

Market-Analysis-Driven Methodology for Assessing Charging Station Cybersecurity

Jakob Löw^{*} , Lukas Eder^{*} , Alexander Müller, and Hans-Joachim Hof 

Technische Hochschule Ingolstadt, Security in Mobility,
Ingolstadt, Germany
`{jakob.loew, lukas.eder, hof}@thi.de`

Abstract. Modern charging communication standards for electric vehicles include optional security controls such as TLS-based authentication and encryption. However, with tens of thousands of fast charging points deployed in any given country, individually testing each one for security control support is infeasible. This paper proposes a scalable, extrapolation-based methodology for assessing charging station cybersecurity at a national level. A market analysis identifies operator-manufacturer pairs, enabling the targeted selection of charging stations for field testing, whose results can then be extrapolated to all stations sharing the same combination. We demonstrate this methodology for Germany, covering over 40000 CCS charging points as of December 2025. With a manageable number of field tests, our extrapolated data examines 51.9% of german CCS charging stations. It shows that only 27.4% of charging stations in our scope provide TLS-protected communication, despite widespread theoretical support.

Keywords: Security · Charging · ISO 15118 · Electric Vehicles · Plug and Charge · CCS · Fast Charging · Rapid Charging · TLS.

1 Introduction

Electric vehicles are becoming increasingly popular in Germany and the rest of the world [3]. While many users charge their vehicles at home or at work, fast charging stations are required on long-distance trips in order to minimize break times. Fast charging stations rely on high-level communication to keep the high-power charging process within safe limits, preventing battery damage and degradation. While this high-level communication enables convenience features such as automatic digital payment handled by the vehicle and the charging station, it also results in a larger attack surface for charging communication. Recent papers have demonstrated the feasibility of man-in-the-middle attacks [11, 12, 26] as well as payment fraud [4, 9] against charging communication. Although current charging communication standards already include security controls that

^{*} Both authors contributed equally to this work.

provide session authentication and could prevent such attacks, their use is currently optional. At present, there is no overview of what percentage of charging stations in the field today actually support these optional security controls.

Given the scale and heterogeneity of modern charging infrastructures, exhaustive security testing of all deployed charging stations is impractical. To address this challenge, we introduce an extrapolation-based methodology that leverages market structure and targeted measurements to assess the cybersecurity posture of charging infrastructure at national scale. By performing a market analysis, specific charging stations are selected, allowing extrapolation from a small number of tested stations to an overview of the current cybersecurity posture of charging communication. The methodology is based on two assumptions, which are validated later. Most charging point operators do not manufacture their own charging hardware. While there are thousands of fast charging stations in the field today, operated by hundreds of operators, the vast majority were built by a small number of manufacturers. The first assumption is therefore that charging stations manufactured by the same company support the same set of features, e.g. support for transport layer security (TLS). The second assumption is that two charging stations built by the same manufacturer and operated by the same company use the same configurations and thus support the same set of security controls. Together, these assumptions imply that testing one charging station allows the test results to be extrapolated to all stations built by the same manufacturer and operated by the same company.

We validate these assumptions and demonstrate the methodology for Germany, where it enables a qualified assessment of security control availability for more than half of all charging stations using a manageable number of field tests.

Our analysis reveals a significant gap between the security mechanisms defined in standards and their deployment in practice. While most charging station hardware supports TLS-based secure communication, only a minority of stations in the field actually enable and successfully use these mechanisms. This indicates that the current security posture of charging infrastructure is primarily limited by operational and configuration challenges rather than technical capabilities.

2 Charging Communication Security

In order to charge an electric vehicle, AC power from the grid has to be converted to an adequate DC voltage for charging the vehicle battery. In addition, safety parameters such as maximum current, temperature constraints, and voltage limits need to be followed. For fast charging stations, this AC to DC conversion happens outside of the vehicle, inside the charging station. Therefore, the vehicle needs to be able to communicate with the charging station and exchange safety parameters.

The leading standard for charging communication in Europe is ISO 15118 [17–19]. The standard builds on common communication protocols such as powerline communication, IPv6, and Transport Layer Security. Figure 1 shows the communication technology used in ISO 15118 for each of the open systems inter-

connect (OSI) model layers. The initialization steps, namely signal level attenuation characterization (SLAC) and the service discovery protocol (SDP), are designed specifically for charging communication. SLAC is used to form a joint powerline network between the vehicle and the charging station. Afterwards, SDP is used to exchange network addresses and to decide on the optional use of TLS for encrypting the main charging communication. Since SLAC messages are transmitted in plain text and SDP messages do not include means of message authentication, the initialization steps of ISO 15118 open up the possibility of misuse scenarios [4, 10, 11, 22, 26]. When both the vehicle and the charging station signal support for TLS, the main charging communication can be authenticated and encrypted using state-of-the-art algorithms. When TLS is used, the ISO 15118 standard also enables a special certificate-based automatic payment scheme. The use of TLS prevents potential attackers from impersonating a communication party or eavesdropping on the communication, significantly improving the security posture of a charging communication session.

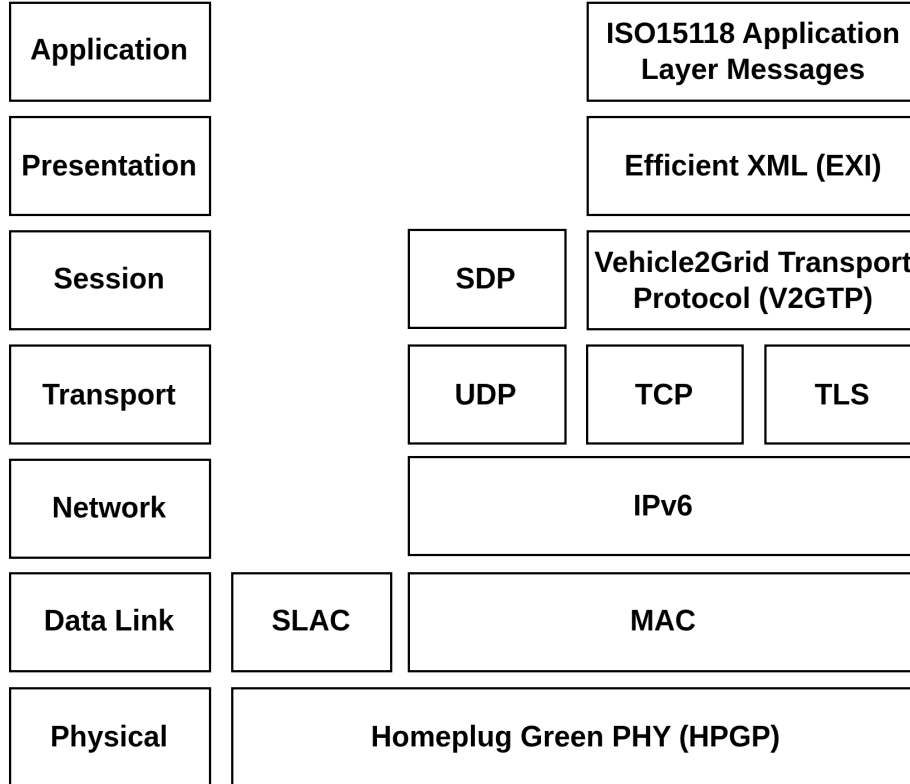


Fig. 1. Charging Communication OSI Layer Overview

For clear terminology throughout the paper, Figure 2 shows the participants in the charging process relevant to this work. Charging stations can have one or more charging points, i.e., can serve one or more vehicles at the same time. For comparability, we count individual charging points rather than charging stations, since stations can have varying numbers of points depending on manufacturer, model, and hardware version. Charging stations are often part of charging parks, each run by one charge point operator (CPO). Operators run multiple parks, resulting in larger operators operating hundreds or even thousands of charge points. The charging stations operated by a CPO also have a manufacturer, which is generally not the CPO itself. Most CPOs do not manufacture charging stations themselves; instead, they buy off-the-shelf models. Another participant in the charging process is the mobility operator (MO), which handles everything related to billing. Multiple roles (MO, CPO, manufacturer) can be held by the same party or company, but this is not required.

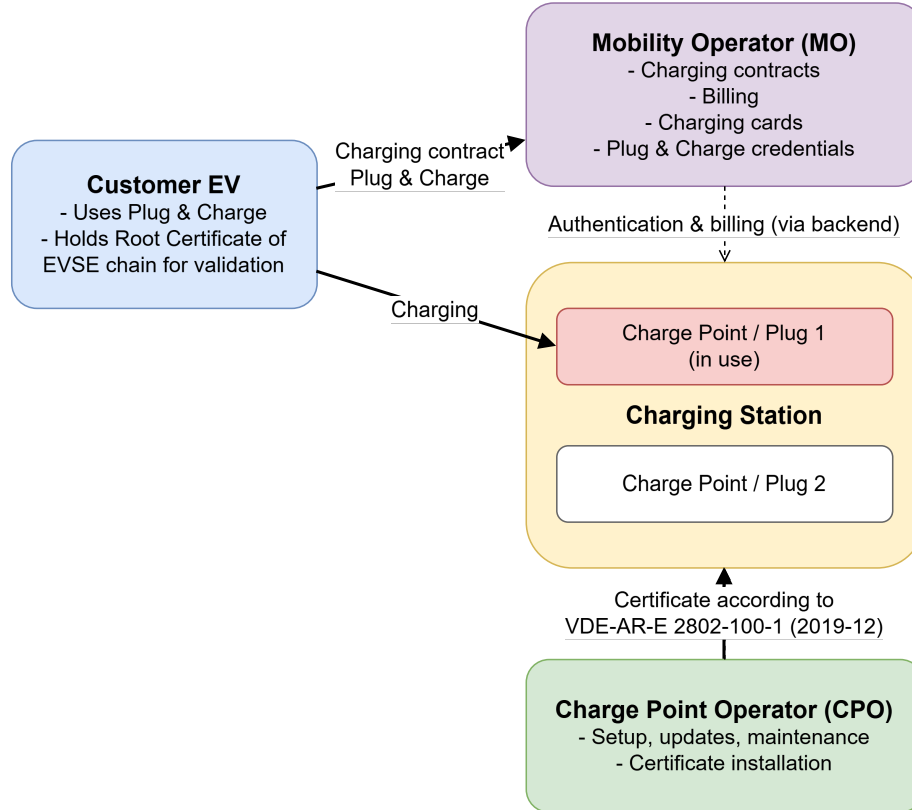


Fig. 2. Simplified overview of EV charging participants

3 Related Work

Prior surveys and threat analyses have examined the attack surface of ISO 15118 and CCS-based fast charging [6, 21, 22]. At the powerline and physical layer, concrete attacks have been demonstrated, including practical exploitation of HomePlug AV [10], powerline-based command injection against V2G charging [11], passive PHY-layer eavesdropping of CCS sessions [5], wireless denial-of-service via signal interference [20], and wireless SDR-based man-in-the-middle attacks including TLS stripping [26]. A separate line of work targets the powerline modems themselves: these have been shown to expose configuration and data-extraction interfaces over the powerline [25], a primitive that has subsequently been leveraged to install filter and firewall rules enabling sniffing and man-in-the-middle attacks on the charging session [12]. At the application layer, relay attacks against the charging protocol [9] and plug-and-charge payment-authentication relays [4] have been used to commit payment fraud. While most of these works propose new countermeasures alongside the vulnerabilities they identify, the basic security mechanisms already specified in the charging standards – most importantly TLS for authentication and encryption – are themselves only optional and require support from both the vehicle and the charging station to take effect. Whether deployed charging stations actually enable these standardized mechanisms is an empirical question that has so far received only limited attention; this paper argues that closing the deployment gap for these existing controls is at least as pressing as proposing new ones.

Szakály et al. [24] present the closest prior measurement study. The authors tested almost 400 charging stations across the United Kingdom, Switzerland, and Hungary for supported communication protocols and security controls. Their sample is opportunistic rather than stratified: stations were measured as accessible, without targeted selection by charge point operator or hardware manufacturer. As a result, their work establishes that TLS deployment varies significantly between operators and documents concrete configuration shortcomings, but it cannot quantify how prevalent each configuration is within a given country or region. The methodology proposed in this paper is designed for exactly this question: by stratifying field tests along the (CPO, manufacturer) dimensions that, as shown in Section 4.4, govern configuration in practice, we extrapolate from a small sample to national-scale deployment estimates. The two approaches are complementary; we in fact incorporate 25 of the charging stations measured by Szakály et al. into our assumption-validation set in Section 4.4, where their cross-country measurements of overlapping CPOs strengthen the case that configurations are consistent within a (CPO, manufacturer) pair across borders.

4 Market Analysis Methodology

The proposed methodology combines a market analysis of the target region with targeted field testing and extrapolation to assess the cybersecurity state of charging infrastructure at scale. The goal is to identify all charging stations, their

manufacturers, and their operators, in order to select a minimal set of stations for field testing that maximizes extrapolation coverage. We demonstrate this methodology for Germany using openly available data sources, as described in the following subsections.

Extrapolating from a limited number of field-tested charging stations to a larger population requires two assumptions to hold:

- A1: Charging Stations of the same manufacturer support the same set of features, while the CPO controls which features are enabled through configuration and certificate provisioning.
- A2: CPOs use the same configuration on all Charging Stations from the same manufacturer.

The validity of these assumptions is empirically evaluated in Section 4.4 based on measurements across multiple manufacturers, models, installation years, and CPOs.

4.1 Extrapolation-Based Assessment Methodology

The methodology consists of the following steps:

Step 1 - Data Acquisition: Publicly available datasets are collected to obtain charging point locations, charge point operators (CPOs), and charging station manufacturers and models. In this work, data from the Bundesnetzagentur [7] and goingelectric.de [2] are used.

Step 2 - Data Preprocessing: The collected data is cleaned and normalized. This includes unifying inconsistent manufacturer labels (e.g., *Tesla* vs. *Supercharger*) and removing incomplete entries. The resulting dataset contains only charging points with known CPO and manufacturer assignments.

Step 3 - Clustering: Charging points are grouped into clusters based on their CPO and manufacturer:

$$\text{Cluster} = (\text{CPO}, \text{Manufacturer})$$

Each cluster is assumed to represent a homogeneous configuration domain.

Step 4 - Sampling Strategy: Clusters were ranked according to the number of charging points represented in the dataset. Starting with the largest clusters, charging stations were selected for testing within a reachable distance from our office. The selection aims to maximize coverage of charging points while minimizing the number of required tests.

Step 5 - Field Testing: Selected charging stations are analyzed using the proposed EV-side testing device. The following properties are evaluated:

- availability of TLS,
- supported communication protocols (DIN SPEC 70121, ISO 15118-2),

- presence of valid certificate chains.

Step 6 - Extrapolation: The results obtained from tested charging stations are extrapolated to all charging points within the same cluster. This is based on the assumption that charging stations within a cluster share identical capabilities and configuration.

Step 7 - Aggregation: The extrapolated results are aggregated across all clusters to estimate the overall security posture of the charging infrastructure, including TLS deployment rates and protocol distribution at national scale.

This structured approach enables scalable assessment of large charging infrastructures while requiring only a limited number of field measurements.

4.2 Data Collection

The proposed extrapolation of charging station tests requires quantified knowledge about charging points, manufacturers, and charge point operators. While official sources such as the charging station list provided by the federal network agency [1] exist, these include only operator and connector information and lack details about the hardware used. Therefore, the official data must be enriched with additional sources in order to obtain a fully featured dataset.

The German website *goingelectric.de* hosts a community of electric vehicle enthusiasts, including a forum, a wiki, and a curated map of charging stations. In addition to charging locations, users can add pictures and metadata to each charging point, such as supported charging power, manufacturer, and model. While the dataset includes information about some charging points in other countries, its main focus is on charging stations in Germany. As part of this research, we used the official *goingelectric* API as well as web scraping to download information such as charging station manufacturers and models.

Since the information about charging station manufacturers and models is added manually by individuals, the data required some manual sanitization. For example, some charging stations built and operated by Tesla are labeled as *Tesla*, while others are labeled as *Supercharger*. Out of 114078 CCS charging points present on *goingelectric.de* in December 2025, 44313 (or 39%) are located in Germany. Of these 44313 charging points, another 3364 (or 7.6%) do not have a charging station manufacturer labeled, leaving 40949 charging points for analysis.

For each of these charging points, the charging station manufacturer, the model, the CPO operating the station, and the corresponding mobility operator were extracted. In most cases, the charge point operator is identical to the mobility operator handling the billing of charging sessions.

4.3 Data Summary

The collected data shows a large number of small and medium-sized charge point operators. Many traditional companies active in the energy sector, such

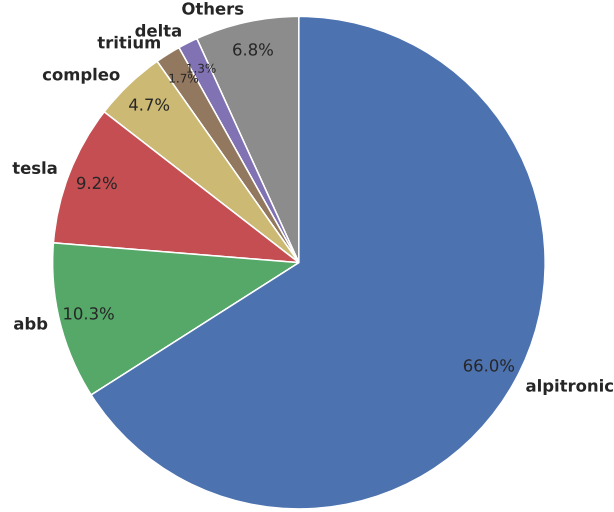


Fig. 3. Charging Station Manufacturers Market Share

as *EnBW*, *EWE*, *allego*, *innogy*, *Vattenfall*, *E.ON*, and *TEAG*, have invested in the electric vehicle charging market. Automotive players are also among the top charge point operators, including *Tesla*, *Volkswagen* (as *Elli*), and various other carmakers through *IONITY*. Retail chains such as *Lidl*, *Aldi*, *Kaufland*, and *Edeka* have built charging stations at their existing locations. Lastly, players from the fossil energy sector, such as *Aral* with *Aral Pulse* and *Shell* are also among the top CPOs in Germany.

Regarding charging station manufacturers, the collected data shows that nearly 66% of CCS charging points belong to charging stations built by a single manufacturer: *Alpitronic*. Both *ABB* and *Tesla* hold around a 10% market share of installed charge points in Germany. The remaining 14.5% are split among multiple smaller manufacturers. Figure 3 shows an overview of the manufacturer market share among all CCS charging points in Germany.

Many charge point operators use *Alpitronic* charging stations almost exclusively. As shown in Table 1, four of the five leading CPOs use Alpitronic charging stations for more than 90% of their charging points; the fifth is Tesla, which builds its charging stations itself. This concentration simplifies the planned security analysis of charging stations in Germany.

4.4 Validation of Extrapolation Assumptions

The proposed methodology relies on two assumptions: (A1) charging stations from the same manufacturer provide the same set of communication capabilities, and (A2) charging stations operated by the same CPO are configured consistently within each manufacturer group. For the validation, the extrapolation dataset was expanded with additional charging stations selected to maximize diversity in manufacturers, installation years, and deployment locations in order to identify potential counterexamples to these assumptions. The data used for the validation can be found in the repository linked at the end of section 6. In addition, existing data from [24] was used to verify and extend our validation data with EVSE tests in Hungary, the UK, and Switzerland.

Validation of A1 (manufacturer capability consistency). To evaluate (A1), charging stations from multiple manufacturers (Alpitronic, ABB, Tritium, Compleo, Efacec, EKOenergetyka, ChargePoint) were analyzed across different model generations and installation years (2018–2024). In all observed cases, charging stations from the same manufacturer supported the same set of communication capabilities at the protocol level.

In particular, no case was observed in which two charging stations from the same manufacturer differed in their capability to support TLS. Charging stations manufactured between 2018 and 2024 showed identical TLS capability within each manufacturer, including both older and newer hardware generations. This suggests that hardware revisions do not significantly affect the availability of the communication capabilities considered in this work.

Additionally, analysis of publicly available firmware documentation [14] indicates that different models of a major manufacturer share a common software platform and configuration interface, further supporting this assumption.

Validation of A2 (CPO configuration consistency). To evaluate (A2), multiple charging stations from the same CPO–manufacturer combinations were tested across different locations and installation years. In total, 16 charging stations from three major CPOs were analyzed:

- EnBW (Alpitronic): 8 stations across 5 locations
- Aral (Alpitronic, Compleo): 5 stations across 4 locations
- IONITY (Alpitronic, ABB, Tritium): 3 stations across 3 locations

Across all tested stations within each CPO–manufacturer pair, identical behavior regarding TLS support and supported protocols was observed, independent of installation year (2019–2025) and hardware model. This suggests a high degree of configuration standardization within each CPO.

To further support this observation, measurement data from [24] was incorporated. For overlapping CPOs (e.g., IONITY, Allego, Fastned), consistent configurations were observed across different European countries. This adds 25 additional charging stations (ABB and EKOenergetyka, 2018–2022) to the validation set.

Limitations. The validation is based on a finite number of sampled charging stations and may not capture all sources of variation. In particular, the following factors may influence the validity of the assumptions:

- configuration changes over time (e.g. certificate rollouts),
- regional differences within large CPOs,
- temporary misconfigurations or partial deployments,
- underrepresented small CPOs.

Therefore, the extrapolation results should be interpreted as an approximation of the current deployment state rather than an exact measurement. Nevertheless, the high consistency observed across all tested samples suggests that large-scale charging networks are operated with highly standardized configurations, supporting the feasibility of the proposed methodology.

Table 1. Charging Station Manufacturers per Operator

Operator	Points	Points (%)	Manufacturer	Points (%)
enbw	7593	18.5	alpitronic	96.1
			abb	3.0
tesla	3770	9.2	tesla	100.0
aral	2887	7.1	alpitronic	92.8
			volkswagen	6.9
ewe	1999	4.9	alpitronic	99.3
allego	1860	4.5	alpitronic	95.3
			efacec	4.2
pfalzwerte	1662	4.1	alpitronic	82.9
			enercharge	8.1
			abb	6.5
			siemens	2.2
newmotion	1573	3.8	alpitronic	59.8
			abb	35.0
			volkswagen	5.0
be.energised	1454	3.6	alpitronic	67.6
			ads-tec	13.3
			compleo	6.5
			abb	6.1
ionity	1363	3.3	ekoenergetyka	1.1
			tritium	48.3
			abb	32.9
			alpitronic	18.8
ladenetz	1355	3.3	alpitronic	58.2
			compleo	15.9
			abb	8.7
			enercharge	7.7
			ads-tec	4.0
			siemens	2.0
			delta	1.0

5 Charging Station Testing Device

To analyze the supported communication protocols and security mechanisms of CCS charging stations under real-world conditions, a dedicated charging station testing device was developed. The device is designed to emulate the EV-side communication behavior required for standardized high-level charging communication, while deliberately excluding any energy transfer functionality. This enables systematic, reproducible, and safe measurements of protocol support, TLS availability, and certificate deployment across different electric vehicle supply equipments (EVSE) without interacting with high-voltage components. The following subsections describe the hardware and software architecture of the testing device in detail.

5.1 Hardware Setup

We designed our testing device to be portable. It emulates the EV side required for charging communication analysis. The system can be operated in a fully mobile manner, requiring only the test device itself and an external power bank, which enables flexible deployment independent of fixed laboratory infrastructure.

A Raspberry Pi Zero 2 W serves as the central processing unit of the test device. It executes the complete communication logic and is responsible for recording and logging all exchanged data. To enable HomePlug Green PHY (HPGP) power line communication, a Codico RED-BEET-EVAL-BOARD-E 2.0 power line modem is integrated into the system. The modem is electrically connected to the Raspberry Pi via an existing SPI interface and a power connection, providing a compact and efficient communication link between both components.

The physical interface to the EVSE is realized using a modified Type 2 charging cable. Since the test device is exclusively intended for communication analysis, no DC power contacts are required. The communication process is intentionally terminated before the EVSE would enable any power transfer, thereby ensuring that no voltage is applied during operation.

Within the Type 2 connector, a set of resistors combined with switches is implemented to accurately reproduce the different CP-states as specified by the relevant standards. Furthermore, a diode is integrated into the connector to suppress negative voltage components of the PWM signal on the control pilot line. The PP resistor is statically implemented in the connector to represent a fixed cable current rating. The CP and PE conductors are directly connected to the power line communication modem.

Overall, the proposed hardware setup provides a complete emulation of the EV-side communication components required for charging while omitting high-power and high-voltage elements. This approach enables a portable analysis of the communication behavior between EV and EVSE in a controlled manner.

5.2 Software Setup

The charging station testing device implements a vehicle-side simulation of standardized charging communication between an EV and an EVSE for testing pur-

poses. The simulated communication supports DIN SPEC 70121, ISO 15118-2, and ISO 15118-20, thereby enabling a systematic and reproducible assessment of protocol compliance and security-related properties of charging stations.

The software strictly follows the normative communication sequence defined by the standards. This sequence comprises the SLAC coupling procedure, the service discovery protocol, the optional establishment of a secured communication channel using TLS, and the subsequent supported application protocol negotiation. These phases collectively determine the protocol stack, security mechanisms, and application profiles that are supported and selected for a charging session.

To systematically evaluate EVSE behavior under different communication and security configurations, the test process is executed in multiple independent test cycles. In each cycle, the simulated EV advertises a predefined set of communication capabilities and security requirements during the service discovery and protocol negotiation phases. The tested scenarios include:

1. Service discovery requests that require TLS exclusively, allowing the detection of TLS support and the availability of certificates at EVSE-side
2. Protocol negotiation requests for ISO 15118-2 without the use of TLS
3. Protocol negotiation requests without TLS that advertise all supported standards, including DIN SPEC 70121, ISO 15118-2, and ISO 15118-20
4. Protocol negotiation requests without TLS that advertise only DIN SPEC 70121

The first test allows the detection of TLS support and the availability of certificates on the EVSE side. Tests 1, 2, and 4 check for HLC communication protocol availability. Test 3 identifies the specific communication protocol selected by the EVSE when the EV supports all available protocol options.

All information relevant for protocol selection and security evaluation – including the supported and selected communication standards, the availability of secured communication, and the use of digital certificates – is exchanged during these early stages of the communication process. As no additional information required for the intended analysis is negotiated beyond this point, the test process is deliberately terminated after the successful completion of these steps. This controlled termination ensures that the charging session does not proceed to energy transfer, resulting in the desired behavior that the EVSE does not output charging voltage.

6 Test Results

Table 2 summarizes the observed protocol and security feature support across the analyzed CCS charging stations. As expected for CCS EVSEs, all tested charging stations implement DIN SPEC 70121 while most also support ISO 15118-2. In contrast, the practical use of TLS is limited. Although ISO 15118-2 allows TLS for secure communication, only a small fraction of the measured charging stations successfully established TLS-protected sessions. In most cases,

TLS was either disabled or not operational. Our extrapolation covers 51.9% of German charging stations and specifically shows that only 27.4% of them provide TLS-secured charging communication.

The measurement results suggest that the lack of TLS deployment is not caused by technical limitations of the charging hardware, but by challenges in certificate provisioning and trust management. This conclusion is supported by the observation that charging stations from the same product families – and in several cases even newer hardware revisions – exhibited differing TLS behavior. Specifically, EVSE models that did not establish TLS were observed alongside equivalent or older models from the same product line that successfully supported TLS, indicating that hardware capabilities alone do not explain the absence of TLS in practice.

For TLS to be accepted by the vehicle, the EVSE certificate chain must terminate in a root CA trusted by the EV. While on the web, obtaining certificates for encrypted communication is free and easy to automate, in the charging domain PKI providers usually charge a one-time fee as well as recurring fees for each charging station. This effectively hinders the use of TLS for secure charging communication.

At the time of writing, at least four operators of V2G public key infrastructures are known to provide trusted root CAs for ISO 15118 [8, 15, 16, 23]. However, within our dataset, only certificates issued under the Hubject V2G Root CA [15] were observed. All other stations either operated without TLS or failed to present a certificate.

TLS in ISO 15118 is mandatory when using plug and charge. Therefore, all networks that support plug and charge payment also support TLS. IONITY has supported plug and charge since October 2021 and appears to have updated chargers built before that date, providing them with the certificates required for successful TLS communication. Similarly, Aral introduced plug and charge in early 2022. Charging stations built before this introduction also support TLS, indicating updates after initial construction.

In general, support for TLS seems to be mainly driven by the introduction of plug and charge payment rather than security concerns. While in our dataset 27.4% of charging spots support TLS, we assume the real-world number to be even lower. Due to the required effort and upfront cost, plug and charge is currently mainly supported by large charging point operators. While our dataset includes both large and small operators, the distribution is not proportional to the total number of charging points installed. Small CPOs left out of the dataset are expected to have an even lower rate of support for TLS.

This expectation can be substantiated for a part of the remaining 48.1% of charging points not covered by our extrapolation. While in most cases the CPO also acts as the mobility operator handling billing, several mobility operators – *NewMotion*, *be.energised*, *Ladenetz*, and *innogy* – do not operate charging stations themselves, but instead allow third parties, typically small CPOs, to register charging stations within their network. None of these networks advertise support for plug and charge, which makes the availability of security controls

such as TLS in those charging stations unlikely. Our field tests of some CPOs that use these networks confirm this assumption. The same reasoning applies to the long tail of small CPOs and networks outside these mobility operator networks: each of them operates only a small number of charging stations, for which the integration effort and the one-time and recurring PKI fees required for plug and charge rarely pay off. We therefore expect the TLS deployment rate among the charging points outside our extrapolation scope to be considerably below the 27.4% observed within it.

As discussed above, this deployment gap is operational rather than technical: the hardware of all major manufacturers supports TLS, but enabling it requires certificate provisioning and trust management that many operators forgo. Regulatory incentives may close this gap in the future. The technical specifications adopted under the European Alternative Fuels Infrastructure Regulation (AFIR) [13] require newly deployed publicly accessible charging points to support ISO 15118-20 starting in 2027. Since ISO 15118-20 mandates the use of TLS, this requirement effectively enforces TLS deployment for new installations, although the existing infrastructure measured in this work remains unaffected.

Apart from the extracted results shown in table 2 we are also publishing all raw data gathered from various charging stations including communication dumps as well as model information on github: <https://github.com/M4GNV5/charging-station-tests-germany>

7 Conclusion

Our research shows a significant lack of support for security controls in chargers deployed in the field today. While current research continues to identify vulnerabilities and shortcomings in charging communication and to propose new security controls to prevent attacks, in reality most chargers do not support even basic authentication or encryption. While some operators have made the effort to support TLS, this appears to be a prerequisite for introducing plug and charge rather than a proactive step to improve the cybersecurity of the charging infrastructure. The current state of cybersecurity in charging communication appears to resemble that of the web years ago. Making TLS mandatory for all charging sessions could improve the confidentiality and integrity of charging communication.

The proposed market-analysis-driven methodology is not limited to Germany and can be applied to any country or region where charging station data is available, enabling comparable assessments of charging infrastructure cybersecurity elsewhere.

Future research could evaluate current certificate distribution techniques and investigate how a certificate enrollment process similar to the Automatic Certificate Management Environment (ACME) used for web servers could be integrated into the charging ecosystem. Similar to the service provided by Let’s Encrypt, an easy, automatic, and free way to obtain certificates could significantly accelerate the adoption of authentication and encryption in charging communication.

CPO	CPO %	OEM	OEM %	Cluster %	Model	Year	ISO 15118-2	TLS
EnBW	18.5	Alpitronic	95.9	17.7	HYC400	2023	✓	✗
					HYC300	2019, 2025	✓	✗
					HYC200	2024	✓	✗
					HYC150	2021, 2023	✓	✗
Aral	7.1	Alpitronic	92.8	6.6	HYC300	2021, 2023	✓	✓
		Compleo	0.1	0.0	Cito BM 500	2020	✗	✗
EWE	4.9	Alpitronic	99.3	4.9	HYC300	2021, 2022	✓	✗
allego	4.5	Alpitronic	95.2	4.3	HYC300	2022	✓	✓
pfalzwerke	4.1	Alpitronic	82.9	3.4	HYC150	2021	✓	✗
IONITY	3.3	Tritium	48.3	1.6	Veefil PK	2019	✓	✓
		ABB	32.9	1.1	HP CP500	2024	✓	✓
		Alpitronic	18.8	0.6	HYC400	2023	✓	✓
Lidl	2.4	ABB	79.2	1.9	Terra 60	2021	✓	✗
Elli	2.3	Compleo	95.7	2.2	Cito BM 500	2022	✓	✗
Mer	2.0	Alpitronic	90.8	1.8	HYC150	2021	✓	✗
Aldi	2.0	Alpitronic	98.8	2.0	HYC150	2021	✓	✗
Kaufland	1.7	ABB	92.4	1.6	Terra 54	2022	✓	✗
Edeka	1.1	Compleo	84.1	0.9	Cito BM 500	2021	✗	✗
fastned	0.8	Alpitronic	100	0.8	HYC300	2021	✓	✗
Circle K	0.7	ABB	65.0	0.5	HP CP500	2021	✗	✗
% Of All % Of Clusters	55.4			51.9			48.7	14.2
				100			93.8	27.4

Table 2. Test Results for various CPOs

Additionally, such an approach could help bring secure-by-default practices to charging communication, rather than requiring network operators to manually obtain and configure certificates for each charging station individually.

Acknowledgments. 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. Bundesnetzagentur - Ladesäulenkarte, <https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/E-Mobilitaet/Ladesaeulenkarte/start.html>
2. Dokumentation der Stromtankstellen API, <https://www.goingelectric.de/strom-tankstellen/api/docs/>, <https://www.goingelectric.de/stromtankstellen/api/docs/>
3. Open EV Charts. <https://open-ev-charts.org/>, <https://open-ev-charts.org/>, accessed: 30 June 2025.
4. Iso 15118 security controls, vulnerabilities and possible remedies. pp. 1–2 (2026)
5. Baker, R., Martinovic, I.: Losing the Car Keys: Wireless {PHY-Layer} Insecurity in {EV} Charging. pp. 407–424 (2019), <https://www.usenix.org/conference/usenixsecurity19/presentation/baker>
6. Bao, K., Valev, H., Wagner, M., Schmeck, H.: A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Computer Science - Research and Development* **33**(1), 3–12 (Feb 2018). <https://doi.org/10.1007/s00450-017-0342-y>, <https://doi.org/10.1007/s00450-017-0342-y>
7. Bundesnetzagentur: Anzahl der öffentlichen Ladepunkte in Deutschland von Januar 2017 bis Oktober 2023 [Graph], Bundesnetzagentur (Feb 2024), https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/E_Mobilitaet/Ladesaeuleninfrastruktur.xlsx?__blob=publicationFile&v=5
8. CharIN: CharIN V2G PKI goes live!, <https://www.charin.global/news/charin-v2g-pki-goes-live/>, <https://www.charin.global/news/charin-v2g-pki-goes-live/>
9. Conti, M., Donadel, D., Poovendran, R., Turrin, F.: EVExchange: A Relay Attack on Electric Vehicle Charging System. In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds.) *Computer Security ESORICS 2022*. pp. 488–508. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-031-17140-6_24
10. Dudek, S.: HomePlugAV PLC: Practical attacks and backdooring. *Netw. Anal.* (2015), https://penthertz.com/resources/NSC2014-HomePlugAV_attacks-Sebastien_Dudek.pdf
11. Dudek, S., Delaunay, J.C., Fargues, V.: V2g injector: Whispering to cars and charging units through the power-line. In: *Proceedings of the SSTIC (Symposium sur la sécurité des technologies de l'information et des communications)*. pp. 1–26. SSTIC, Rennes, France (2019), https://www.sstic.org/2019/presentation/v2g_injector_playing_with_electric_cars_and_charging_stations_via_powerline/
12. Eder, L., Löw, J., Hof, H.J.: Charging Communication Sniffing and Man-in-the-Middle Attacks. In: *Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems*. pp. 799–804. E-Energy '25, Association for Computing Machinery, New York, NY, USA (Jun 2025). <https://doi.org/10.1145/3679240.3734648>, <https://dl.acm.org/doi/10.1145/3679240.3734648>

13. European Parliament and Council of the European Union: Regulation (EU) 2023/1804 of the European Parliament and of the Council of 13 September 2023 on the deployment of alternative fuels infrastructure, and repealing Directive 2014/94/EU (2023), <https://eur-lex.europa.eu/eli/reg/2023/1804/oj>
14. GmbH, A.: hyperdoc | dashboard, <https://doc.hypercharger.it/>
15. Hubject: Download Public Key Infrastructure (PKI) | Hubject, <https://www.hubject.com/download-pki>, <https://www.hubject.com/download-pki>
16. irdeto: Open and secure ev charging, <https://irdeto.com/smart-mobility/crosscharge-ev-charging>
17. ISO/IEC: ISO/IEC DIS 15118-2: Road vehicles - Vehicle to grid communication interface Part 2: Network and application protocol requirements (2012), http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?ics1=43&ics2=120&ics3=&csnumber=55366
18. ISO/IEC: ISO/IEC DIS 15118-3: Road vehicles - Vehicle to grid communication interface Part 3: Physical and data link layer requirements (2012), http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=43&ics2=120&ics3=&csnumber=59675
19. ISO/IEC: ISO/IEC DIS 15118-20: Road vehicles - Vehicle to grid communication interface part 20: 2nd generation network layer and application layer requirements (2022), <https://www.iso.org/standard/77845.html>
20. Köhler, S., Baker, R., Strohmeier, M., Martinovic, I.: Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging. In: Proceedings 2023 Network and Distributed System Security Symposium. Internet Society, San Diego, CA, USA (2023). <https://doi.org/10.14722/ndss.2023.23251>, https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_s251_paper.pdf
21. Lee, S., Park, Y., Lim, H., Shon, T.: Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology. In: 2014 International Conference on IT Convergence and Security (ICITCS). pp. 1–4 (Oct 2014). <https://doi.org/10.1109/ICITCS.2014.7021815>, <https://ieeexplore.ieee.org/document/7021815>
22. Löw, J., Mayer, K., Hof, H.J.: Fast Charging Communication and Cybersecurity: A Technology Review (Nov 2024)
23. nexusgroup: Identities for Plug and Charge/vehicle-to-grid - V2G PKI, <https://doc.nexusgroup.com/pub/identities-for-vehicle-to-grid-v2g-pki>, <https://doc.nexusgroup.com/pub/identities-for-vehicle-to-grid-v2g-pki>
24. Szakály, M., Köhler, S., Martinovic, I.: Current Affairs: A Security Measurement Study of CCS EV Charging Deployments (Feb 2025). <https://doi.org/10.48550/arXiv.2404.06635>, <http://arxiv.org/abs/2404.06635>, arXiv:2404.06635 [cs]
25. Szakály, M., Köhler, S., Martinovic, I.: Short: PIBuster: Exploiting a Common Misconfiguration in CCS EV Chargers. pp. 243–249 (2025), <https://www.usenix.org/conference/vehiclesec25/presentation/szakaly>
26. Szakály, M., Strohmeier, M., Martinovic, I., Köhler, S.: Dception: Real-world Wireless Man-in-the-Middle Attacks Against CCS EV Charging (Jan 2026). <https://doi.org/10.48550/arXiv.2601.15515>, <http://arxiv.org/abs/2601.15515>, arXiv:2601.15515 [cs]