VicOne

Driving Automotive Cybersecurity Forward

Securing the Charge:

Hidden Risks in ISO 15118

Salvatore Gariuolo, Rainer Vosseler
FTR Research for VicOne

Trend Research

Introduction

The rapid rise of electric vehicles (EVs) is transforming global mobility, paving the way for a cleaner, more sustainable future. However, this shift is not without challenges. By 2040, more than 600 million EVs are expected to be on the roads, placing unprecedented pressure on electricity grids worldwide. Without proper management, this surge could lead to grid instability and disruptions in the energy supply, especially during periods of peak demand.

To address this challenge, the International Organization for Standardization (ISO) introduced ISO 15118, a standard designed to enable technologies such as smart charging and vehicle-to-grid (V2G) communication. These innovations aim to ease the strain on power grids while also improving the user experience of EV charging, making it more intuitive and, more importantly, more secure. However, while the standard mitigates several critical cybersecurity concerns, it also introduces new risks.

This research paper examines how ISO 15118 reshapes the cyberthreat landscape of EV charging infrastructure. We explore the risks it mitigates, shifts, and creates, and highlight how even well-intentioned standards and policies can create a false sense of security. In some cases, measures designed to strengthen protections can inadvertently leave threats unaddressed or even introduce new vulnerabilities.

Key takeaways

- ISO 15118 is designed to address grid-related challenges and improve user convenience. It also strengthens the security of the EV charging ecosystem by securing communication between EVs and charging stations and shifting sensitive operations from stations to e-Mobility Service Providers (eMSPs).
- The standard resolves several long-standing cybersecurity issues. However, it also leaves certain risks unaddressed and introduces new vulnerabilities, particularly through features such as smart charging and vehicle-to-grid (V2G) communication.
- Despite ISO 15118's improvements, charging stations remain among the most vulnerable components in the EV charging ecosystem. These weaknesses could compromise the very security the standard seeks to provide.
- No single standard can cover every threat surface. Robust security requires a coordinated, multi-stakeholder approach involving car manufacturers (OEMs), charging station manufacturers, grid operators, and eMSPs.

ISO 15118: A Strategic Response to the EV Surge

The problem: a grid under strain

The global transition to EVs is accelerating, and with it, the pressure on the electricity infrastructure. Projections suggest that by 2040, the number of EVs on the road will exceed 600 million, representing nearly 30% of the global vehicle fleet.[1, 2]

While this marks a significant milestone in the fight against carbon emissions, it also reveals a critical vulnerability: today's power grids were not designed to handle the corresponding surge in electricity demand. If a large number of EVs charge simultaneously, the grid could face serious strain, leading to voltage fluctuations, transformer overheating, and even localized blackouts.

This is not a theoretical concern; it is already happening. In the Netherlands, grid operator Stedin has proposed shutting down public EV chargers between 4 p.m. and 9 p.m. to prevent outages when the grid is under the most stress.[3] In the US, the California Independent System Operator (CAISO) issued a similar warning, asking EV owners to voluntarily reduce charging during hot days when air conditioning further increases electricity demand.[4] Without intervention, rapid EV adoption could threaten the very infrastructure that enables it.

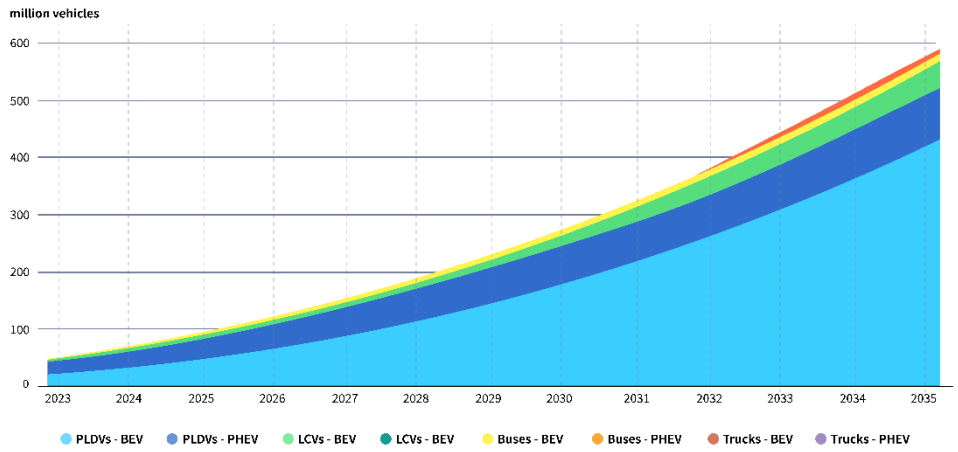

Figure 1. EV growth projections through 2035[5]

However, the grid strain is not caused by EVs alone. It is also a byproduct of the way we produce and consume electricity. A sharp imbalance between generation and demand can cause the grid's frequency to drift outside its safe operating range. The blackout that struck Spain in April 2025 illustrates this risk.[6] On some days, wind and solar power supply more than half of Spain's electricity needs.[7] But unlike fossil fuels and nuclear power, renewables are intermittent. Their output can fluctuate quickly with the weather, making it difficult to balance supply and demand in real-time. When there is excess electricity and there's no efficient way to store or redirect the

surplus, the grid becomes unstable. For this reason, large-scale battery storage parks are being built across Europe, such as the planned facility in Waltrop, Germany.[8]

To manage this volatility, grid operators also rely on price signals. When renewable output surges, electricity prices drop sharply, sometimes even turning negative. This encourages more consumption to absorb the excess supply. However, when increasing the consumption alone is not enough, generation must also be reduced. Unfortunately, power sources such as nuclear plants cannot lower their output quickly,[9] creating an oversupply that disrupts grid frequency, the system's electrical "heartbeat." In Spain's case, frequency drifted too far from the 50 Hz target. Although safeguards were in place to stabilize deviations, they were unable to respond fast enough.[10] As a result, the entire grid was disconnected to prevent a full-scale collapse.

The solution: smarter charging, more efficient grids

Upgrading the power grid may seem like the most straightforward solution to these challenges, but it comes with a hefty price tag. Global infrastructure upgrades could exceed $4.5 billion per year,[11] making this approach financially impractical. Fortunately, while EVs contribute to the strain on the grid, they can also be part of the solution. Technologies such as smart charging and V2G offer a way to balance demand with supply without costly infrastructure overhauls.

Smart charging, for example, is an approach designed to prioritize grid stability. Unlike conventional charging, which begins as soon as the EV is plugged in, smart charging considers real-time grid conditions. It determines the optimal time and rate to charge, ensuring EVs draw power only when the grid can support it. At the same time, it accommodates the charging needs and cost preferences of users. This means that charging can be discouraged during peak times through higher electricity prices. When demand peaks, higher electricity prices can discourage charging, shifting usage to times when energy is cheaper, such as periods of low demand or when renewables produce a surplus. The result is a win-win scenario: EV owners enjoy lower costs and the grid experiences reduced strain.

V2G communication takes a step further by turning EVs into mobile energy storage systems. Since private cars are parked around 95% of the time,[12] they represent a largely untapped resource. In situations like Spain's blackout, where surges in renewable energy can destabilize the grid, V2G technology can prove particularly useful. EVs can absorb excess electricity, with owners earning compensation for doing so, and later feed power back into the grid during high-demand periods. This transforms EVs into flexible, distributed energy storage assets, helping to build a more resilient and adaptive energy system.

This is where ISO 15118[13] comes into play. The standard establishes a framework that enables both smart charging and V2G, supporting grid stability as EV adoption continues to grow. But grid integration is only part of the story. Just as importantly, ISO 15118 streamlines the EV charging experience and strengthens security within the infrastructure. One of its key features, Plug & Charge, automates the entire charging process, from authentication to billing.

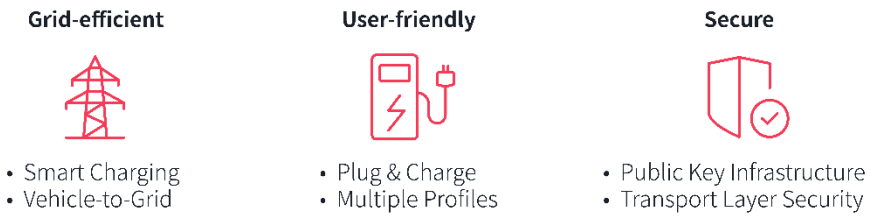

Figure 2. ***Key Features of ISO 15118.*** *Released in 2014, ISO 15118-2 introduced smart charging, Plug & Charge, and encrypted communication. The 2022 revision, ISO 15118-20, expanded the standard to include V2G capabilities.*

Plug & Charge uses a public key infrastructure (PKI) that relies on digital certificates to make EV charging more seamless and more secure. Each vehicle stores one or more certificates linked to the owner's account, which are automatically verified when the EV is plugged into a charging station. This confirms the owner's identity and authorizes the session, eliminating the need for RFID cards, apps, or manual payment steps.

To further safeguard sensitive data, ISO 15118 employs Transport Layer Security (TLS), encrypting communication between EVs and charging stations. This ensures that the authentication data, billing details, and other sensitive information remain protected throughout the charging session.

But like any standard, ISO 15118 comes with trade-offs. While solving several critical challenges, it also opens the door to new complexities and potential risks, which will be explored in the next section.

How ISO 15118 Changes the Threat Landscape

With its innovations, ISO 15118 significantly strengthens the cybersecurity posture of the EV charging ecosystem. However, it does not eliminate all risks. Some threats persist, others shift to new actors, and new vulnerabilities emerge as unintended consequences of the standard's innovations.

Understanding these nuances is essential to fully grasp the impact of ISO 15118 . We need to examine the key changes the standard introduces to the EV charging ecosystem to better comprehend how it redefines the cybersecurity landscape and why it can create a false sense of security.

Mitigated risks: Securing communication between EVs and charging stations

One of ISO 15118's most significant contribution is securing the communication link between EVs and charging stations. This helps mitigate several long-standing vulnerabilities, including unauthorized charging sessions and session hijacking.

In the past, unauthorized charging sessions were surprisingly easy to execute. Many charging stations relied on RFID cards for authentication, which could be stolen or cloned, allowing bad actors to charge their EV at another user's expense. For example, MIFARE Classic RFID tags have been proven to be easily cloned using inexpensive equipment.[14] ISO 15118 addresses this risk through Plug & Charge, which leverages PKI-based digital certificates stored in the vehicle to replace vulnerable physical tokens. As long as the encryption remains intact, attackers have very limited options. They would need to tamper with the vehicle's hardware to extract its private key or compromise the certificate authority to generate fraudulent credentials, both of which are extremely difficult to pull off.[15]

Session hijacking posed another major challenge. Prior to ISO 15118, communication between EVs and charging stations was often unencrypted, leaving sensitive data such as session IDs and charging parameters exposed in plain text.[13] Attackers could eavesdrop on this data by modifying the charging cable and then resuming or extending another user's session. This vulnerability persisted even in ISO 15118-2, which prioritized cost and convenience over full security. The standard, in fact, allowed unencrypted communication in certain scenarios, such as workplace stations or residential chargers using External Identification Means (EIM).[15] With the release of ISO 15118-20, this gap is finally addressed. TLS 1.3 encryption is now mandatory,[16] making interception-based attacks far less feasible.

Even with stronger encryption, a few edge-case attacks remain theoretically possible, though they are highly impractical. One example is the EVExchange relay attack,[17] where a malicious actor replays encrypted data between an EV and a charging station. Because the attacker does not need

to decrypt or alter the data, TLS alone cannot prevent the attack. However, successfully executing the EVExchange is extremely challenging. It requires two EVs connected to different chargers on the same backend, physically tampering with both chargers, and installing custom relay devices to capture and forward the encrypted signal in real-time. Timing is also critical: the attacker must act when the victim steps away from their EV, either to continue charging at the victim's expense or to trigger a V2G discharge and receive payment for injecting the victim's energy into the grid. While technically clever, the attack is fragile, highly invasive, and difficult to scale, making it highly unlikely in practice.

Threat	Pre-ISO 15118	ISO 15118-2	ISO 15118-20
Unauthorized charging	High	Low	Low
Session hijacking	High	Medium	Low

Table 1. ***How ISO 15118 mitigates risks by securing communication between EVs and stations.*** *ISO 15118 reduces the likelihood of unauthorized charging and session hijacking, especially in its latest version, 15118-20, which requires encrypted communication. Relay attacks remain technically possible but are considered low risk due to their complexity.*

With digital certificates, mandatory TLS encryption, and stronger authentication mechanisms, ISO 15118 has significantly improved the security of the EV charger interface. However, making one part of the system stronger does not eliminate risk. As responsibilities shift from charging stations to other components of the ecosystem, new attack surfaces emerge. The next section focuses on the e-Mobility Service Provider (eMSP), the entity handling user data, billing, and backend communication. Under ISO 15118, the eMSP is a critical link in the EV charging ecosystem and a potential point of vulnerability.

Shifted risks: Moving data security to a centralized backend

ISO 15118 not only secures the connection between EVs and charging stations. It also fundamentally changes how and where sensitive data is handled**.** By design, the standard shifts the responsibility for managing user information, payment details, and transaction records away from individual charging stations, where cybersecurity measures are often inconsistent, and toward centralized backend systems, known as eMSPs. This shift enables more consistent data protection, but it also concentrates risk, making eMSPs highly attractive targets for cybercriminals.

Every time an EV plugs in, two separate digital conversations take place. The first is between the vehicle and the charger, managed by ISO 15118. The second is between the charger and the eMSP, typically over the Open Charge Point Protocol (OCPP). This backend communication handles

authorization, energy usage tracking, and billing data, with the charging station acting as a translator between the vehicle and the backend systems.

To enable seamless coordination between EVs and eMSPs, OCPP has evolved alongside ISO 15118. Its latest version, OCPP 2.1,[18] introduces features that enable V2G transactions, dynamic pricing, and renewable energy integration. These advancements create a smarter, more flexible energy ecosystem, where vehicles can help stabilize the grid rather than strain it. OCPP also introduces enhanced cybersecurity measures, including signed firmware updates, digital certificates, and TLS encryption, which help secure data exchanges between chargers and backend systems. While ISO 15118 ensures the EV-to-charger link, OCPP secures the charger-to-backend channel. In this sense, OCPP is a critical complement to ISO 15118.

The result is a notable improvement in how data is secured across the EV charging ecosystem. Before ISO 15118, individual charging stations and their local management systems often handled sensitive data, including user records, payment details, and session metadata.[19] Although this information was often stored remotely, it remained accessible through the charging station and could be cached locally. This created a fragmented security landscape: while some chargers implemented strong safeguards, others were left vulnerable to misconfigurations or local exploits. For example, in 2019, researchers discovered that Tritium's Veefil-RT chargers leaked billing and personal data through their management interface due to weaknesses in local software configuration.[20]

Threat	Pre-ISO 15118	ISO 15118-2	ISO 15118-20
Data theft	High (at the charging station)	Medium (at the eMSP)	Medium (at the eMSP)

Table 2. ***How ISO 15118 shifts the risk of data theft from charging stations to eMSPs****. ISO 15118 moves user data management away from individual stations, where fragmented and inconsistent protections often leave data exposed, to centralized backend operators. This shift reduces the risk of station-level breaches, but it also concentrates risk at the eMSP level, where a single compromise could expose data on a large scale.*

Instead of relying on independently secured charging stations, ISO 15118 places data handling in the hands of eMSPs, which can enforce consistent cybersecurity policies at scale. But this centralization comes with its own trade-offs. A breach at the eMSP level could compromise a larger pool of data, potentially affecting thousands or even millions of EV owners in a single incident.

Despite these new risks, the overall direction remains positive. What was once a highly fragmented, loosely secured ecosystem is becoming a more cohesive and robust architecture.

Residual risks: Charging stations remain the weakest link

While ISO 15118 introduces robust protections, the standard provides no guidance on securing the physical hardware of charging stations,[21] which remain among the most vulnerable components in the EV charging ecosystem. This oversight risks undermining the very protections it aims to enforce.

Because EV charging stations are publicly accessible and often unattended, they are particularly susceptible to physical tampering. Security audits have revealed that some models still rely on low-cost, off-the-shelf components such as Raspberry Pi boards and expose maintenance interfaces or insecure remote access paths,[19] making them relatively easy targets for attackers. Once an attacker gains physical access, they can load a modified operating system or kernel and escalate privileges to gain full root access, often via vulnerable runtime applications.[22] With full control, attackers can run arbitrary code, disable critical functions, or alter system behaviour entirely, potentially causing denial-of-service (DoS) attacks or more covert manipulation. In short, even with ISO 15118 in place, many EV charging stations remain vulnerable to persistent compromise.

The risks extend far beyond service disruption. Because EV chargers are cyber-physical systems, their compromise can lead to serious real-world safety consequences. An attacker impersonating a charging station could send harmful voltage or current levels that exceed the EV's operational limits.[22] In fact, while ISO 15118 requires EVs and chargers to negotiate acceptable power levels, it lacks mechanisms to enforce compliance. A compromised charger could ignore, delay, or manipulate control signals, resulting in premature component wear, hardware damage, and even safety hazards.[23]

More alarmingly, vulnerabilities at the charging station level can reintroduce risks that ISO 15118 was specifically designed to mitigate. A notable example involves time synchronization. The standard does not require charging stations to synchronize their clocks with a trusted time source. This opens a loophole: if malicious actors manipulate the system clock, they could trick the charger into accepting expired or revoked certificates,[15] bypassing authentication and enabling unauthorized charging sessions. In doing so, attackers effectively undermine the trust model on which ISO 15118 is built.

These risks persist because ISO 15118 assumes that charging stations are trusted entities but provides no requirements to ensure that this trust is warranted. While the standard defines secure communication protocols and authentication mechanisms, it says nothing about hardening the underlying hardware or validating the software integrity.[22] This omission creates a blind spot: even if communication is encrypted and the credentials are valid, a compromised station can still behave maliciously, and there is no standardized way to detect it.

Threat	Pre-ISO 15118	ISO 15118-2	ISO 15118-20
DoS attacks	High	High	High
Unsafe power delivery	High	High	High
Unauthorized charging	High	High	High

Table 3. ***How EV charging station compromise remains a high risk despite ISO 15118.*** *ISO 15118 neither addresses vulnerabilities in the hardware of charging stations nor provides mechanisms to validate the integrity of their software. As a result, the risk of persistent compromise remains high across all versions of the standard – enabling DoS attacks, unauthorized charging sessions, and unsafe power delivery that can damage components or create safety hazards.*

Emerging risks: How innovation opens the door to new threats

As ISO 15118 expands the functionality of EV charging, it also introduces new risks, not from flawed design but as unintended consequences of its innovations. Features such as smart charging, dynamic pricing, and V2G communication offer significant benefits to EV owners and grid operators. Yet, without proper safeguards, these capabilities can also create new attack surfaces.

Smart charging, for example, adapts charging patterns based on real-time grid conditions, helping smooth electricity demand and reduce grid strain. But this flexibility can be exploited. A compromised charging station could manipulate grid signals to simulate congestion,[24] artificially inflating prices beyond user-defined thresholds, forcing charging sessions to pause or delay unexpectedly. This disruption can leave vehicles undercharged and drivers frustrated, especially since about one-third of EV models fail to resume charging automatically after an interruption.[25]

Notably, this threat is amplified in ISO 15118-20, which introduces Dynamic mode. Unlike Scheduled mode, where charging parameters are fixed before the session begins, Dynamic mode allows chargers to actively control the session:[26] adjusting power levels, pausing charging, or requesting discharge in response to grid conditions.

ISO 15118 isn't the only element of the ecosystem that brings new risks. OCPP 2.1 adds support for local price calculation,[18] a feature designed to ensure uninterrupted charging even when stations lose internet connectivity. While this enhances resilience, it also removes backend oversight. A compromised station operation - when offline - could falsify meter readings or manipulate pricing data, either overcharging other users or lowering costs for the attacker. In effect, this well-intentioned feature can unintentionally open the door to new forms of billing fraud.

V2G communication, which allows EVs to return electricity to the grid, introduces even more complex threats. Through a compromised charging station, an attacker could simulate false grid demand signals, triggering charging and discharging cycles.[27] These cycles accelerate battery degradation while remaining invisible to EV owners, who lack visibility into long-term energy flows.

Given that the battery often accounts for 30% to 40% of a vehicle's total cost,[28] this form of exploitation could cause significant financial damage to victims.

The emerging risks extend beyond individual EV owners; they also pose a threat to the grid. If multiple compromised charging stations are connected to the same power transformer, attackers could coordinate them to draw power simultaneously and inject energy back into the grid.[24] This could overload transformers, trigger localized brownouts,[29] or even push the grid's frequency beyond its safe operating limits, potentially inducing widespread blackouts similar to Spain's April 2025 incident. The fact that these attacks require greater technical sophistication does not rule them out. It instead restricts the pool of attackers to well-resourced adversaries who have both the motive and the means to act.

Threat	Pre-ISO 15118	ISO 15118-2	ISO 15118-20
Charging session Manipulation	Medium	Medium	High
Billing fraud	High	Low	Medium
Vehicle battery degradation	-	-	High
Grid attack	-	-	Medium

Table 4. ***How ISO 15118 introduces risks as unintended consequences of its innovations.*** *Before ISO 15118-20, the primary way to interrupt charging sessions was by disabling functions on compromised stations. With the introduction of Dynamic mode, the attack surface expands, as stations can now pause or delay sessions in response to grid conditions, increasing the likelihood of session manipulation. Billing fraud was mitigated under ISO 15118-2 by shifting control to eMSPs. However, OCPP 2.1 reintroduces this risk by enabling local price calculation when stations operate offline. Risks such as vehicle battery degradation and grid attacks become possible only with ISO 15118-20, as they require V2G communication. While technically complex, these attacks remain significant due to insufficient safeguards at charging stations and the potential severe damage they can cause.*

Conclusion

ISO 15118 represents an important step forward for the EV charging ecosystem, enabling smarter, more efficient, and more secure charging processes. On the surface, its improvements are significant: securing communication between vehicles and charging stations, and shifting sensitive operations, such as payment handling, to centralized backend systems. These changes mitigate several of the early, critical vulnerabilities in EV charging.

However, ISO 15118 is not a comprehensive fix, and treating it as one risks creating a false sense of security. For one, the standard offers no security guidance on securing charging stations, which remain one of the most vulnerable elements in the EV ecosystem. A compromised station can still be exploited to launch DoS attacks, deliver unsafe power levels, or initiate unauthorized charging sessions – the very threats ISO 15118 was designed to prevent.

To make matters more complex, ISO 15118 introduces entirely new attack surfaces. Features such as smart charging, dynamic pricing, and V2G communication expand capabilities but also enable new forms of exploitation, from billing fraud and charging session manipulation to grid-level disruptions. Counterintuitively, some of these risks were better contained in the first version of the standard. Moreover, since the latest revision, ISO 15118-20, does not replace the previous version of the standard, multiple versions may coexist in the field. This makes it difficult to know which protections are active, leaving EV users without a clear understanding of which risks they face.

All of these points point to a deeper issue: the EV charging ecosystem is built on a web of interdependent standards and protocols governing vehicles, charging stations, grid operations, and the backend data flows.[30] This complexity creates security blind spots. Even if one element, such as charging stations, falls outside the scope of these standards, the security of the entire ecosystem is at risk, no matter how secure the individual parts may seem. In short, while the ISO 15118 standard is a valuable tool, it cannot secure the EV charging ecosystem on its own.

Takeaway for cybersecurity

A standard can improve security, but it can also leave threats unaddressed, shift risks to other areas, and introduce new vulnerabilities. Instead of simply asking, “What does the standard protect?” industry stakeholders should ask, “What does the standard change, and what does it leave behind?” This shift in perspective is especially important for parts of the ecosystem that the standard doesn’t explicitly address. These overlooked areas are often where new threats can quietly emerge. Adopting this mindset helps avoid a false sense of security.

Ultimately, securing the EV charging ecosystem requires more than just well-designed standards. It demands coordinated action across the entire value chain, from car OEMs and grid operators to charging station manufacturers and eMSPs. Security is dynamic, and no single policy, protocol, or standard can fully capture the evolving nature of risk.

Recommendations

While the ISO 15118 standard introduces essential protections for EV charging, it does not eliminate all threats. A shared and coordinated effort is crucial to addressing cybersecurity challenges that extend beyond its scope. Every stakeholder in the EV charging value chain must recognize their role in securing the charging infrastructure.

The following strategies are recommended for each key player in the ecosystem:

- For charging station manufacturers: **Strengthen physical and software security.** Manufacturers should integrate tamper-resistant hardware, secure firmware updates, and deploy intrusion detection systems. These measures reduce the risk of attackers compromising charging stations or using them as entry points into the broader infrastructure.

- For eMSPs: **Protect centralized data.** eMSPs should implement strong encryption, continuous monitoring, and strict access control for centralized data repositories. This helps ensure that sensitive data, including payment information, is securely managed and protected from unauthorized access or breaches.

- For grid operators: **Secure smart charging and V2G protocols.** Grid operators should build safeguards to detect and mitigate data manipulation or unauthorized interactions within the electrical system. These measures help ensure that data integrity is maintained and that grid stability is not compromised.

- For car OEMs: **Strengthen in-vehicle security**. Automakers should implement intrusion detection systems and other in-vehicle security to protect vehicle data and prevent unauthorized manipulation. These controls safeguard both EV owners and the broader ecosystem.

By working together, all stakeholders can build a more secure, resilient, and future-proof EV charging ecosystem. This layered, collaborative defense strategy will not only strengthen the security of the EV charging infrastructure but also foster trust and reliability, accelerating EV adoption safely and sustainably.

References

[1] International Energy Agency, https://www.iea.org/reports/global-ev-outlook-2024/outlook-for-electric-mobility

[2] Bloomberg NEF, https://about.bnef.com/electric-vehicle-outlook/

[3] NL Times, https://nltimes.nl/2024/02/27/grid-manager-wants-turn-electric-car-charges-1600-2100

[4] The New York Times, https://www.nytimes.com/2022/09/01/us/california-heat-wave-flex-alert-ac-ev-charging.html

[5] International Energy Agency, https://www.iea.org/data-and-statistics/charts/electric-vehicle-stock-by-mode-in-the-announced-pledges-scenario-2023-2035

[6] The New York Times, https://www.nytimes.com/2025/04/29/business/spain-renewable-energy-power-grid.html

[7] Red Electrica, https://www.ree.es/en/press-office/press-release/news/press-release/2025/01/renewable-energies-generated-56-per-cent-spains-electricity-mix-2024

[8] Bayern Innovativ, https://www.bayern-innovativ.de/en/emagazine/mobility/detail/battery-storage-park-instead-of-hard-coal/

[9] Nuclear Energy Agency, https://www.oecd-nea.org/jcms/pl_62445/technical-and-economic-aspects-of-load-following-with-nuclear-power-plants

[10] Axle, https://www.axle.energy/blog/spain-blackout

[11] Ofgem, https://www.ofgem.gov.uk/blog/investing-smarter-more-flexible-grid

[12] RAC Foundation, https://www.racfoundation.org/wp-content/uploads/standing-still-Nagler-June-2021.pdf

[13] International Organization for Standardization, https://www.iso.org/standard/77845.html

[14] Encripto AS, https://www.encripto.no/2017/10/security-concerns-ev-charging-ladebrikke/

[15] Bao, K., Valev, H., Wagner, M. and Schmeck, H. (2017). A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Computer Science - Research and Development*, 33(1-2), pp.3–12, link: https://doi.org/10.1007/s00450-017-0342-y

[16] Trialog, https://www.trialog.com/en/iso-15118-20-not-only-a-further-step-towards-bidirectional-charging/

[17] Conti, M., Donadel, D., Poovendran, R., Turrin, F. (2022). 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. ESORICS 2022. Lecture Notes in Computer Science, vol 13554. Springer, Cham. https://doi.org/10.1007/978-3-031-17140-6_24

[18] Ampeco, https://www.ampeco.com/blog/what-every-cpo-needs-to-know-about-ocpp-2-1/

[19] Johnson, J.; Berg, T.; Anderson, B.; Wright, B. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. Energies 2022, 15, 3931. https://doi.org/10.3390/en15113931

[20] Tanyıldız, H., Şahin, C. B., Dinler, Ö. B., Migdady, H., Saleem, K., Smerat, A., Gandomi, A. H., & Abualigah, L. (2025). Detection of cyber attacks in electric vehicle charging systems using a remaining useful life generative adversarial network. Scientific reports, 15(1), 10092. https://doi.org/10.1038/s41598-025-92895-9

[21] Security Boulevard, https://securityboulevard.com/2024/07/balancing-security-and-convenience-with-ev-charging/

[22] Porter R.; Biglari-Abhari M.; Tan B.; Thrimawithana D. Enhancing Security in the ISO 15118-20 EV Charging System, Green Energy and Intelligent Transportation, 2025, 100262, https://doi.org/10.1016/j.geits.2025.100262

[23] VicOne, https://vicone.com/blog/electric-vehicle-charger-security-risks-how-vulnerabilities-could-lead-to-fire-hazards
[24] Alcaraz, C., Cumplido, J. & Triviño, A. OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. Int. J. Inf. Secur. 22, 1395–1421 (2023). https://doi.org/10.1007/s10207-023-00698-8
[25] Brinkel, N., van Wijk, T., Buijze, A. et al. Enhancing smart charging in electric vehicles by addressing paused and delayed charging problems. Nat Commun 15, 5089 (2024). https://doi.org/10.1038/s41467-024-48477-w
[26] Vector, https://cdn.vector.com/cms/content/know-how/_technical-articles/Emobility_ISO15118-20_Charging_emobliltytec_202210_PressArticle_EN.pdf
[27] Sarieddine K., Sayed M. A., Torabi S., Atallah R., Assi C., Edge-based detection and localization of adversarial oscillatory load attacks orchestrated by compromised EV charging stations, International Journal of Electrical Power & Energy Systems, Volume 156, 2024,109735, https://doi.org/10.1016/j.ijepes.2023.109735
[28] Institute for Energy Research, https://www.instituteforenergyresearch.org/renewable/electric-vehicle-battery-costs-soar/
[29] R. Porter, M. Biglari-Abhari, B. Tan and D. Thrimawithana, "Extending ISO 15118-20 EV Charging: Preventing Downgrade Attacks and Enabling New Security Capabilities," 2024 21st Annual International Conference on Privacy, Security and Trust (PST), Sydney, Australia, 2024, pp. 1-9, doi: 10.1109/PST62714.2024.10788058
[30] VicOne, https://vicone.com/blog/unleashing-the-charge-safeguarding-the-electromobility-era-from-cybersecurity-storms