in a wireless manner with power transfer via induction. (We only consider the static case, when the vehicle is stationary during charging.[[8]](#footnote-9)) Energy is transmitted over an air gap between coils in the infrastructure and the vehicle. In a typical implementation, the dispenser coil is embedded in the floor or in a moveable pad or platform, and a mating coil is mounted on the underside of the EV, as shown in Figure X1 [r1]. Charging is done by positioning the vehicle over the pad for optimal energy flow between the coils; this could be accomplished by moving either coil but typically uses automatic vehicle control (e.g. EV autonomous driving capabilities). Naturally, the communications used to control inductive charging is also wireless. Some commercially available systems send control signals on the energy transfer frequency (~25 kHz or 85 kHz), while another approach uses JSON messages over IEEE 802.11/Wi-Fi® for message exchanges governing coil compatibility and positioning.[[9]](#footnote-10)



## Hydrogen Surface Vehicle (HSV) fueling

Gaseous hydrogen fuel couplers support one-way infrared communication. Light Emitting Diodes (LEDs) in the coupler enable the HSV to advertise its fueling pressure (H35 or H70 service) using the IrDA protocol stack. The HSV can also send an ‘emergency/stop fueling’ message if an unsafe condition is detected. The dispenser can also detect an anomaly and shut down, but it doesn’t communicate the condition or its cause to the vehicle.[[10]](#footnote-11)

This introduces an obvious service and security vulnerability: blocking an infrared sensor on either the HSV inlet or the dispenser nozzle will render fueling impossible. A nuisance attack might use a small bit of duct tape, Blu-Tack, or chewing gum. A more serious attack, meant to cause monetary damage, might apply paint or permanent ink on a led lens. Perhaps the system designers believed the LED lenses would be hard to locate or reach, although their location is clearly described in a readily-available open standard.[[11]](#footnote-12) This exploit has been exercised in a lab setting with very little difficulty.

Next-generation HSV fueling protocols are being explored in ISO TC197. Candidates for the communication link between HSVs and dispensers include bi-directional infrared, NFC, and IEEE 802.11/Wi-Fi.

## Conclusions

### Almost all AFV fueling sessions use old, stale, not secure communications standards and technologies at the point of delivery (dispenser 🡨🡪vehicle).

### Security is almost exclusively physical; where digital security is required for EV charging, it currently relies on deprecated standards and often fails.

### There is plenty of room for improvement!

# Use cases for IEEE 802 LAN/MAN standards in AFV fueling infrastructures.

## EV charging: depot and public charging sites – passenger/delivery EV charging.

### Robotic control of a conductive coupler.

* Using WLAN (802.11, perhaps in p2p; also 802.11)
* Revise to use more recent 802.11 version/features, better architecture?

### Wireless control of inductive charging.

* Using WLAN (802.11, 802.15) for
* Could replace current, proprietary communications methods.

### Wireless LAN (802.11, 802.15) connecting EVSE/dispensers with site- or cloud-based energy/charging services management systems.

* Could support asset management, optimize energy use, enhance service delivery and fleet logistics.
* LAN configuration sketched in OPCC V2.x (Local GatewayLocal Proxy) but no technical specification or requirements [check draft OCPP 2.1]

### Wireless LAN (802.11, 802.15) for valet parking/charging service

* Use Next-Gen V2X communications (802.11bd) to connect EV to site-based auto-pilot server, direct EV to available and suitable EVSE
* On a separate WLAN or a VLAN on a multi-service WLAN (e.g. supporting use case 3.a.iii).

## EV charging: depot and public charging sites – Medium/Heavy Duty EV charging.

### L1-2 standard for the Megawatt Charging System (MCS)

* Replace HomePlug GP at Layer 1-2 with SPE (IEEE 802.3cg, 10BASE-T1S)
* Being standardized by ISO TC22/JWG1/WG4 as ISO/IEC 15118-10.

### Site wired/wireless LAN connecting EV charging, DER, microgrid controllers.

* Supports next-gen EV charging energy resiliency requirements.
* Opportunity to use 802.1X and 802.1AE for industrial-strength security.
* Analogous to IEEE 802.1/IEC 60802 approach to evolving IACS comms.

## EV charging: integrated into Home and Building Energy Management Systems

### Opportunity for HEMS and BEMS systems to manage EV charging/BPT.

* EV charging is a new load category, growing in significance and impact.
* Potential for optimizing energy use via inter-device (source, load) micro-negotiations.

### Potential for EVs to provide energy services to homes, building sites, and property portfolios.

* Back-up energy during outages, replacing petrol/diesel fueled generators.
* Energy shifting/flexibility (e.g. responding to dynamic utility energy pricing).
* Participation in utility Demand Response programs (e.g using predictive analytics for aggregated loads).

## EV charging: Wireless Battery Management System

* Potential for IEEE 802.15.4 to replace proprietary wireless comms for EV battery module/pack management

## HSV fueling: dynamic two-way communications between vehicle and dispenser.

* Potential for IEEE 802.11 or 802.15 to replace IrDA standards
* Advantages in performance, security, functionality and performance, cost, supply chain, etc.

## EV Charging integrated into Energy Management Systems

* EV charging: integrated into Distributed Energy Resources Management System  
  < Describe how EV charging would be integrated into DERMS domain. >
* EV charging: integrated into Building Energy Management Systems  
  < Describe how EV charging would be integrated into BEMS domain. Also indicate if Smart Home/HEMS is a subset of BEMS, or its own separate domain? >
* EV charging: integrated into Grid-Level Energy Management Systems  
  < Describe how EV charging would be integrated into Grid EMS domain. Is this at the level of generation:load balancing? AFAIK this currently only exists at the bulk energy level. Would it therefore be centered on Automated Demand Response e.g. using OpenADR 2.0b/IEC 62746-10-1? Would it include aggregation of EV charging loads? Etc. >

# IEEE 802 network and system considerations

## Medium flexibility and extensibility

### Support for wired and wireless endpoints

* E.g. IEEE 802.3 and IEEE 802.11 stations in controllers, actuators
* MAC (Layer 2): common architecture, addressing, bridging, VLANs, etc.
* WSNs (IEEE 802.15) less integrated but might be applicable

## IEEE 802.15 for sensors and IoT

* IEEE 802.24 IoT Whitepaper?

## Network security and management (802.1)

### Benefits from mainstream IT industry tools, techniques, insights, support

### YANG models, netconf

* “Belt and suspenders” approach: 802.1X+802.1AE (MACSEC) provides link security for any/all upper-layer protocols
* Being applied in other domains (IACS; aviation; automotive?; IoT?)
* Framework for EV charging/energy-edge domain-specific Layer 2 profiles

## Extensibility/innovation of standards and technologies

* Example: auto industry driving SPE for 10Mbps-10Gbps, copper and fiber
* Example: MAC address randomization (802.11bh) for enhanced privacy
* Example: IEC 60802 profile of TSN for IACS

# Performance requirements

## A table of message length and duration per use case / link / network segment.

## Summary: 10-100-1000 Mbps will largely suffice in the near term.

# Supply chain and ecosystem considerations

## AFV industry needs would probably be met by high-mix low-yield suppliers

## We’re in the early days of radio (horizontal integration is just beginning)

# Conclusion

1. For a helpful description of Pulse-Width Modulation, see https://en.wikipedia.org/wiki/Pulse-width\_modulation [↑](#footnote-ref-2)
2. *Caveat*: this pertains only to links between dispenser and vehicle. Either device may have additional interfaces for communication with other e.g. cloud-based systems, for diagnostics, maintenance, other services, etc.; security considerations of these are not within our scope here. [↑](#footnote-ref-3)
3. For CHAdeMO, see https://en.wikipedia.org/wiki/CHAdeMO and https://www.chademo.com/  
    For GB/T, see <https://en.wikipedia.org/wiki/GB/T_charging_standard> and https://francis-press.com/index.php/papers/6333. [↑](#footnote-ref-4)
4. For CAN industry news and technical articles, see <https://can-cia.org/>. For a survey of vehicle CAN bus security issues and mitigations, see <https://pmc.ncbi.nlm.nih.gov/articles/PMC7219335/> [↑](#footnote-ref-5)
5. The last, definitive Version 1.1.1 of the HomePLug Green PHY specification is available here: https://web.archive.org/web/20180825120357if\_/https://www.homeplug.org/media/filer\_public/74/40/7440ccd5-8c66-49ed-a2ce-5ef661932c27/homeplug\_gp\_specification\_v111\_final\_public.pdf [↑](#footnote-ref-6)
6. The second version of ISO 15118 (-20) has stronger requirements for mutual TLS v1.3 protection of all EV-station control messages. However, if the TLS handshake fails the standard provides for fallback to TCP/IP without TLS, enabling an obvious protocol downgrade attack. [↑](#footnote-ref-7)
7. The HomePlug Green PHY / Ethernet preamble attack is documented here: <https://www.brokenwire.fail/> [↑](#footnote-ref-8)
8. There have been trials of dynamic wireless charging systems using energy transmitted by coils along or under a road segment to power a moving vehicle. Such solutions have not achieved market acceptance or growth. [↑](#footnote-ref-9)
9. See <https://www.sae.org/news/2020/10/new-sae-wireless-charging-standard-is-ev-game-changer> and https://www.sae.org/standards/content/j2847/6\_202009/ [↑](#footnote-ref-10)
10. The IdRA based protocol for HSV fueling, as well as the physical layer (LED, mechanical) details of the coupler, are specified in SAE J2799-2024: Hydrogen Surface Vehicle to Station Communications Hardware and Software, <https://www.sae.org/standards/content/j2799_202406> and [↑](#footnote-ref-11)
11. See SAE J2600-2015 <https://www.sae.org/standards/content/j2600_201510> and <https://www.energy.gov/sites/prod/files/2014/09/f18/fcto_webinarslides_intro_sae_h2_fueling_standardization_091114.pdf>, drawing on slide #17. [↑](#footnote-ref-12)