irdeto metergram

The essential guide for NEVI funded EV projects

Table of Contents

1. What is NEVI?

The NEVI program represents a significant federal initiative, aiming to establish a comprehensive, accessible and reliable Electric Vehicle (EV) charging network nationwide. This is a critical component of the broader strategy to foster EV adoption, aiming to mitigate environmental impact while paving the way for a sustainable transportation future.

How it started

Embarking on an electrifying quest since 2021 under the visionary Bipartisan Infrastructure Law, the NEVI program has been the driving force behind the nationwide deployment of EV charging infrastructure.

As we cruise into 2024 and beyond, the mandatory compliance with OCPP 2.0.1 and ISO/IEC 15118 for all new EV charging station installations funded under NEVI ensures interoperability and cybersecurity standards.

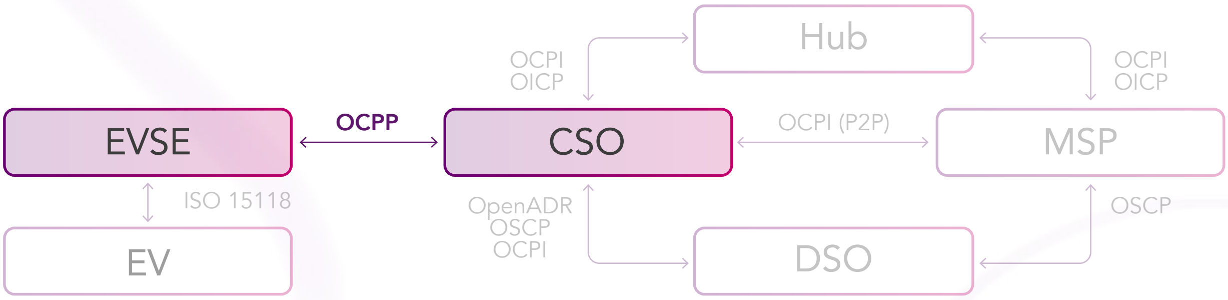
2025 will be the reflection year and an assessment period for the initial phase of NEVI-funded projects and based on that, updated guidelines will be released.

What will you learn

This white paper is your guide to help you steer NEVI funded EV charging projects to success. It is packed with the practicalities of managing projects under the NEVI program, intricacies of funding, cybersecurity and software standards critical to building a future-ready EV charging network. Join us as we:

- Uncover the impact of the key protocols and standards (OCPP, OCPI and Grid Communication) on project planning, execution and success
- Reveal the importance of robust cybersecurity and the relevance of the ISO/IEC 15118 standard
- Provide expert guidance on how to navigate the practical, technical and operational challenges of NEVI-funded projects
- Provide insights into the future of EV charging infrastructure, including emerging trends, policy developments and technological innovations.

2. Open Charge Point Protocol (OCPP)



2.1 NEVI COMPLIANCE AND FUNDING

Under the NEVI program, implementations and maintenance of solutions conforming to the OCPP standards are eligible for funding. Referred to in the documentation as "software maintenance and repair costs, including service agreements with third-party contractors" and "Other operating costs that are necessary and directly related to the charging of vehicles".

The NEVI program has specific stipulations regarding the use of OCPP and it explicitly requires using OCPP for EV charging infrastructure projects receiving federal funding. This directive ensures that funded projects adhere to standards promoting interoperability, security and future scalability.

The requirements under NEVI are stated as follows:

- ***680.108 - Interoperability of electric vehicle charging infrastructure***

(b) Charger-to-Charger-Network Communication. Chargers must conform to Open Charge Point Protocol (OCPP) 1.6J or higher. By February 28, 2024, chargers must conform to OCPP 2.0.1.

- ***680.114 Charging network connectivity of electric vehicle charging infrastructure.***

(a) Charger-to-charger-network communication.

(1) Chargers must communicate with a charging network via a secure communication method. See 680.108 for more information about OCPP requirements.

(2) Chargers must have the ability to receive and implement secure, remote software updates and conduct real-time protocol translation, encryption and decryption, authentication and authorization in their communication with charging networks.

(3) Charging networks must perform and chargers must support remote charger monitoring, diagnostics, control and smart charge management.

FHWA clarifications on OCPP

The Federal Highway Administration (FHWA) has issued clarifications crucial for aligning with OCPP 2.0.1 standards, particularly under the NEVI program. These clarifications highlight the importance of adopting OCPP 2.0.1 for securing federal funding, emphasizing robust security protocols, standardized data sharing and the ability to adapt to evolving EV needs. The FHWA's guidance is instrumental in ensuring that charging stations comply with national standards and are equipped to meet future demands.

2.2 OCPP OVERVIEW

The OCPP is a vital communication standard that links Electric Vehicle Supply Equipment (EVSE) and Charging Station Management Systems (CSMS). Originating in the Netherlands in 2009, it was developed by the Open Charge Alliance (OCA), a global consortium of public and private EV infrastructure leaders. The OCA governs the development and adoption of OCPP, ensuring it remains an open and accessible standard for all.

OCPP was created to promote interoperability across charging stations and network management system vendors. Standardizing the communication between EVSEs and CSMSs allows for a diverse range of products and services to integrate seamlessly, fostering a competitive and innovative market.

Over the years, OCPP has undergone several updates, each enhancing its capabilities to address evolving industry needs:

- **EVSE** serves as the core of EV charging infrastructure, delivering electrical power to electric vehicles for charging. EVSEs come in various charging levels, speeds and connectivity options, playing a crucial role in shaping the user experience and operational efficiency of EV charging networks.
- **The CSMS** acts as the operational command center for EVSEs, overseeing key functionalities such as charging session authorization, billing, real-time data monitoring and maintenance. The effectiveness and reliability of the CSMS are essential for ensuring the seamless operation and delivery of high-quality service in EV charging stations.
- **OCPP 2.0.1** is the latest evolution of the Open Charge Point Protocol and introduces advanced features enhancing EV charging communication. These include heightened security, streamlined transaction management and enhanced data reporting capabilities, aligning with the complex needs of modern EV charging infrastructure.

2.3 UPGRADING FROM OLDER OCPP VERSIONS TO OCPP 2.0.1

As the EV charging infrastructure evolves, so do the standards that govern it. Upgrading to OCPP 2.0.1 from older versions (such as 1.5, 1.6 or 1.6J) is a strategic move for charging network operators seeking to leverage the latest technological advancements and meet current regulatory requirements.

Key enhancements in OCPP 2.0.1

OCPP 2.0.1 introduces significant improvements over previous versions, including:

- **Advanced security features** to address modern cybersecurity challenges.
- **Improved data management** for more efficient and comprehensive reporting.
- **Improved transaction management** features for smoother user transactions.
- **Smart charging capabilities**, critical for effective grid management and optimization.

Essential considerations for upgrading

When considering an upgrade, several broad factors must be taken into account for all older versions:

- **Assess the current infrastructure** to determine compatibility and adaptation requirements for OCPP 2.0.1.
- **Understand the technical challenges and operational adjustments** necessary to adopt the new protocol version.
- **Evaluate the training needs** of staff to effectively manage and operate the upgraded system.
- Engage with vendors to **comprehend the support** available for upgrading and ensure uninterrupted service.

Strategic upgrade path

Adopting a strategic approach to the upgrade involves:

- **Prioritizing needs**: Identify critical aspects of the upgrade and prioritize them based on operational importance.
- **Phased implementation:** Opt for a phased rollout to ensure a smooth transition, starting with pilot projects or specific sites.
- **Regulatory compliance:** Ensure alignment with current regulations and standards, including those outlined in the NEVI program.
- **Seeking expertise:** Leverage external expertise and consultancy services if needed to navigate the upgrade process effectively.

2.4 IMPLEMENTING OCPP FROM SCRATCH

The adoption of the OCPP is a critical milestone for organizations entering or transitioning within the EV charging domain. OCPP facilitates the interoperability between charging stations and charging station management systems, laying the foundation for a scalable, flexible and vendor-independent EV charging infrastructure.

Benefits of OCPP

Aside from unlocking funding opportunities, adopting OCPP offers numerous advantages:

- **Vendor independence:** Avoid vendor lock-in by selecting hardware and software from any manufacturer supporting OCPP.
- **Scalability and flexibility:** Easily expand and integrate new technologies or services.
- **Conformance:** Ensure alignment with industry standards and regulatory requirements, enhancing eligibility for incentives and funding.

Initial considerations

Before we dig into implementation, several key aspects require careful consideration:

Infrastructure assessment

Evaluate the existing or planned infrastructure to determine the requirements for OCPP compatibility, including hardware capabilities and network connectivity.

Vendor selection

Choose vendors offering OCPP-compliant charging stations and CSMS platforms, considering their track record, customer support and commitment to OCPP versions.

To consider: The devil is in the details, so be mindful and ask questions about the specific implementation, concerning what parts of the protocol are actually implemented and supported.

Compliance and standards

Familiarize yourself with local regulations and standards governing EV charging operations, ensuring selected OCPP versions meet requirements.

Implementation steps

A structured approach to implementation ensures a smooth transition to using OCPP.

Planning and design

Develop a comprehensive plan outlining deployment strategy, including charging station locations, network architecture and integration with existing IT systems.

Hardware and software selection

Choose OCPP-compliant hardware (EVSE) and software (CSMS) aligned with your operational needs and budget. Consider future-proofing your selection to accommodate advancements in EV technology.

Installation and configuration

Proceed with the physical installation of charging stations, followed by the configuration of the CSMS to establish communication with the EVSE via OCPP. This step may involve network configuration and ensuring secure internet connectivity.

Testing and validation

Conduct comprehensive testing to validate the setup's functionality, interoperability and security. This includes testing all use cases, error handling and data communication processes.

Training and support

Organize training sessions for staff to familiarize them with the new system's operations and management. Establish a support framework with your vendors to address future issues or updates.

BEST PRACTICES FOR SUCCESSFUL IMPLEMENTATION

Implementing OCPP from scratch requires adhering to best practices to ensure success.

Make sure to engage with the OCPP community to access valuable knowledge, experience and advice, prioritize scalability and flexibility to accommodate future growth and changes. Additionally, prioritize security measures to safeguard your infrastructure against cyber threats.

Embracing open standards and focusing on interoperability is the best way to position your organization for success. By ensuring adaptability and compliance, you equip your infrastructure to meet the dynamic demands of the EV market.

2.5 BUILD OR BUY A CSMS?

Deciding whether to build a custom CSMS or to purchase an off-the-shelf solution is a pivotal decision for organizations deploying EV charging infrastructure. This choice has significant implications for cost, time to market and future flexibility.

BUILDING A CUSTOM CSMS

ADVANTAGES

- **Tailored solution:** Custom-built CSMSs precisely match organizational operational needs and specific requirements.
- **Control and flexibility:** Provides complete control over system features, integration capabilities and future updates.

CHALLENGES

- **Higher initial costs:** Custom solutions often require higher upfront costs due to specialized development expertise.
- **Longer development time:** Conception-to-deployment duration may delay service launch.
- **Maintenance and support:** Ongoing maintenance and updates may demand significant internal resources or continued developer engagement.

BUYING AN OFF-THE-SHELF CSMS

ADVANTAGES

- **Speed to market:** Ready-made solutions allow for quicker deployment, as they are already developed and tested.
- **Cost-effectiveness:** Often more cost-effective in the short term, with transparent pricing structures and lower upfront investment.

CHALLENGES

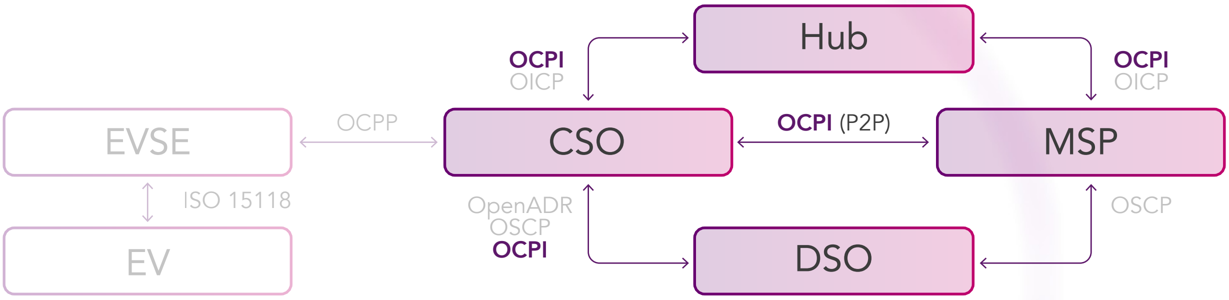
- **Limited customization:** While many solutions offer customization options, there will be limitations compared to a fully custom system.
- **Dependence on vendor:** Reliance on the vendor for updates, support and future enhancements can be a drawback, especially if the vendor's roadmap doesn't align with the organization's evolving needs.

Making the decision

There are four key factors to consider when deciding between building or buying a CSMS:

- **Budget and resources:** Assess both the initial and ongoing costs of each option, including internal resource availability for development and maintenance.
- **Operational requirements:** Assess whether the functionalities required from the CSMS can be met by an off-the-shelf solution.
- **Scalability and flexibility:** Determine how well each option supports future growth and adapts to changing technologies or business models.
- **Time to market:** Determine the urgency of deployment and the speed at which each option can be implemented.

3. Open Charge Point Interface (OCPI)



3.1 NEVI COMPLIANCE AND FUNDING

Implementation and maintenance of solutions securing conformance with OCPI are eligible for funding under NEVI. Referred to in the documentation as "software maintenance and repair costs, including service agreements with third-party contractors" and "Other operating costs that are necessary and directly related to the charging of vehicles".

The requirements under NEVI are stated as follows.

- ***680.108 Interoperability of electric vehicle charging infrastructure.***

(c) Charging-Network-to-Charging-Network Communication. By February 28, 2024, charging networks must be capable of communicating with other charging networks in accordance with OCPI 2.2.1.

- ***680.114 Charging network connectivity of electric vehicle charging infrastructure.***

(c) Charging-network-to-charging-network communication. A charging network must be capable of communicating with other charging networks to enable an EV driver to use a single method of identification to charge at Charging Stations that are a part of multiple charging networks.

These are the clearest indications that OCPI usage is mandated, but it's essential to consider even paragraphs that may not explicitly mention OCPI. For instance,

- ***680.116 Information on publicly available electric vehicle charging infrastructure locations, pricing, real time availability and accessibility through mapping.***

and

- ***680.112 Data submittal.***

This paragraph brings up a plethora of specific requirements on detailed reporting and data submittal. Having an implementation of OCPI in place can support many of these requirements.

FHWA Clarifications on OCPI

While the FHWA primarily focuses on OCPP for charging station communication, the NEVI's principles of interoperability and open standards also apply to OCPI. Ensuring that your network's OCPI implementation conforms to the latest standards is crucial for facilitating widespread access and compatibility.

3.2 OCPI OVERVIEW

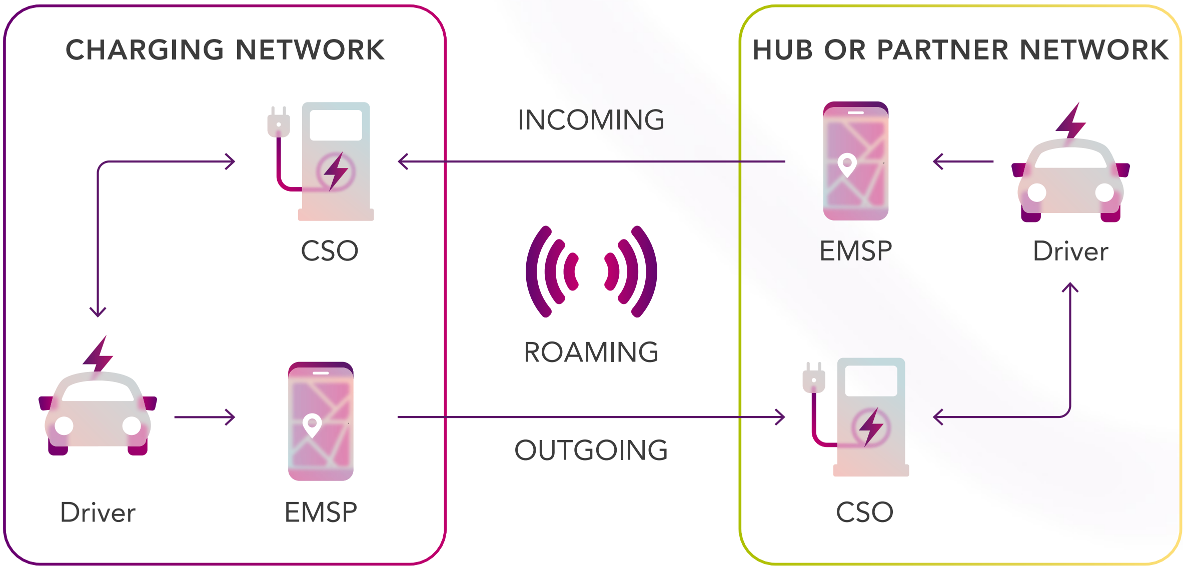
The OCPI protocol aims to standardize and simplify the exchange of information between various stakeholders in the EV charging ecosystem, including EV service providers, charging station operators and mobility service providers. OCPI facilitates direct communication and data exchange, enabling features like real-time status updates, roaming services for EV drivers and remote start/stop charging sessions.

3.2.1 VERSIONS

OCPI has evolved through several versions, with 2.2.1 being the latest at the time of writing. Each version introduces enhancements that improve interoperability, security and the range of services that can be offered.

Adopting OCPI 2.2.1 brings several advantages, including improved support for roaming agreements, enhanced transaction handling and better data transparency. Conformance with this version ensures that charging networks are capable of providing a seamless user experience and are prepared for future scalability and integration challenges.

The potential roles and directions of roaming between a CSO and eMSP



3.2.2 IMPLEMENTATIONS

Organizations have two main paths for implementing OCPI: leveraging third-party services or developing an in-house solution.

THIRD-PARTY OCPI SERVICES

Advantages: Speed to market, reduced complexity and access to established networks

Considerations: Dependency on the service provider and potential limitations in customization

DEVELOPING AN IN-HOUSE OCPI SOLUTION

Advantages: Full control over the integration, customization and data handling

Challenges: Requires significant investment in development, maintenance and establishing roaming agreements

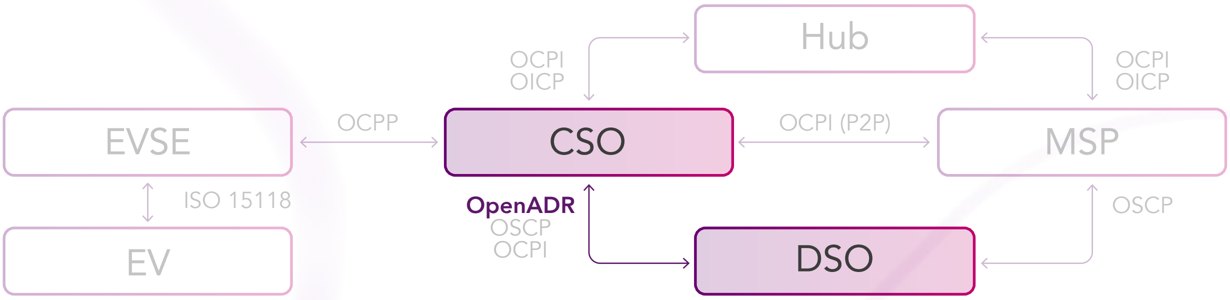
3.2.3 UPGRADING TO NEWER VERSIONS

The transition to OCPI 2.2.1 from older versions or other protocols should be carefully planned to minimize disruptions. A phased approach, beginning with a pilot project before full-scale rollout, can help identify potential issues and ensure a smooth upgrade process. Take note that you might need to run several versions of the implementation simultaneously as some of your partners will only support older versions of the protocol. In contrast, others only support the latest version.

Benefits of upgrading OCPI

- **Payments:** Simplifies the integration of diverse payment solutions, making it easier for drivers to pay for charging services across different networks.
- **Reporting:** Provides detailed data on charging sessions, facilitating accurate and comprehensive reporting for station operators and service providers.
- **Roaming:** Enhances the customer experience by enabling EV drivers to access a broader network of charging stations with seamless authentication and payment.

4. Grid communication and Open Automated Demand Response (OpenADR)



As a bonus, we also want to mention another opportunity regarding implementing standards in the EV charging world.

These aspects of communication within the industry are mentioned under NEVI as follows.

- ***680.114 Charging network connectivity of electric vehicle charging infrastructure.***

(d) Charging-network-to-grid communication. Charging networks must be capable of secure communication with electric utilities, other energy providers or local energy management systems.

4.1 GRID COMMUNICATION OVERVIEW

As the adoption of EVs accelerates, the impact on the electrical grid becomes increasingly significant. Efficient grid communication is essential for balancing demand, ensuring stability and integrating renewable energy sources. This is where standards like Open Automated Demand Response (OpenADR) come into play, offering a framework for automated, real-time communication between utility providers and EV charging infrastructure.

Benefits of integrating OpenADR

- **Enhanced grid stability:** By adjusting charging loads in response to grid demand, EV charging stations can help prevent overloading the grid, especially during peak periods.
- **Cost savings:** Operators can optimize electricity use by charging during off-peak hours when rates are lower, resulting in cost savings.
- **Support for renewable energy:** Integration with OpenADR enables greater use of renewable energy by coordinating charging times with the availability of solar or wind power, promoting sustainability.

4.2 IMPLEMENTING OPENADR IN EV CHARGING INFRASTRUCTURE

Compatibility and conformance

Ensuring that EV charging stations and management systems are compatible with OpenADR standards is the first step toward integration. This often involves working with hardware and software that are certified or conformant with OpenADR specifications.

Strategic implementation

Implementing OpenADR demands strategic planning to harmonize with business objectives, operational needs and regulatory mandates. This involves setting up communication protocols, data exchange formats and response strategies for demand response signals.

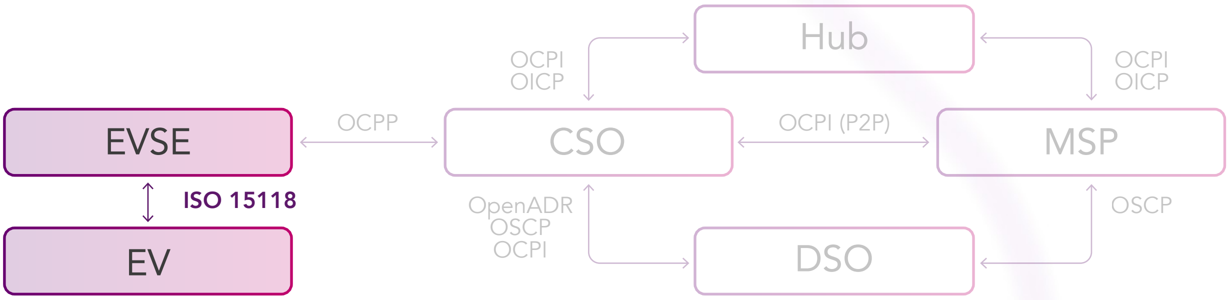
Challenges and considerations

While integrating OpenADR offers numerous benefits, it also presents challenges such as ensuring data security, managing the complexity of implementation and aligning with existing infrastructure. Careful consideration and planning are essential for a successful deployment.

4.3 THE FUTURE OF GRID COMMUNICATION

As the EV market continues to grow, the importance of streamlined grid communication and intelligent charging infrastructure will become increasingly paramount. OpenADR and similar standards will play a crucial role in enabling scalable, sustainable and efficient EV charging networks that support the broader transition to renewable energy and electrified transportation.

5. ISO 15118



5.1 NEVI COMPLIANCE AND FUNDING

Implementation and maintenance of solutions securing conformance with ISO-15118 are eligible under NEVI funding. Referred to in the documentation as "software maintenance and repair costs, including service agreements with third-party contractors" and "Other operating costs that are necessary and directly related to the charging of vehicles."

The requirements under NEVI are stated as follows.

- ***680.108 Interoperability of electric vehicle charging infrastructure.***

(a) Charger-to-EV communication. Chargers must conform to ISO 15118–3 and must have hardware capable of implementing both ISO 15118–2 and ISO 15118–20. By February 28, 2024, charger software must conform to ISO 15118–2 and be capable of Plug and Charge. Conformance testing for charger software and hardware should follow ISO 15118–4 and ISO 15118–5, respectively.

- ***FHWA clarifications on ISO 15118***

Plug and Charge refers to a charging initiation method where an EV charging customer simply plugs their vehicle's connector, triggering an authentication process through digital certificates as specified by ISO-15118. With that, a charging session starts and payment is transacted automatically, eliminating the need for any additional actions by the customer at the charging point.

5.2 ISO 15118 OVERVIEW

ISO 15118 is a standard that specifies the communication protocol between EVs and the charging infrastructure, ensuring interoperability and secure communication during the charging process. This protocol is instrumental in enabling the Plug and Charge functionality, streamlining authorization for EV drivers when connecting to compatible charging stations.

Through this protocol's Plug and Charge feature, EV drivers can obtain instant authorization at linked charging stations by plugging the vehicle into the charging point. As mentioned above these standards have been endorsed by FHWA's Final Rules.

Structured with a layered architecture, ISO 15118 encompasses the physical layer, data link layer, network layer and application layer.

Each layer carries specific responsibilities aimed at facilitating communication between EVs and charging stations:

Physical layer (ISO-15118-3)

The standard defines the physical connection between the EV and the charging station, specifying communication methods such as Powerline Communication (PLC) or other technologies.

Data link layer (ISO-15118-3)

This layer specifies data link protocols, error detection and correction mechanisms. It ensures reliable data transfer between the EV and the charging station.

Network layer (ISO-15118-2 and ISO-15118-20)

The network layer focuses on networking protocols, including addressing and routing. It manages the communication flow between the EV and the charging station.

Application layer (ISO-15118-2 and ISO-15118-20)

The highest layer is responsible for application-level protocols and messages exchanged between the EV and the charging station. Key functionalities include authentication, authorization and charging control.

The importance of application layer

The application layer within ISO 15118 serves as a vital component in establishing secure and interoperable communication between EVs and charging stations.

At the core of this layer lies the innovative Plug and Charge concept, which automates authentication and authorization processes, streamlining charging and eliminating the need for manual intervention.

The Plug and Charge system's security measures prevent unauthorized usage and provide an additional layer of protection against potential threats and vulnerabilities:

- Public Key Infrastructure (PKI) utilizes digital certificates, public and private keys and a trusted Certificate Authority (CA) to secure communication between the EV and the charging station.
- Authentication verifies the legitimacy of the EV's participation in the charging session.
- Authorization determines whether the EV has the necessary permissions to access the charging infrastructure.
- Encryption secures the communication channel, preventing unauthorized access and eavesdropping.
- Integrity checks and digital signatures verify the authenticity of messages between the EV and the charging station.

These features create a resilient framework, safeguarding sensitive information and instilling confidence in the reliability of the EV charging process.

In summary, Plug and Charge enhances user experience, while its security measures safeguard sensitive information and create a more trustworthy EV charging ecosystem.

5.3 THE DIFFERENCE BETWEEN ISO15118-2 AND ISO15118-20

ISO 15118-20 is an extension to the ISO 15118 standard which builds on the ISO 15118-2 version. It should be noted that while the newer version is based off of the original, they are not compatible with one another.

Here are the key enhancements from ISO 15118-20:

- **Fortified security measures**

Enforced data security: Mandates the use of Transport Layer Security (TLS) across all use cases and identification mechanisms to ensure encrypted communication channels and message authenticity.

- **Enhanced power transfer**

Bidirectional Power Transfer: Integration of bidirectional power transfer capabilities, or Vehicle-to-Grid (V2G), enables EVs to supply energy back to the grid.

Automated Connection Device (ACD): Introduction of ACD to facilitate automatic connection and disconnection processes for conductive energy transfer, particularly beneficial for scenarios like charging electric buses.

- **Charging flexibility and handling**

Wireless Power Transfer (WPT): Provision of a basic framework for WPT, accommodating ongoing changes in IEC 61980 specifications.

Dynamic control mode for flexible control delegation and multiplexed communication to enable parallel exchange of messages related to various services.

- **Streamlined contract handling**

Easier contract management simplifies the handling of multiple contract certificates, providing flexibility for diverse charging scenarios.

5.4 HOW TO NAVIGATE THE UPDATE

Embrace a strategic upgrade approach by:

- **Prioritizing needs:** Identify which aspects of the upgrade are most critical to your operations and prioritize them.
- **Phased implementation:** Consider a phased rollout to manage the transition smoothly, starting with pilot projects or specific sites.
- **Regulatory compliance:** Ensure the upgrade aligns with current regulations and standards, including those under the NEVI program.
- **Seeking expert guidance:** Tap into external expertise and consultancy services for seamless navigation through the upgrade process.

5.5 ISO 15118 IMPLEMENTATION FROM SCRATCH

Implementing ISO 15118 involves several steps to ensure that EV charging infrastructure adheres to the communication standards defined by ISO 15118. Here is a general implementation plan:

1. GET FAMILIAR WITH ISO 15118 STANDARDS

- Familiarize yourself with the ISO 15118 series standards, especially ISO 15118-2 and ISO 15118-20, to grasp communication protocols and prerequisites effectively.

2. ASSESS AND EQUIP

- Evaluate your current EV charging setup for compatibility with ISO 15118.
- Confirm that hardware and software on both EVs and charging stations are up to par for ISO 15118 standards.

3. STRENGTHEN SECURITY MEASURES

- Implement vital security measures like TLS, XML-based digital signatures and X.509v3 certificates for foolproof communication security.

4. TAILOR FEATURES TO FIT

- There are some optional and mandatory features. Create a plan and address the features as they may impact the security and operation.

5. TEST AND VALIDATE

- Thoroughly test implemented ISO 15118 features to verify seamless interoperability and standard compliance across diverse scenarios.

6. DOCUMENT AND EDUCATE

- Meticulously document feature implementations and configurations.
- Provide training to personnel involved in managing and maintaining the EV charging infrastructure.

7. AIM FOR CERTIFICATION

- Look into certification avenues to validate compliance with ISO 15118 standards and industry benchmarks.

8. EVOLVE CONTINUOUSLY

- Stay informed about updates and revisions to ISO 15118 standards.
- Continuously improve the implementation based on feedback, evolving technology and any requirements introduced in subsequent versions of the standards.

6. Cybersecurity state plans under NEVI funding

After analyzing 26 state plans, representing over 70% of the total NEVI Funding (+$610mil USD), we've uncovered key similarities and crafted a summary to offer insights into the cybersecurity state plans. From this, we've developed a comprehensive cybersecurity plan packed with innovative products and services.

Key observations:

- States uniformly **prioritize cybersecurity** to protect EV charging infrastructure, recognizing its central role to assure reliability and customer trust.
- The implementation of **annual reviews and updates for cybersecurity measures** to make sure that the infrastructure remains resilient and compliant with developing cybersecurity standards and threats.
- Emphasis on **compliance with cybersecurity standards** such as National Institute of Standards and Technology (NIST) guidelines, NEVI Standards, ISO 15118, OCPP and ISO 27001 for a powerful security structure.
- **Keeping customer data safe is a top concern.** With secure transmission and storage methods states are mitigating the risk of unauthorized access and breaches.
- **Incident response plans** are in place to swiftly address cyber threats and minimize potential disruptions and vulnerabilities as soon as possible. Many of these cybersecurity measures are mandated through contractual agreements [DR1] for suppliers.
- Numerous states integrate **physical security measures** in conjunction with their cybersecurity strategies to protect both infrastructure and users.

With a sharp eye on following the rules, safeguarding data and handling incidents, states are taking proactive steps to tackle cyber threats head-on. This united front, backed by substantial funding, highlights a shared commitment to protecting the trustworthiness and safety of the EV charging network.

6.1 CYBERSECURITY ATTACKS EXPLAINED

The state plans also specify attacks they try to mitigate. These attacks represent the primary cyber threats that state plans aim to mitigate in the context of EV charging station security:

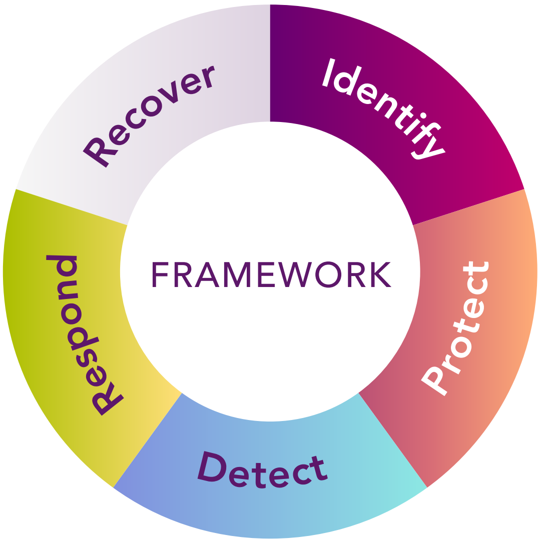
- **Intrusion attacks (23.08%):** Unauthorized access attempts into the network or systems that can compromise sensitive data and disrupt operations.
- **Data breaches and information leakage (21.15%):** Theft of sensitive customer data, such as payment information and personal details.
- **Malware installation and propagation (17.31%):** Malware, which can infect systems through various means, including compromised software updates or security vulnerabilities.
- **Physical tampering and unauthorized access (15.38%):** Although not a cyber attack in the traditional sense, several plans included measures against physical tampering of charging stations and unauthorized physical access, which could lead to cyber vulnerabilities.
- **Denial of Service (DoS) attacks (13.46%):** Attacks, which can disrupt the availability of charging stations by overwhelming the network with traffic.
- **Billing and payment fraud (9.62%):** Manipulating payment systems or stealing payment information.

6.2 CYBERSECURITY STRATEGY/PLAN

An intro to NIST cybersecurity framework

The NIST cybersecurity framework is a voluntary framework for critical infrastructure that consists of standards, guidelines and best practices to manage cybersecurity-related risk. Its prioritized, adaptable and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

The framework comprises three main components:



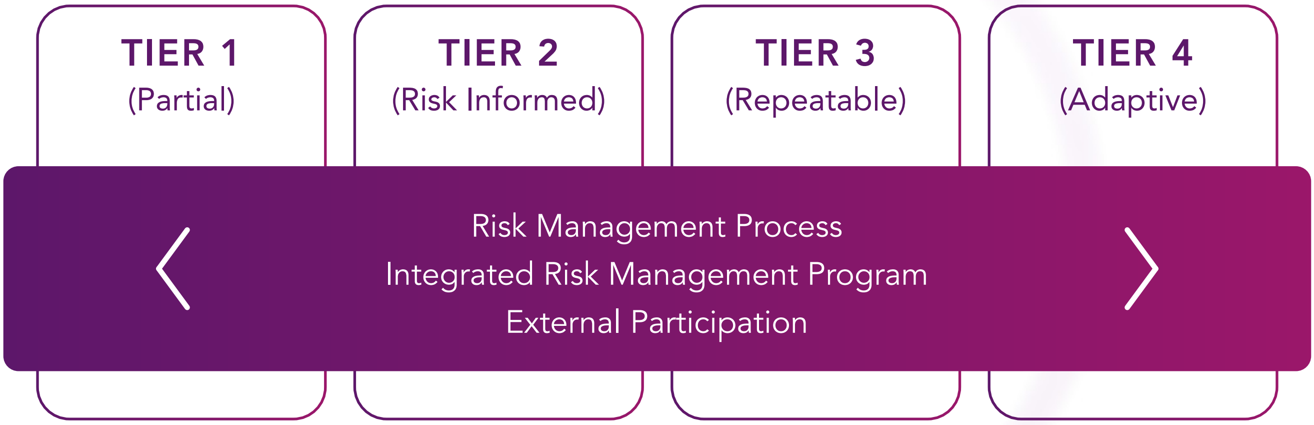
1. COMPONENT #1: THE FRAMEWORK CORE

A clear set of activities, desired outcomes and references, explaining what it takes to be secure and resilient in a language that is understandable to a broad audience. The core is structured into three parts – functions, categories and subcategories and includes five high-level functions:

These five functions are not only applicable to cybersecurity risk management but also to risk management at large.

2. COMPONENT #2: THE FRAMEWORK IMPLEMENTATION TIERS

These tiers help organizations by providing context on their approach to cybersecurity risk management. They describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework (e.g., risk and threat awareness, repeatability and adaptability).



3. COMPONENT #3: THE FRAMEWORK PROFILES

Profiles align standards, guidelines, and practices to the framework core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "current" profile (the "as is" state) with a "target" profile (the "to be" state).

The third component listed above is what every company searching for compliance per the NEVI guidelines should be looking at.

Understand your position

When creating a current profile, a company should assess its cybersecurity posture by evaluating its adherence to relevant standards, guidelines, and practices in alignment with the framework core. This involves identifying the cybersecurity measures currently in place, understanding how effectively they address risks and documenting the strengths and weaknesses of the current state.

Next comes defining a target profile, outlining the desired cybersecurity posture the company aims to achieve. This involves aligning standards, guidelines and practices with the framework core while considering regulatory requirements, industry best practices and risk tolerance. It's helpful to refer to specialized resources like the *NIST IR 8473 Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure*; this guideline has been meticulously created to meet the requirements of the diverse ecosystem players in the e-mobility world.

Following that, the company should craft a roadmap to bridge the gap between the current and target profiles. This plan should outline actionable steps and priorities for enhancing cybersecurity measures, such as implementing new controls, updating policies, investing in security technologies and providing staff training.

Continuous monitoring and reassessment are essential throughout this process to track progress, identify emerging threats and adjust strategies accordingly. By refining current and target profiles based on evolving cybersecurity needs and trends, the company can effectively strengthen its security posture and protect its assets, data and operations against cyber threats.

By doing this, a company will already cover over 90% of what is stated in the NEVI funding program. These include, but are not limited to the following:

- Asset identification (physical and software)
- Cybersecurity planning and strategy (annual updates)
- Product development against standards
- Implementation of physical security measures
- Conducting a threat and risk analysis
- Governance
- Audit and reporting
- Execute risk assessment
- Cybersecurity vigilance and training
- Best practices implementations like threat identification, risk prioritization, reporting mechanism, risk mitigation plan and data encryption, amongst others.

Another vital aspect to consider for NEVI Funding is data classification and privacy level definition for various data sets. While the NIST cybersecurity framework primarily addresses cybersecurity risks for safeguarding critical infrastructure and information assets, it doesn't extensively cover privacy concerns.

To fill this gap, it's advisable to refer to the *NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."* This resource provides guidance on privacy controls for federal information systems, including access controls, encryption and auditing, ensuring the confidentiality, integrity and availability of personal information.

RECOMMENDATION

Conduct a Privacy Impact Assessment (PIA) to evaluate and manage potential privacy risks associated with technologies or projects. A PIA evaluates how a system, application or process collects, uses, shares and manages personal information. It identifies potential privacy risks and outlines mitigation strategies, ensuring compliance with relevant privacy laws, regulations and organizational policies. NIST recommends conducting these assessments as part of the risk management process.

Implement products for compliance and operations

Once compliance requirements are clear and a plan is in place, it's time to act. Some products may be implemented before preceding steps, requiring later integration. If needed documentation is lacking, conduct audits, seek certifications or include services in risk assessments.

Sets of products for the charging stations

Based on the recommendations and state plans, four main sets of products/services will be implemented in the charging stations. The priority of the implementation and frequency of how many states require these systems go from the first to the last.

SET OF PRODUCTS #1: PKI, cryptographic agility and support for multiple PKIs

PKI is integral to secure communication and data exchange in EV charging networks as outlined previously in ISO 15118, OCPP, and OCP. These standards and protocols rely on certificate exchange. They provide secure authentication, encryption and digital signatures, verifying identities and securing communication channels between EVs, charging stations and operators. PKI enables secure charging processes, remote management, monitoring and billing. It secures information exchanges, supports various cryptographic methods and multiple PKIs and ensures the authenticity of devices.

Additional organizational and product hassles can be tackled by implementing a comprehensive and complete serviced Key Lifecycle Management System (KLMS).

SET OF PRODUCTS #2: User identity and access management

This set ensures that only authorized personnel have access to resources within organizations. It focuses on implementing robust solutions for user authentication and access control to maintain system security. It involves policies, technologies and processes managing digital identities, authentication, authorization and user account management.

Identity and access management systems control access based on user roles and responsibilities. This includes features like single sign-on, multi-factor authentication and password management, aiming to streamline access control and ensure compliance.

User management is essential in the EV-relevant standards. The standards define protocols for secure communication amongst several stake holders, ISO 15118 between EVs and charging stations, and OCPP and OCPI between charging stations and central management systems.

SET OF PRODUCTS #3: Software and firmware update and patch management

This set focuses on secure and timely updates to prevent malware installation and propagation with managing software vulnerabilities and maintaining system integrity.

According to NIST, software and firmware updates involve modifying existing software or firmware on a device to address security vulnerabilities and bugs or introduce new features. Patch management is a systematic process of acquiring, testing and installing patches (code changes) to resolve vulnerabilities in software and firmware.

Software updates and patch management are vital for maintaining the security, functionality and interoperability of EV charging infrastructure. These aspects are addressed within standards like ISO 15118, OCPP, and OCPI, providing mechanisms for securely deploying updates to EVs and charging stations to address vulnerabilities and bugs or introduce new features.

SET OF PRODUCTS #4: Intrusion Detection and Incident Management System

This set is a separate product and involves utilizing systems to monitor, detect and respond to cyber threats, including malware and unauthorized access attempts. It emphasizes the need for documented proof of these mechanisms' capabilities and maintaining incident response plans for swift action in case of breaches.

In the context of ISO 15118, OCPP, and OCPI standards, intrusion detection and incident management systems play central roles in EV charging networks' cybersecurity. An intrusion detection system monitors network traffic and system logs to identify and respond to unauthorized access attempts and potential security breaches, aligning with the security objectives outlined in these standards. Incident management systems provide a structured approach to managing and responding to security incidents, providing effective handling of cybersecurity threats and incidents following standard requirements.

6.3 BEST PRACTICES

To complement the strategy above, we wanted to provide an example of best practices that are shown in the 2023 Missouri plan.

Recommended cybersecurity best practices, including risk management, configuration and change management, identity and access management are available here.

An extended list of further standards and requirements can be found below

- NEVI Standards and Requirements (23 CFR 680): Federal standards specific to the National Electric Vehicle Infrastructure program.
- NIST:
  - NIST SP 800-115: Technical Guide to Information Security Testing and Assessment.
  - NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.
  - NIST 800 series in general for cybersecurity standards and practices.
- Payment Card Industry Data Security Standards for securing credit and debit card transactions and protecting cardholder data.
- Health Insurance Portability and Accountability Act U.S. legislation for data privacy and security provisions for safeguarding medical information.
- North American Electric Reliability Corporation Critical Infrastructure Protection Standards to secure the assets required for operating North America's bulk electric system.
- Architecture Reference for Cooperative and Intelligent Transportation for a framework for planning, defining and integrating intelligent transportation systems.
- OCPP: An application protocol for communication between electric vehicle charging stations and a central management system.
- ISO 15118: An international standard defining the communication between electric vehicle charging stations and electric vehicles.
- ISO 27001: An international standard for managing information security.
- PKI: A set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
- FHWA NEVI Final Rule 23 CFR 680: Federal regulations governing the NEVI program.
- State-specific cybersecurity legislation: Various states mentioned compliance with their specific cybersecurity laws and regulations.
  - Arizona Statewide Policy (8130) System Security Acquisition and Development: A specific policy for system security in the state of Arizona.
  - Code of Virginia Breach of Personal Information requirements: State legislation in Virginia regarding the breach of personal information.
  - Office of the Chief Information Officer Security Standards - Washington Security policy and standards for state computer systems and networks in Washington.
  - Senate Bill 327 - California: Legislation specific to California regarding the security of connected devices.

irdeto

Protect. Renew. Empower.

Irdeto is the world leader in digital platform security offering cyber services and technology solutions that protect platforms, digital assets and software applications across multiple industries. Irdeto's products meet the rapidly changing mobility demands and exceed cybersecurity regulations for automotive and beyond. We provide solutions throughout the product lifecycle to prevent cyberattacks and help protect assets for connected cars, commercial fleet and construction equipment.

With a rich heritage of security innovation and rapid adaptation to the changing demands of the cyber security space, Irdeto is the preferred partner to empower a secure world where people can connect with confidence.

metergram

Metergram provides advisory services, software development services and system integration for EV charging. We're dedicated to providing Charge Point Operators and eMobility Service Providers with custom, easily integrated solutions tailored to the unique demands of the EV charging sector.

Understanding that our clients face diverse challenges across the EV ecosystem, we focus on creating software that not only meets but exceeds their expectations. Utilizing standards like OCPP and OCPI, we ensure our solutions enhance connectivity and streamline operations.

Our team is all about collaboration, working closely with clients to craft software that optimizes user experience and accelerates value delivery. As innovators and contributors to industry standards, Metergram is your partner in driving the evolution of EV charging with superior software solutions.