*38th International Electric Vehicle Symposium and Exhibition (EVS38) Göteborg, Sweden, June 15-18, 2025*

# Smart Charging and Cybersecurity: Addressing Vulnerabilities in the EV Ecosystem

Lisa Calearo[1], Malthe Thingvad[1], Torben Fog[1], Marco Balossini[2], Stefano Longari[2], Hugo Morais[3], Lucas Pereira[4], Samuel Matias[5], Joao F. Mateus[5]

[1]*Spirii, Copenhagen, DK, lisa.calearo@spirii.com*

[2]*Politecnico di Milano, IT*

[3]*INESC-ID, Técnico Lisboa, PT*

[4]*ITI, LARSys, Técnico Lisboa, PT*

[5]*CNET – Centre for New Energy Technologies, PT*

**Executive Summary**

As electric vehicle (EV) adoption grows, cybersecurity challenges across the e-mobility ecosystem become critical. The EU co-funded AHEAD project addresses these challenges by mapping the Information and Communication Technology (ICT) infrastructure and developing an attacker model. This paper presents the first step of mapping the ICT infrastructure within the e-mobility ecosystem, categorizing its components into stakeholders, physical infrastructure, and IT infrastructure. Furthermore, we introduce the AHEAD methodology to assess the practices and procedures of partners in the e-mobility sector and share initial results that highlight the growing interconnectedness of stakeholders as smart charging and vehicle-to-everything (V2X) technologies become standard. The findings indicate a common concern among stakeholders regarding the potential risks of AI-based attacks and the importance of prioritizing human factors in security measures. Additionally, there is a recognized need for future investments in AI-driven monitoring and cloud security to safeguard the evolving e-mobility landscape.

*Keywords: Electric Vehicles, Cybersecurity, V2G, Smart grid integration and grid management, Supply and value chain.*

## 1 Overview

The rapid growth of electric vehicle (EV) adoption necessitates a comprehensive understanding of the Information and Communication Technology (ICT) infrastructure spanning the entire e-mobility ecosystem. Cybersecurity challenges in the EV market have been the focus of increasing academic and industry interests, with several studies highlighting the growing complexity of securing the e-mobility ecosystem. In [1] the vulnerabilities in EV charging infrastructure are discussed, and the authors identified key risks, such as the lack of standardized cybersecurity protocols across stakeholders and potential attacks on demand-side energy management. Ref. [1] presents the EV charging system network, highlighting infrastructure and protocol-centric vulnerabilities with possible cyber-attack scenarios. However, the article also highlights the increasing complexity of smart charging systems and the need for further investigation. In [2] the focus is on cloud systems, which play a crucial role in the EV ecosystem by hosting services and data. The article demonstrates the vulnerability to cyberattacks of such systems. In [3] a detailed security assessment of the EV charging infrastructure is presented, identifying and categorizing cyber threats that target different players in the EV charging ecosystem. The paper discusses vulnerabilities specific to home and public charging

infrastructures and suggests various security solutions proposed in the literature, such as enhancing communication protocols like Open Charge Point Protocol (OCPP) with security features. However, the article still identifies potential vulnerabilities in the context of the evolving Vehicle-to-Everything (V2X) communications and the integration of emerging technologies. Similarly, Ref. [5] reviews the importance of open communication protocols in ensuring integration of EVs with electricity grids, advocating for adoption of open protocols, such as ISO 15118 and OCPP, to support interoperability and dynamic smart charging strategies. However, the article also identifies gaps, including the need for more collaboration to harmonize existing protocols and the development of bidirectional charging capabilities. Ref. [4] highlights similar key areas of concern such as the vulnerabilities in the communication systems between EVs, electric vehicle supply equipment (EVSE), and the power grid, including the lack of comprehensive cybersecurity frameworks and best practices across the EV ecosystem. The article also advocates for the development of threat models, mitigation strategies, and collaborative efforts among stakeholders. Similarly, Ref. [7] highlights vulnerabilities in network communications, cloud reliance, third-party suppliers, and EV charging infrastructure, while calling for the need of stronger collaboration among automakers, utilities, and governments to safeguard the expanding EV ecosystem.

As part of the EU co-funded project AHEAD (AI-informed Holistic EVs Integration Approaches for Distribution Grids), various stakeholders from the EV ecosystem are collaborating on the development of an ICT mapping of the e-mobility infrastructure. This initial phase of the mapping is included in Deliverable [6], and this paper contributes to that effort. For complete details, please refer to the full deliverable. The following three key tasks are being tackled during the AHEAD project:

- Mapping the current ICT infrastructure supporting the EV value chain, encompassing communication protocols, hardware, software, and systems integration.
- Developing an attacker model by analyzing known attacks within the EV charging sector, assessing the dynamics between all stakeholders that are identified in the first task. This model will then be utilized to test potential threats in demonstrations project work packages.
- Defining cybersecurity requirements for a secure EV charging ecosystem by consolidating insights from demos and earlier tasks. This task will also deliver guidelines for attack prevention, detection, reaction, and recovery, and suggest improvements based on current practices.

This article focuses on the mapping of the ICT infrastructure. This analysis is essential for developing a comprehensive threat model for the e-mobility ecosystem. By examining the structure of the ecosystem, future efforts can more accurately identify attacker profiles, attack paths, and their potential exploitation methods.

With the involvement of stakeholders from various sectors of the EV ecosystem, this work touches upon current cybersecurity practices, offering a holistic view of their effectiveness across stakeholders. This is especially crucial when looking at the additional layers of smart charging and V2X, where stronger partnerships will be required to close security gaps and ensure robust protection across the e-mobility ecosystem.

The paper is structured as follows. Section 2 presents the IT security in the e-mobility ecosystem. Section 3 presents the methodology used in Deliverable [6] to identify all relevant actors in the ecosystem and how this is interconnected with the AHEAD project. Section 4 and Section 5 follow with the ecosystem actors identification and mapping. Finally, Section 6 presents major practices known and performed from the AHEAD partners, and Section 7 concludes the paper with the major conclusions.

# 2 IT in a smart e-mobility ecosystem

## 2.1 IT security in e-mobility

IT security involves protecting digital information from unauthorized access, use, sharing, alteration, or destruction. Effective IT security utilizes tools and practices such as encryption, firewalls, multi-factor authentication, and regular audits to safeguard personal and corporate data in a digital environment.

As EVs advance, their reliance on digital technologies creates new cybersecurity challenges beyond traditional IT security. EV cybersecurity must protect a complex ecosystem of interconnected physical and digital components. The rapid growth of EV technologies and manufacturers has led to a lack of standardization, increasing vulnerabilities. Cyber threats can result in unauthorized vehicle access, data

breaches, and disruptions to power infrastructure. Security must be prioritized across all levels, including software, communication protocols, and user privacy.

The e-mobility platform can be seen as a multi-layer Cyber-Physical-Social system, which architecture is needed to safeguard the security of the overall system [10]. The physical space includes the power system layer with electrical grid components and the transportation layer with EVs, batteries, and charging infrastructure. The cyber space is generally responsible for data sensing, resource management, and computing services, and specifically in the e-mobility platform it includes a big part of data collection and transmission. Third, the social space oversees the human relations including policy, legislative, and governance layer, business layer and market and pricing layers. This work investigates the Cyber-Physical layers, whereas from the social perspective, the interest of this work is limited to identifying the stakeholders involved in the ecosystem, with only highlighting how they relate and exchange information. Correlated business, market, and pricing layers are out of the scope of this work.

Therefore, unlike conventional IT systems, where threats primarily target data and software, EV security must account for vulnerabilities at multiple levels, ranging from digital communication protocols to physical hardware and user-related risks. The interconnected nature of the e-mobility ecosystems creates numerous entry points for potential attacks, making it crucial to identify and address the most critical weaknesses. Some of the potential attack surfaces are here highlighted [11][12]:

- Physical entry points to EV charging stations that can not only disrupt service but also pose safety hazards to users and the power grid.

- User-related security risks, or social attack vectors, e.g., from weak authentication practices or unintentional user errors. A lack of strong encryption and access control can turn users into targets for data theft, identity fraud, and privacy violations.

- Communication channels and protocols facilitate interactions between vehicles, charging infrastructure, and grid operators; however, many of the protocols lack adequate security measures. Additionally, V2X communication introduces unique risks, as attackers can potentially exploit weak encryption to disrupt network operations, manipulate charging transactions, or even interfere with grid stability.

- E-mobility mobile apps can suffer from security vulnerabilities such as inadequate encryption, backdoors, or excessive data permissions. Cloud-based platforms that manage EV charging operations and billing systems are attractive targets for cybercriminals, as gaining access to these servers could enable large-scale data breaches, fraudulent transactions, or even remote control over charging infrastructure.

### 2.2 Smart charging and flexibility

The EV ecosystem today is closely tied to the concepts of flexibility and smart charging [9]. Charging flexibility refers to the ability to delay the start time or adjust the power of an EV charging session in response to external signals. Smart charging leverages this flexibility for various purposes, such as grid management and load balancing [8]. Smart charging interconnects various components, such as EVs, charging stations, and power grids, which introduces several cybersecurity challenges. Even a relatively "simple" smart charging feature, like a user setting their vehicle to charge during low electricity price periods, adds multiple layers of data exchanges. In this scenario, the user must provide plug-in and plug-out times and specify their charging preference. The backend system then accesses external data sources to retrieve electricity price information and determine when to start and stop charging. These added layers of data exchange increase the system's complexity and the attack surface, making it more appealing to cybersecurity attackers looking to exploit vulnerabilities.

## 3 Methodology

To identify all possible potential attack points of the e-mobility ecosystem, a detailed mapping of electricity

and data flows across key stakeholders is necessary. A detailed mapping of the system, from the EV to the grid, will serve as a basis for broadening the previously mentioned list of potential attacks in Section 2.1 and recognizing all potential vulnerabilities within the system, including smart charging and V2X interactions.

The first step has been to identify the major areas for the mapping of the e-mobility ecosystem:

1. Stakeholders: The charging business ecosystem consists of various entities that interact to support the production, charging operation, and management of EVs.
2. Physical infrastructure: The physical infrastructure of the e-mobility platform includes the components necessary for EV charging, as well as for implementation of smart charging and V2X.
3. IT infrastructure: The digital backbone that supports the functionality, scalability, and efficiency of the ecosystem, combining all components that are needed for the operation and management of the EV charging, including users, charging networks, energy systems, etc.

The second step has been to identify how the AHEAD project partners are interconnected with the three major areas, and how they interact and share data. This has then been evaluated by comparing with collected practices on cybersecurity from the partners in AHEAD.

In the following sections, the three major areas for the mapping are presented with the various subcategories, as well as the initial results and practices collected.

# 4 Ecosystem categorization

## 4.1 Stakeholders

The EV charging business ecosystem comprises various entities that collaborate to support the production, operation, management, and adoption of the e-mobility ecosystem. Key players include:

1. EV Users: The end consumers of EVs, including individual and business users.
2. Charging infrastructure Providers: Responsible for building and managing charging networks, including Charging Station Owners (CSOs), Charge Point Operators (CPOs), Charge Point Management System Providers (CPMS), and E-mobility Providers (EMPs).
3. EV related: This category includes Original Equipment Manufacturers (OEMs) and battery manufacturers.
4. Technology providers: Offer software and hardware solutions, including telematics, IoT solutions, and payment services, to enhance the e-mobility ecosystem as well as fleet operators, which manage large-scale EV fleets for transportation and logistics.
5. Electrical grid related: Energy providers and grid operators manage energy supply and integration with the electricity grid, as well as energy utilities, renewable energy providers, balance responsible parties (BRPs), aggregators.
6. Policy and regulatory bodies: Establish the legal framework for EV adoption, including government agencies and standards organizations.
7. Influencing stakeholders: Financial entities, research institutions, and industry alliances play supportive roles.

Collaboration among all stakeholders is crucial for addressing challenges like infrastructure scalability and user adoption, ultimately facilitating the transition to electrified transport.

## 4.2 Physical infrastructure

The physical infrastructure of the e-mobility platform encompasses the essential components for EV charging, which include:

1. Electric Vehicles (EVs): Battery-powered vehicles such as cars, bikes, scooters, heavy-duty vehicles (buses and trucks), and vessels that require recharging through dedicated infrastructure.
2. Electric Vehicle Supply Equipment (EVSE): This includes all components necessary for charging EVs.
3. Electrical Grid Connection: Infrastructure such as transformers, power lines, and substations that supply electricity to charging stations.
4. Local Infrastructure including buildings that house or support charging facilities, sharing grid connections with EVSE; Battery Energy Storage Systems (BESS) that store excess energy and can buffer charging power when grid capacity is limited; Renewable Energy Sources (RES): Wind turbines or solar systems that provide sustainable power to EVSE, often in conjunction with BESS.
5. While less visible, data centers, servers, and networking equipment are crucial for the operation of the e-mobility platform, providing the necessary IT infrastructure for connectivity and data management.

To perform smart charging, it is necessary that EVSEs are equipped with intelligent features for optimizing charging based on various factors. Those require additional hardware (like smart meters) and software components to communicate with the grid or external stakeholders and manage charging sessions. Additionally, bidirectionality (V2X) upgrades standard EVSE to support power flow in both directions, necessitating bidirectional inverters for both AC and DC charging.

## 4.3 IT infrastructure

The IT infrastructure of the e-mobility platform is the digital backbone that supports the functionality, scalability, and efficiency of the ecosystem, combining all components that are needed for the operation and management of the EV charging, including users, charging networks, energy systems, etc.. The IT infrastructure comprises:

1. Backend System: Manages data processing, storage, and business logic, connecting hardware to users. Key features include data management, integration with external services, authentication, and real-time data exchange for smart charging and V2X.
2. Networking and Connectivity: Facilitates communication between EVs, charging infrastructure, user interfaces, and external systems.
3. Data Management: Involves the collection, processing, and usage of various data types, including vehicle, user, charging infrastructure, grid, local component, and external API data.
4. Frontend Interfaces: Mobile applications enable users to locate, reserve, and pay for charging stations; Web Portals provide detailed information and account management for CPOs and users; customer support tools offer assistance through chatbots and ticketing systems.

## 4.4 Security, communication & compliance

Robust measures are vital for protecting data, communications, and operational integrity in e-mobility, ensuring compliance with legal and industry standards. Key security pillars include data, network, application, physical, and IoT security, which safeguard user data and build stakeholder trust.

Some major communication channels that are necessary for operation of the e-mobility ecosystem are between: EV auxiliary equipment, EV and charger, charging infrastructure and backend, backend and roaming networks, backend and grid operators. Table **1** provides some of the major communication standards and protocols with focus on the communication between the EV and the charger and the charger and the backend.

Table 1 Communications between major entities in the e-mobility platform [13][14][15].

| Entity | Communication/Protocol used | Key Data Exchanged |
|---|---|---|
| EV ↔ Charger | CCS (DC Charging): ISO 15118, DIN SPEC 70121 | Authentication (Plug & Charge), Charging power negotiation, Battery status, Charging session monitoring |
| | CHAdeMO (DC Charging): CAN bus | Vehicle authentication, battery charge request, charging status, Vehicle-to-Grid (V2G) support |
| | Type 2 (AC Charging): IEC 61851-1, ISO 15118, SAE J1772 | Basic charging start/stop, safety checks |
| Charger ↔ Backend (CPO/EMP) | Public & Private Chargers: OCPP 1.6 / 2.0.1, proprietary protocols | Remote start/stop, authentication (RFID, app, Plug & Charge), charging session details, charger status updates |

Furthermore, the introduction of smart charging, V2X, and the use of EVs for flexibility markets brings new stakeholders and physical infrastructure into play. An architectural model presented in [16] illustrates the extensive interconnections among various flexibility market participants, including BRPs, aggregators, both large and small-scale flexibility asset owners, transmission system operators, distribution system operators, energy suppliers, data hubs, and meter data companies. Another architectural model is provided in [17] with a large focus on the bidirectional (V2X) charging and new stakeholders like V2G providers.

Finally, as vehicles become more connected, the amount of personal data generated and processed increases, raising privacy risks. In the EU, two key legislations govern digital privacy:

1. GDPR: Established in 2018, it regulates data protection and privacy, requiring businesses to handle personal data, such as location and payment information, in compliance with strict standards.

2. ePrivacy Directive (ePD): Supplements GDPR by mandating consent for storing information.

Additionally, ISO/IEC 27001 provides a framework for managing information security, while SOC 2 offers a more detailed assessment of an organization's security posture. Although both are voluntary, they are often required for compliance. The NIS-2 Directive is a mandatory EU regulation focused on strengthening cybersecurity, requiring e-mobility stakeholders to implement risk management and incident reporting.

# 5 Ecosystem mapping

Figure **1** provides the mapping of the ecosystem. It highlights the key physical components – electrical grid, EVSE, and EVs – along with their physical connections. Stakeholders operate the software and share data via cloud platforms to manage the servers. This analysis does not include direct communication through email or phone, which, while important and potentially vulnerable to hacking that could result in the exposure of sensitive information, is not considered essential for the primary data and electricity flow exchanges. In the figure, CPOs and CSOs are depicted in the CPMS, as they often communicate directly (via email or telephone) with each other and with the CPMS; however, the actual control of the charger is executed through the CPMS backend. Along with the physical connection, authentication and payment (and, when necessary, roaming) are the two steps required to initiate a charging process. These also introduce data exchanges, stakeholders, and standards that are not directly presented in the paper but are considered in the AHEAD project and further detailed in Deliverable [6].

Additionally, the part on the right of the figure illustrates all the interconnections with grid operators, aggregators, BRP, Balance Service Provider (BSP), and resource providers (RES), which are crucial, especially when implementing smart charging within flexibility markets.

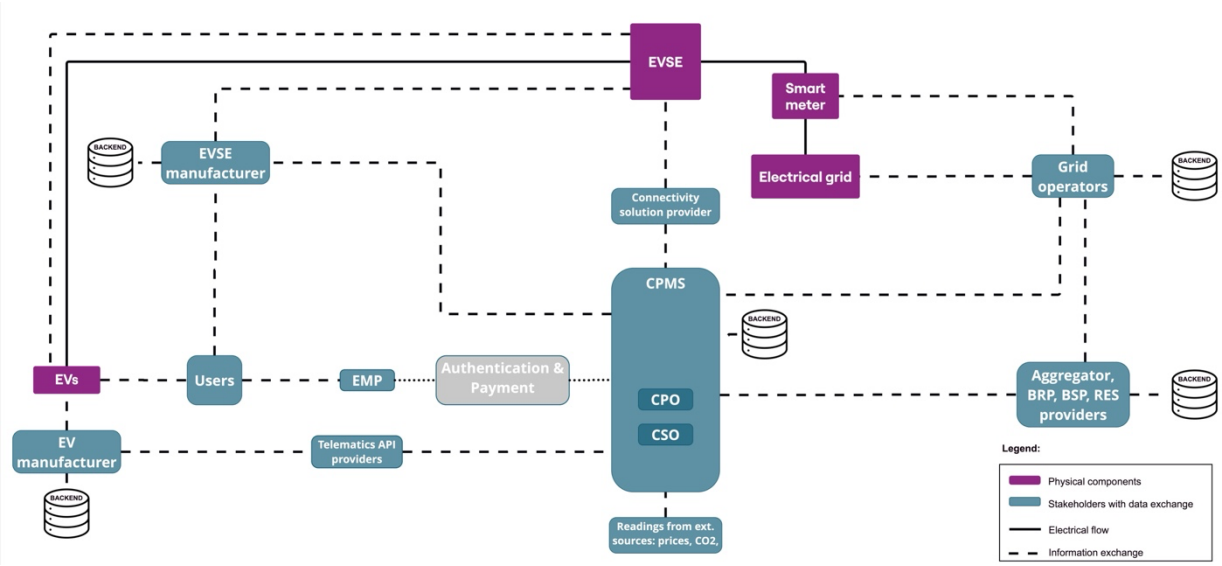

Figure 1 Mapping of the e-mobility ecosystem including stakeholders interconnections and physical infrastructure.

# 6 AHEAD practices

The AHEAD project is developed by a diverse group of partners with knowledge and experience from different categories of the e-mobility ecosystem. Figure **2** shows the stakeholders in AHEAD as part of the categories described in Section 4.1.

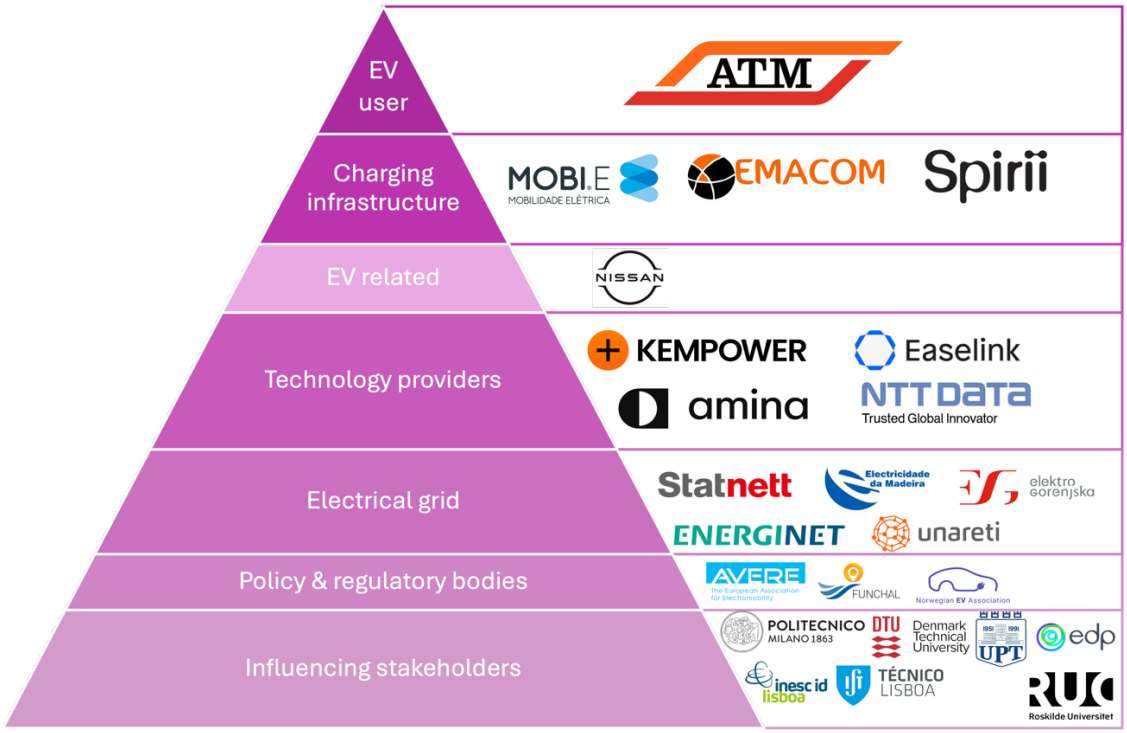

Figure 2 Stakeholders overview in the value chain.

By covering a large majority of the stakeholders identified in Section 4.1, it is reasonable to assume that the partners have knowledge on the IT infrastructure and data exchanged between different physical infrastructure to fill the map in Figure **1** with ongoing procedures, data exchanges, as well as standards and protocols. Therefore, we have conducted a two-level investigation approach to identify what are today's

practices, procedures, data exchange in the mapping. First, we have requested cybersecurity ongoing procedures from the different partners on a general term. Second, we have implemented a questionnaire to tailor specific requests. This article presents some initial results from the first step, whereas the full results overview is presented in [6]. Not all partners participated in the information collection; further details are provided in the deliverable.
Initial results show that:

1. Most stakeholders keep up to security standards like ISO 27001
2. Most stakeholders perform yearly security audits
3. Current concerns in common to all stakeholders are:
    a. The use of AI techniques to automate the attack process
    b. Threats targeting people, such as social engineering and phishing
    c. Managing threats within the company's supply chain

This is then also reflected into the future security investments, which focus mostly on Zero-Trust architecture, a security model that requires all components to verify each other before granting access, to avoid lateral movement within the system and AI-based automated monitoring systems to speed up the system incident detection, prevention and response.

These fears and needs increase with the advent of smart charging and V2X, which require more stakeholders and physical interconnections. This interconnectedness is anticipated to expand further with the integration of flexibility markets, leading to increased data exchanges and collaboration.

# 7 Conclusions

This paper has mapped the ICT infrastructure of the e-mobility ecosystem by categorizing its components into stakeholders, physical infrastructure, and IT infrastructure. The initial AHEAD results show the importance of attention to AI attack processes and automated monitoring systems to speed up the incident detection, prevention and response. These fears and needs increase with the advent of smart charging and V2X, which require new stakeholders and physical interconnections. This interconnectedness is anticipated to expand further with the integration of flexibility markets, leading to increased data exchanges and collaboration.
The initial findings from the AHEAD project will be further expanded in the project with results from the questionnaire analysis which will go into details of different areas of the e-mobility ecosystem and stakeholders. This also includes an upgrade of the figure mapping of the infrastructure with protocols and standards for all the interconnections. This work serves as a foundational step in the AHEAD project, setting the stage for future research that will focus on threat modeling and the development of requirements and guidelines to secure EV charging infrastructure. As the e-mobility landscape continues to evolve, these efforts will be essential in fostering a secure and sustainable environment for all stakeholders involved.

# Acknowledgments

The work in this paper has been supported by the research project AHEAD (CINEA EU gr. Number: 101160665).

# References

[1] S. Acharya, Y. Dvorkin, H. Pandzic, R. Karri. *Cybersecurity of Smart Electric Vehicles Charging: A Power Grid Perspective,* IEEE Access 2020, 10.1109/ACCESS.2020.3041074.

[2] S. Hamdare, O. Kaiwartya, M. Aljaidi, et. al. *Cybersecurity Risk Analysis of Electric Vehicles Charging Stations*, Sensors 2023, 23, 6716. https://doi.org/10.3390/s23156716 .

[3] P. Patil, S. A. Dogan, S. Tout, R. Parmar. *Exploring the EV charging ecosystem and performing and experimental assessment of its cloud and mobile application infrastructure security,* International Journal of Computer Science & Information Technology (IJCSIT) Vol 16, No 1, February 2024. DOI:

10.5121/ijcsit.2024.16101.

[4] J. Antoun, M. E. Kabir, B. Moussa, C. Assi. *A detailed security assessment of the EV charging ecosystem,* IEEE Network, 2019, 10.1109/MNET.001.1900348.

[5] J. Johnson, et. al. *Cybersecurity for Electric Vehicle Charging Infrastructure,* Sandia Report, July 2022.
[6] Deliverable 5.1, AHEAD, *ICT requirements in the EV value chain*, https://cordis.europa.eu/project/id/101160665 . Under revision.

[7] M. Neaimeh, P. B. Andersen. *Mind the gap- open communication protocols for vehicle grid integration,* Energy Informatics, 2020, https://doi.org/10.1186/s42162-020-0103-1 .

[8] N. Malimage, P. Terpening, T. A. Brashares, et. al. *Cybersecurity Challenges in the Electric Vehicle Market*, 2023, Agricultural Engineering International : The CIGR e-journal.

[9] M. Secchi, *Electric Vehicle Technologies – Part II,* Course presentation DTU Lyngby Campus, 07/03/2024.

[10] U. Cali, M. Kuzlu, O. Elma., et al, *Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure*. EICC 2023, Norway, https://doi.org/10.1145/3590777.3591406 .

[11] Johnson, J., Berg, T., Anderson, B., & Wright, B. (2022). Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies*, *15*(11), 3931. https://doi.org/10.3390/en15113931 .

[12] Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D., & Lloret, J. (2023). Cybersecurity Risk Analysis of Electric Vehicles Charging Stations. *Sensors*, *23*(15), 6716. https://doi.org/10.3390/s23156716 .

[13] Sevdari, K., Andersen, P. B., & Marinelli, M. (2025). *Aggregation and Control of Electric Vehicles AC Charging for Grid Services Delivery*. IEEE Transactions on Smart Grid, 16(2), 1523-1534. https://doi.org/10.1109/TSG.2024.3492391

[14] Greenflux, Roaming protocols: OCPI, OICP, OCHP and eMIP, https://www.greenflux.com/expertise/blogs/roaming-protocols-ocpi-oicp-ochp-and-emip/, visited 20th March.

[15] Spirii, Roaming Network, https://www.spirii.com/en/glossary/roaming-network , visited 20th March.

[16] Afzal, Z.; Ekstedt, M.; Müller, N.; Mukherjee, P. *Security Challenges in Energy Flexibility Markets: A Threat Modelling-Based Cyber-Security Analysis*. Electronics 2024, 13, 4522. https://doi.org/10.3390/electronics13224522

[17] Joint report by European Working Group 1 “Car charging and Aggregators” and European Working Group 2 “Energy and Grid Topics” in the “Coalition of the Willing on Bidirectional Charging”, 2024.

## Presenter Biography

Lisa is a Senior R&D Engineer at Spirii, working in the Future Tech department. She holds a Ph.D. from the Technical University of Denmark, completed in 2022, and a double master’s degree obtained in 2018 as part of the TIME project between Padova University and DTU. In her current role, she leads the innovation content of ongoing Europe-wide projects with external partners, scopes and develops R&D projects, and engages in innovation efforts across the organization to commercialize services, functions, and ideas.