# Fast Charging Communication and Cybersecurity: A Technology Review

Jakob Löw, Kevin Mayer, Hans-Joachim Hof
CARISSMA Institute of Electric, Connected and Secure Mobility
University of applied sciences Ingolstadt
Ingolstadt, Germany
e-mail: {jakob.loew | kevin.mayer | hof}@thi.de

***Abstract*—With the increasing amounts of electric vehicles on the road, the demand for public charging stations increases as well. While alternating current (AC) is used for charging at home, direct current (DC) fast charging is commonly used when traveling long distances. Since DC fast charging requires higher level communication between vehicle and charging station, it provides an increased attack surface to both sides. This paper reviews communication standards and their implementations used in fast charging scenarios. Focusing on cybersecurity aspects of these communications, we cover current and future security measures built into the communication standards between vehicles and charging stations.**

***Keywords-charging; fast charging; ccs; iso15118; DC charging; electric vehicle; vehicle charging.***

## I. Introduction

Many countries are currently transitioning away from combustion engine vehicles towards battery electric vehicles. This transition is happening at a rapid rate, because buying an electric vehicle often gets incentivised through tax reductions or straight refunds [1]. With people buying more and more electric vehicles, the demand for charging infrastructure rises. In Germany, not only electric vehicles, but also the buildup of charging infrastructure got heavily subsidized by the government. This high demand and government incentives resulted in a rapid growth in charging station numbers, suppliers and operators [2]. Due to the rushed development, the cybersecurity of current charging stations is below average compared to other cyberphysical systems [3]–[5]. Recently, cybersecurity researchers investigating charging backend infrastructure have found a range of textbook vulnerabilities, such as SQL injection, cross site scripting or unauthenticated remote update procedures [3].

This paper focuses on DC fast charging stations. Because of their functional design, described in Section II-B, they have a demand for complex two-way communication with the vehicle for exchanging charging parameters and limits. While other works, such as Tu et al. [6] have already covered electrical and other aspects of fast charging stations, this paper will focus on communication aspects. The ISO15118 standards [7], [8] was created for communication between charging stations and vehicles, enabling interoperability between stations and vehicles from different manufacturers. This high level communication protocol provides a larger attack surface compared to other charging techniques, making it more interesting for cybersecurity reserarch.

This paper will first lay out the communication principles and handshake flow of ISO15118 and related standards in Section II. Afterwards, a review of today's charging station vendors and architectures is given in Sections III and IV, respectively. Lastly, different attack vectors and research gaps of charging communication are discussed in Section V.

## II. Charging Station Communication

Electricity generally comes in two forms: Alternating Current (AC) and Direct Current (DC). While power grids are running on AC, batteries need to be charged using DC. Therefore, the AC needs to be converted to DC either in the car or in the charging station itself. Cars usually come with an onboard AC to DC converter for charging the onboard battery, their power is usually limited to 7 to 22 kW. In order to achieve higher charging powers, a fast charging station provides a stationary AC to DC converter. Placing it outside of the car removes weight requirements, simplifies cooling and thus allows higher charging currents.

In general, charging stations can be divided into three categories: Unmetered AC charging (often used in residential buildings), Commercial AC charging stations and DC fast charging stations. The following subsections describe the communication and payment mechanisms of these three kinds of charging stations as well as the included security concepts.

### *A. Low Level Communication*

AC charging stations usually supply power from the grid directly, making them just sockets with some very basic communication to the vehicle. In the early days of electric vehicle adoption, mainly these kind of charging stations were built. Because charging a modern vehicle using an AC charging station can take multiple hours, they usually are not used for long distance traveling. Because of their low price and low electrical requirements, they are however still widely used and newly installed, especially for home and office charging as well as on park and ride parking lots.

The most common plug for AC charging by far is the type 2 connector shown in Figure 1. It is used not only as the standard charging plug in Europe, but also in China and other parts of Asia. Apart from the typical connections of a 3-phase power socket, the connector incorporates two additional pins: Charge Pilot (CP) and Proximity Pilot (PP). These two pins are used for a very simple resistor based signaling scheme defined in IEC 61851 [9] and explained by [10]: The charging cable includes a resistor between proximity pilot and Protective Earth (PE), which signals the maximum current for this cable. The charging station supplies a +12V/-12V Pulse

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-206-7

Width Modulation (PWM) signal between CP and PE. The vehicle contains both a diode and a resistor between CP and PE, such that the charging station can detect the presence of a vehicle based on the negative voltage being dropped by the diode and the positive voltage being reduced by the resistor. As soon as the vehicle is ready to charge, it connects a second resistor between CP and PE further reducing the voltage. For unmetered AC charging this is sufficient to start a charging session. For public AC charging infrastructure usually external means of payment, such as mobile app activation or contactless payment have to be used before the session is started. During the charging session the charging station tells the vehicle the maximum allowed current through changing the duty cycle of the +12V/-12V PWM signal between CP and PE. There exists a special PWM duty cycle of 5%, which can be used by the charging station to tell the vehicle to use the high level ISO15118 protocol for communication rather than the low level communication described in IEC 61851 [9].

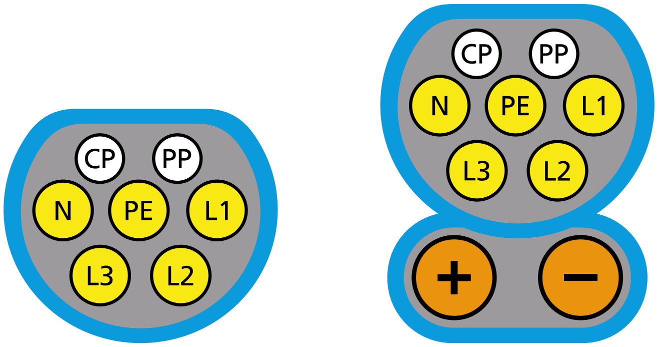

Figure 1. Schematic diagrams type 2 (left) and combined charging system (right) connectors [11]

### B. High Level Communication

While charging a vehicle with AC requires little to no communication, DC charging stations on the other hand are required to communicate to the vehicle for properly supplying the correct voltage and power to the battery. For this high level communication, the industry standard ISO15118 [7] was created, enabling interoperability between different vehicle manufacturers and charging station vendors. The standard is based on more or less common standards for all layers of the Open System Interconnect (OSI) model: After the initial handshake of the low level communication, as described in the previous section, the charging station signals the vehicle to use high level communication by supplying a PWM duty cycle of $5\%$. Afterwards, a powerline communication is modulated on top of the PWM signal between the charge pilot and protective earth. To prevent crosstalk problems [12]–[14] usually arising with powerline communication, ISO15118-3 [8] describes “Signal Level Attentuation Characterization” (SLAC). SLAC measures the interference on the powerline communication line as well as matches vehicles with their nearest charging station connected to the powerline and exchanges a network key for encryption. Once powerline communication is established, IPv6 with link-local stateless autoconfigured addresses is used on top for communication between the charging station and the vehicle. While the ISO15118-2 standard [7] itself is based on the Transmission Control Protocol (TCP), first a User Datagram Protocol (UDP) broadcast service discovery is used for exchanging IPv6 addresses as well as the port to connect to. Afterwards the TCP connection is established, and from there on used for transmitting actual payloads required for starting a charging session and controlling charging limits. For encoding payloads on this TCP connection the standard defines a “Vehicle to Grid Transfer Protocol” (V2GTP) packet format, which apart from some metadata contains one large payload blob encoded in the “Efficient XML Interchange” (EXI) format.

The ISO15118-2 standard defines a list of request messages sent from the vehicle to the charging station and corresponding response messages sent from the charging station to the vehicle. Before charging can start, payment and precharging have to be performed. For payment, the vehicle first asks the charging station for supported payment methods. As of today, mostly the `external` payment method is used, which requires the user to pay through an app, RFID card or electronic cash. The standard also supports certificate based authentication, which will be covered in the next section.

After payment was successful, the charging station performs insulation checks on the charging cable. Afterwards, the precharge procedure is initiated. During precharge, the charging station supplies a voltage to the charging cable, without the main battery contactor relay being closed in the vehicle. The precharging procedure makes sure the voltage present at the cable matches the battery voltage, reducing in rush current and reducing wear on the contactor relay.

After precharging the main charge loop is initiated, consisting of two packets used repeatedly: `CurrentDemandReq` and `CurrentDemandRes`. The first one is sent by the vehicle to request a specific voltage and current flowing into the vehicles battery. The latter one is sent by the charging station informing the vehicle about currently measured voltage and current as well as the charging stations limits. For example, the car might request a voltage of $369V$ and a maximum current of $400A$ resulting in a desired charging power of $148kW$. While the voltage has to be met, depending on the charging stations maximum output power the current might be lower than the requested value, resulting in a slower charging speed.

This main charge loop is repeated until one of the two parties terminates the charging session, opening the main contactor and disabling all current flowing into the battery.

### C. ISO15118 Security Concepts

While the most commonly used scheme for the charging communication is based on plain TCP, the ISO15118 standard also allows to use Transport Layer Security (TLS) for encrypted communication. Using the UDP broadcast packet, the vehicle can signal support for TLS encrypted communication. If the charging station also supports TLS encryption it signals

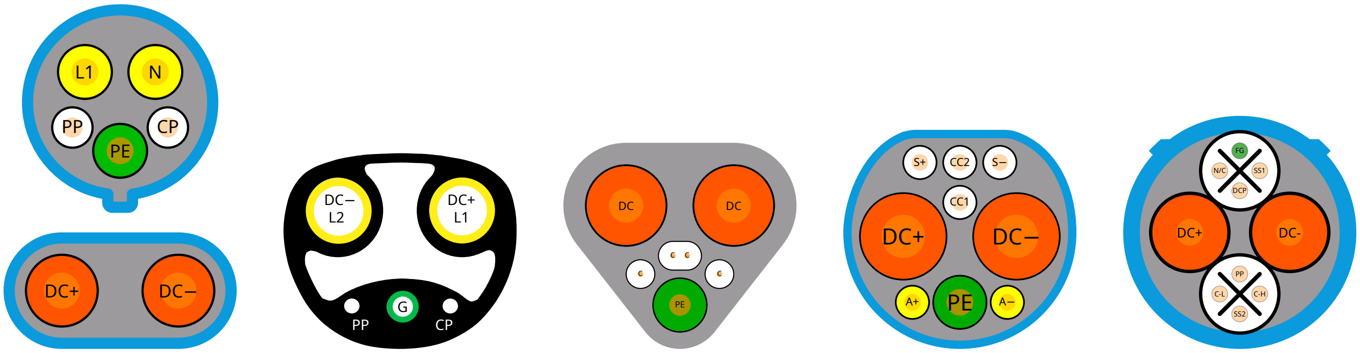

Figure 2. Schematic diagrams of other fast charging connectors. From left to right: Type 1 CCS [15], NACS [16], MCS [17], GB-T [18], Chademo [19]

this to the vehicle in the UDP response including a port to connect to using TLS. While TLS provides a secure way of communication, in order to handle authentication, it requires a Private Key Infrastructure (PKI) to sign and distribute certificates. ISO15118 describes a potential layout of this PKI handing out certificates to vehicle manufacturers and charge point operators, but does not name a specific entity managing this PKI.

### D. Other Communication Standards

While type 2 and combined charging standard (CCS) are the most used plugs for passanger cars in Europe, there do exist some other plugs and charging standards for fast charging battery electric vehicles. In total there are five other major plugs used for fast charging around the globe, listed below and shown schematically in Figure 2:

1) Type 1 CCS formerly used in North America
2) NACS future north american charging standard
3) Megawatt Charging System (MCS)
4) GB/T charging standard used in China
5) CHAdeMO used in Japan

While Europe has the type 2 connector for three phase AC charging, America uses a different connector called type 1, since their power grid is usually not based on three phases. There exists a type 1 CCS connector, adding two pins for DC charging, similarly to type 2 CCS. Since communication is identical they can both be referred to as “CCS connectors”, or specified as “CCS1 connector” for the American version and “CCS2 connector” for the European version. Similarly the megawatt charging system is also based on ISO15118, but uses a different connector, allowing higher currents and thus faster charging intended for trucks and buses. After Tesla open sourced their proprietary connector in 2022 [20] it became quickly adopted by car manufacturers and charging station operators for vehicles sold in America. While its socket is different, it is also based on ISO15118 communication described above.

GB/T and CHAdeMO are the charging standards used in China and Japan, respectively. They use CAN bus for communication rather than powerline making their implementation easier and cheaper, while disallowing advanced use cases ISO15118 provides. Since electric vehicle sales are much higher in Asia than in Europe and North America [21], the worldwide market share of vehicles with GB/T and CHAdeMO sockets remains significant nevertheless their usage only in China and Japan. According to Blech [22] at the end of 2019 the combined market share of GB/T and CHAdeMO was 55%. Figure 3 shows the market share of all connectors.

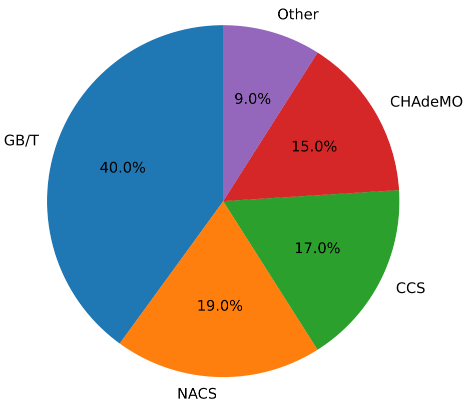

Figure 3. Charging socket market share at the end of 2019, based on Blech [22]

## III. Charging Station Vendors

After the standardization of the type 2 connector in 2009 and even after the introduction of CCS in 2014 most charging stations built offered only AC charging. Since AC charging stations include mostly components also found in home and industrial electric installations, companies active in the field of electric components and installations, such as Mennekes, Hager and E.ON, started building AC charging stations [10].

After CCS connectors became more popular in electric vehicles and the demand for high power fast charging grew [23], some companies started developing and producing DC fast charging stations. While AC charging stations rely on

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-206-7

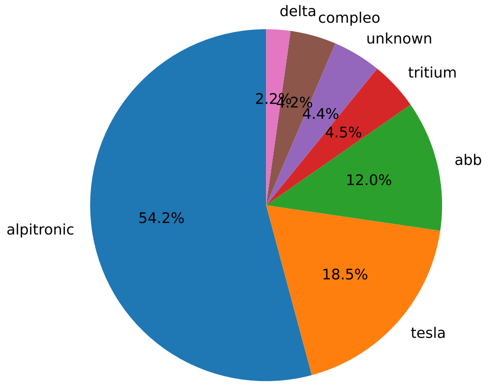

Figure 4. DC charging station vendor market share in Germany

simple components, DC charging stations are more complex, incorporating AC to DC conversion, high level communication and cooling equipment. While the market of AC charging station manufacturers is quite diverse, the complexity of DC charging causes only a handful of companies to produce significant numbers of high power charging stations.

As a part of this research we analyzed the current market share of DC charging stations in Germany. The largest registry of charging stations in Germany is goingelectric.de. This community led effort manages an interactive map as well as an API to fetch positions and metadata for each charging point. Each datapoint in the goingelectric database includes information about the manufacturer and model of the corresponding charging station. By analyzing the counts of all CCS based charging stations in Germany per manufacturer, we calculated the relative market share for each manufacturer.

With currently over 6000 DC charging points Alpitronic manufactured over 50% of todays DC charging stations in Germany. Second place is Tesla with its own supercharger devices and self managed charging network making up 18.5%. ABB is the only traditional electric installation company active not only in the AC charging station market, but also producing DC charging stations, making up 12.0% of all DC charging stations currently installed in Germany. With only three other companies having above 1% market share and Tesla not selling to third parties, the current DC charging station market is dominated by Alpitronic leaving behind well known companies like Siemens, Volkswagen and Porsche Engineering below the 1% mark. Figure 4 shows the market share of all manufacturers currently used in Germany, which have more than 1% market share.

## IV. Charging Station Architectures

While the interface between vehicle and charging station is standardized, the communication with other electric components making up a charging park is not. Other research has already extensively covered different electrical aspects and their attributes in regard to battery charging [6], [23], [24]. While the details of high power electronics are hardly relevant to this technology review, some of their attributes influence charging station architecture as well as communication aspects with other systems.

Since electric vehicle power demand is not linear during a charging cycle [25], DC charging stations often share AC to DC power conversion electronics between multiple outlets. For example, Alpitronic chargers contain two to four AC to DC power conversion modules and typically include two CCS outlets. When two cars are being charged at once, rather than statically assigning conversion modules to outlets, the modules are dynamically switched between outlets. This switching allows the charge power to be distributed unevenly between both vehicles based on the demand of each vehicle, effectively increasing the maximum output per outlet without increasing the total amount of conversion modules.

The first three generations of Tesla superchargers used a similar load sharing technique. The new v4 superchargers feature larger conversion modules converting AC grid power to DC and one DC to DC conversion module for each supercharger outlet.

Apart from the internal communication and power management required to service multiple vehicles from one charging station, most charging stations are essentially independent systems, with no external communication. While integration with external power providers such as solar and stationary battery storage promises to be beneficial for grid optimization [24], we could find only little evidence of charging stations communicating with external devices other than through standardized charging protocols.

## V. Attack Vectors and Impact

There already exists some research regarding the security of charging stations. Most of them however focus either on high level risk assessments [5], [26]–[31] or target aspects of vehicle charging other than DC fast charging communication [3], [32]–[34]. The following subsection describes some of the few attacks successfully carried out against DC charging communications. Afterwards, general problems with implementing the security concepts defined in ISO15118 are discussed.

### A. Low Level Communication Attacks

One attack vector of the ISO15118 standard is targeting the low level powerline communication used as a physical layer. Baker et al. [35] first described an attack on the powerline communication, eavesdropping electromagnetic interference produced by the modulated powerline packets on top of the PWM signal described in Section II-B. While their approach was not reliable enough to capture all of the traffic between charging station and vehicle, they were able to extract the powerline network key exchanged during SLAC, allowing to decrypt further communication.

Another attack on the powerline communication demonstrated by [36] performs a denial of service by jamming the

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-206-7

powerline communication signal. Since this attack effectively terminates the currently running charging session, the user has to re-authenticate and restart charging manually afterwards.

### *B. ISO15118 Security Implementation*

As described in Section II-C, the ISO15118 standard uses TLS for securing communication and even for payment authentication.

Support for TLS is signaled by the vehicle and confirmed by the charging station during the UDP based discovery and handshaking. Since this initial communication is neither encrypted nor authenticated, a potential attacker can easily perform a TLS-downgrading attack, effectively disabling encryption in all further communication.

Another problem with the standard lies in it not naming a company or institute handing out certificates required for TLS communication. As of today there are at least four different companies that created a PKI and allow third parties to acquire certificates [37]–[40]. Normally a certificate authority simply provides certificates for a service provider, for example for a website. With ISO15118 however, the vehicle requires a matching client certificate for authenticating. Thus while having multiple certificate authorities is generally a good idea, it creates a maintenance overhead for both vehicle manufacturers and charging station operators in order to support all authorities. Because of this complexity, as of today the vast majority of all charging communication sessions is not encrypted at all. Since TLS is required in order to use plug and charge (PnC), users have to use external payment menthods such as smart cards or apps rather than PnC. While PnC promises to improve usability and thus overall technology acceptance, the nature of the TLS implementation details set by the ISO15118 charging standard hinder its spread and is thus rarely used today.

## VI. Conclusion

As discussed in this paper, the market of both AC and DC charging stations is growing rapidly. Even though DC fast charging stations come with additional security implications, cybersecurity has not been a focus of the charging station industry in the past, leading to many textbook vulnerabilities in charging infrastructure. In the recent past this situation is starting to improve, with various institutions publishing guidelines and plans on securing charging infrastructure [41], [42].

While this is a step in the correct direction, a lot of low hanging fruits in regard to security research of DC charging stations remain untouched. This is underlined by the fact, that most scientific publications covering cybersecurity of charging communication are purely theoretical. While some AC charging stations and some web based services have been targets of security research, little research has been done targeting DC fast charging stations nor their communication with vehicles.

In future work, our plan is to perform penetration testing on charging station communication implementations both manually and using automated pentesting techniques. The goal of our future research will be to not only identify vulnerabilities in implementations, but also identifying general problems with the ISO15118 standard. One promising approach we are currently working on is to use state of the art fuzzing techniques for automatically identifying edge cases in the protocol and its implementations.

## Acknowledgment

This work was created in the research project “Elektromobiles Sicheres Laden” (ESiLa) funded by the Bavarian Ministry of Economic Affairs, Regional Development and Energy under grant DIK0512/01.

## References

[1] Kraftfahrtbundesamt (English: Federal Motor Transport Authority), *Anzahl der Elektroautos in Deutschland von 2006 bis Januar 2024 (English: Number of electric cars in Germany from 2006 to January 2024)*, https://www.kba.de/SharedDocs/Downloads/DE/Pressemitteilungen/DE/2024/pm_08_2024_bestand_01_24_merkmale_excel.xlsx?__blob=publicationFile&v=6, Mar. 2024.

[2] Bundesnetzagentur (English: Federal Network Agency), *Anzahl der öffentlichen Ladepunkte in Deutschland von Januar 2017 bis Oktober 2023 (English: Number of public charging points in Germany from January 2017 to October 2023)*, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/E_Mobilitaet/Ladesaeuleninfrastruktur.xlsx?__blob=publicationFile&v=5, Feb. 2024.

[3] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, “Power jacking your station: In-depth security analysis of electric vehicle charging station management systems,” *Computers & Security*, vol. 112, p. 102 511, Jan. 2022, ISSN: 0167-4048. DOI: 10.1016/j.cose.2021.102511.

[4] J. Johnson, T. Berg, B. Anderson, and B. Wright, “Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses,” *Energies*, vol. 15, no. 11, p. 3931, Jan. 2022, Number: 11 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 1996-1073. DOI: 10.3390/en15113931.

[5] A. Ahalawat, S. Adepu, and J. Gardiner, “Security Threats in Electric Vehicle Charging,” in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Singapore, Singapore: IEEE, Oct. 2022, pp. 399–404, ISBN: 978-1-66543-254-2. DOI: 10.1109/SmartGridComm52983.2022.9961027.

[6] H. Tu, H. Feng, S. Srdic, and S. Lukic, “Extreme Fast Charging of Electric Vehicles: A Technology Overview,” *IEEE Transactions on Transportation Electrification*, vol. 5, no. 4, pp. 861–878, Dec. 2019, Conference Name: IEEE Transactions on Transportation Electrification, ISSN: 2332-7782. DOI: 10.1109/TTE.2019.2958709.

[7] ISO/IEC, *ISO/IEC DIS 15118-2: Road vehicles - Vehicle to grid communication interface – Part 2: Network and application protocol requirements*, http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?ics1=43&ics2=120&ics3=&csnumber=55366, 2012.

[8] ISO/IEC, *ISO/IEC DIS 15118-3: Road vehicles - Vehicle to grid communication interface – Part 3: Physical and data link layer requirements*, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=43&ics2=120&ics3=&csnumber=59675, 2012.

[9] IEC, *IEC 61851-1 ed2.0: Electric vehicle conductive charging system - Part 1: General requirements*, http://webstore.iec.ch /webstore/webstore.nsf/Artnum_PK/44636, 2010.

ISBN: 978-1-68558-206-7

[10] M. Dalheimer, *Ladeinfrastruktur für Elektroautos: Ausbau statt Sicherheit (English: Charging infrastructure for electric cars: Expansion instead of safety)*, https://media.ccc.de/v/34c3-9092-ladeinfrastruktur_fur_elektroautos_ausbau_statt_sicherheit, Dec. 2017.

[11] Chris828, *Type 2 charging socket, VDE-AR-E 2623-2-2 plug*, https://commons.wikimedia.org/w/index.php?curid=89574378, Apr. 2020.

[12] A. Li, Q. Liu, J. Yang, and N. Zhou, "Crosstalk Analysis between Power Lines and Signal Lines Based on the Finite Difference-Time Domain Method," in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, Xi'an, China: IEEE, Oct. 2019, pp. 638–641, ISBN: 978-1-72811-722-5. DOI: 10.1109/APAP47170.2019.9224975.

[13] N. Theethayi, R. Thottappillil, Yaqing Liu, and R. Montano, "Parameters that influence the crosstalk in multiconductor transmission line," in *2003 IEEE Bologna Power Tech Conference Proceedings,*, vol. 1, Bologna, Italy: IEEE, 2003, pp. 388–395, ISBN: 978-0-7803-7967-1. DOI: 10.1109/PTC.2003.1304162.

[14] D. J. T. Ngo Bisse, D. B. G. Onana Essama, D. J. Koko Koko, P. J. Atangana, and P. S. Ndjakomo Essiane, "Crosstalk Characterization and Reduction in Power Lines," *International Journal of Inventive Engineering and Sciences*, vol. 10, no. 9, pp. 1–11, Sep. 2023, ISSN: 23199598. DOI: 10.35940/ijies.C7883.0910923.

[15] Mliu92, *Drawing of J1772 (CCS1 Combo) connector, with labeled pinouts.* https://commons.wikimedia.org/w/index.php?curid=108177318, Aug. 2021.

[16] RickyCourtney, *Drawing of North American Charging Standard connector, with labeled pinouts.* https://commons.wikimedia.org/w/index.php?curid=133111353, Jun. 2023.

[17] Mliu92, *Speculative diagram of Megawatt Charging System, version 3.2.* https://commons.wikimedia.org/w/index.php?curid=119080953, Jun. 2022.

[18] Mliu92, *GBT-20234.3 electric vehicle connector pinout for DC charging.* https://commons.wikimedia.org/w/index.php?curid=108206603, Aug. 2021.

[19] Mliu92, *CHAdeMO connector (viewed facing the plug that interfaces with the vehicle)*, https://commons.wikimedia.org/w/index.php?curid=108209697, Aug. 2021.

[20] *Opening the North American Charging Standard*, https://www.tesla.com/blog/opening-north-american-charging-standard.

[21] *Trends in electric cars – Global EV Outlook 2024 – Analysis*, en-GB, https://www.iea.org/reports/global-ev-outlook-2024/trends-in-electric-cars.

[22] T. Blech, "Project ChaoJi: The background and challenges of harmonising DC charging standards," *CHAdeMO Europe*,

[23] H. S. Das, M. M. Rahman, S. Li, and C. W. Tan, "Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review," *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109 618, Mar. 2020, ISSN: 1364-0321. DOI: 10.1016/j.rser.2019.109618.

[24] N. Deb, R. Singh, R. R. Brooks, and K. Bai, "A Review of Extremely Fast Charging Stations for Electric Vehicles," *Energies*, vol. 14, no. 22, p. 7566, Jan. 2021, Number: 22 Publisher: Multidisciplinary Digital Publishing Institute, ISSN: 1996-1073. DOI: 10.3390/en14227566.

[25] *Audi e-tron models with high charging performance.* https://www.audi-mediacenter.com/en/press-releases/audi-e-tron-models-with-high-charging-performance-12758.

[26] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3041074.

[27] A. Sanghvi and T. Markel, "Cybersecurity for Electric Vehicle Fast-Charging Infrastructure," in *2021 IEEE Transportation Electrification Conference & Expo (ITEC)*, Chicago, IL, USA: IEEE, Jun. 2021, pp. 573–576, ISBN: 978-1-72817-583-6. DOI: 10.1109/ITEC51675.2021.9490069.

[28] C. Assi, "Ensuring a Resilient and Secure EV Charging Infrastructure for Sustainable Transportation," in *2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, Cosenza, Italy: IEEE, Sep. 2023, pp. 1–1, ISBN: 9798350319514. DOI: 10.1109/ICT-DM58371.2023.10286958.

[29] M. Mahrukh and M. S. Thomas, "Load Altering Attacks-a Review of Impact and Mitigation Strategies," in *2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON)*, May 2023, pp. 397–402. DOI: 10.1109/REEDCON57544.2023.10150456.

[30] Y. Park, O. C. Onar, and B. Ozpineci, "Potential Cybersecurity Issues of Fast Charging Stations with Quantitative Severity Analysis," in *2019 IEEE CyberPELS (CyberPELS)*, Knoxville, TN, USA: IEEE, Apr. 2019, pp. 1–7, ISBN: 978-1-72812-925-9. DOI: 10.1109/CyberPELS.2019.8925069.

[31] K. Bao, H. Valev, M. Wagner, and H. Schmeck, "A threat analysis of the vehicle-to-grid charging protocol ISO 15118," *Computer Science - Research and Development*, vol. 33, no. 1, pp. 3–12, Feb. 2018, ISSN: 1865-2042. DOI: 10.1007/s00450-017-0342-y.

[32] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems," in *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA: Internet Society, 2023, ISBN: 978-1-891562-83-9. DOI: 10.14722/ndss.2023.23084.

[33] K. Sarieddine, M. A. Sayed, S. Torabi, R. Atallah, and C. Assi, "Investigating the Security of EV Charging Mobile Applications as an Attack Surface," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 4, 26:1–26:28, Oct. 2023, ISSN: 2378-962X. DOI: 10.1145/3609508.

[34] T. Nasr, "Large-Scale Study of Internet-Connected Electric Vehicle Charging Station Management Systems: Discovery, Security Analysis and Mitigation,"

[35] R. Baker and I. Martinovic, "Losing the Car Keys: Wireless {PHY-Layer} Insecurity in {EV} Charging," 2019, pp. 407–424, ISBN: 978-1-939133-06-9.

[36] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging," in *Proceedings 2023 Network and Distributed System Security Symposium*, arXiv:2202.02104 [cs], 2023. DOI: 10.14722/ndss.2023.23251.

[37] CharIN, *CharIN V2G PKI goes live!* https://www.charin.global/news/charin-v2g-pki-goes-live/, 2022.

[38] Hubject, *Download Public Key Infrastructure (PKI) | Hubject*, https://www.hubject.com/download-pki.

[39] nexusgroup, *Identities for Plug and Charge/vehicle-to-grid - V2G PKI*, https://doc.nexusgroup.com/pub/identities-for-vehicle-to-grid-v2g-pki.

[40] irdeto, *Irdeto Launches North American V2G Trusted Root CA to Accelerate Plug & Charge Adoption*, https://irdeto.com/news/irdeto-launches-north-american-v2g-trusted-root-ca-to-accelerate-plug-charge-adoption.

[41] J. McCarthy *et al.*, "Cybersecurity framework profile for electric vehicle extreme fast charging infrastructure," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, Tech. Rep. NIST IR 8473, Oct. 2023, NIST IR 8473. DOI: 10.6028/NIST.IR.8473.

[42] ENCS, "Security test plan for EV charging station," *European Network for Cyber Security*, 2019.