Thought Leadership
White Paper

Cybersecurity considerations for electric vehicle charging

Sai Murahari
Product manager for electric vehicle charging infrastructure at Eaton
Frank Sanjay
Manager, Product Cybersecurity Center of Excellence at Eaton

The development of dependable, safe and secure commercial charging networks is essential to electric vehicle (EV) adoption and decarbonization. Cybersecurity is foundational to making that happen.

The U.S. federal government currently aims for EVs to make up 50% of all vehicle sales by 2030 and is setting the stage for a nationwide network of 500,000 EV chargers within the same timeframe. Connectivity is key for the effective operations of this vast charging network, enabling stations to communicate with owners, operators and the grid to authorize charging, sequence charging processes, manage payments, manage electrical loads and more.

Fostering adoption of electric transportation hinges on consumer confidence that these networked charging stations provide the ability to charge quickly, safely, sustainably, affordably and securely. For fleet managers, property owners and facility managers alike, this makes it critical to have a secure, reliable and seamless integration between the hardware and software components used across these connected EV charging applications.

What's important is keeping people safe on the roads, protecting the grid and everything in between. This will take effort from manufacturers committed to designing products and systems with a "defense in depth" approach that not only provides protection against the cyberattack threats of today, but also the emerging vulnerabilities of tomorrow. Responsibility will also fall upon the shoulders of charging network owners and operators to configure and continually manage their EV charging networks to reduce risk.

Powering Business Worldwide

Cybersecurity has never been more important

The federal government is already requiring states to implement physical and cybersecurity strategies for EV charging networks.[1] This is important because grid-connected EV charging networks present a demand-side security threat that could potentially disrupt grid operations. There are many prevalent weaknesses that must be addressed across EV charging networks to ensure secure physical access, system hardening, network protection and monitoring.

If a network is not secured, a well-informed malicious actor could try to destabilize the grid by manipulating charging devices. Additionally, with the easy availability of public data for network configurations, transformer lines and load parameters and charging stations, there is a lot more that could be compromised.

These threats include the unauthorized operation of chargers, compromise of customer credentials, and the ability to gain full control of chargers to either steal electricity, deactivate chargers or potentially inhibit the functionality of vehicles attempting to charge.

As EV adoption increases, so does the potential risk of cyberattack. This makes cybersecurity a foundational consideration that is essential to EV adoption and a more sustainable future.

Our hyper-connected world must be built on a foundation of cybersecurity and it's critical that everyone involved in applying and developing connected technologies takes steps to create secure environments.

Customers need confidence that their charging infrastructure is constructed with trusted products. This means strict procedures and cybersecurity protocols need to be integrated at every phase of product development that involve people, processes and technologies. And everyone involved in the application and development of connected technologies must take steps to create secure environments. When new connected technologies are applied, it is essential to constantly evaluate your systems to understand the associated risks and ways to reduce risk.

Taking the lead on cybersecurity

At Eaton, we believe cybersecurity is an essential consideration in the development of EV charging technology – just like safety and quality – and threats must be met proactively with a systemwide "defense in depth" approach.

Our approach hinges on the ability to constantly evaluate connected systems when new technologies are applied to understand the associated risks and ways to reduce vulnerability.

At Eaton, this approach begins with a Secure Development Lifecycle (SDL) methodology for product development that places cybersecurity front and center, from inception to deployment and lifecycle maintenance. SDL is a proven strategy that can help us stay ahead of cybercriminals by managing cybersecurity risks throughout the entire lifecycle of a product or solution.

We take SDL very seriously to proactively manage cybersecurity risks in products through a framework involving threat modeling, requirements analysis, implementation, verification and ongoing maintenance.

Our product development processes are certified to The International Electrotechnical Commission (IEC) 62443-4-1 standards for secure product lifecycle development in the electrical industry. This IEC standard specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development lifecycle for developing and maintaining secure products. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products.

For manufacturers, adopting a SDL approach that has been validated by a third-party is critical to creating trusted environments. It's this third-party certification that gives customers confidence in the processes and technologies they're applying, much like safety certifications and standards in the National Electric Code (NEC).

Beyond adhering to SDL development processes, it is also critical that organizations across the electrical industry establish a robust cybersecurity program that includes periodic assessment of their networks to ensure they stay on top of vulnerabilities. If this expertise is not available through in-house resources, they can leverage Eaton's cybersecurity services.[2] In addition to assessments, Eaton provides solutions and services designed to help customers deploy robust defense-in-depth strategies.

Although the application of EV charging is somewhat new, the nature of cybersecurity remains the same. It's a continuous journey with constantly evolving complexities, threat scenarios and technologies. For the sake of our customers and their critical systems, it's important that we all start thinking like cybersecurity engineers and embark on that journey together. Everyone in the development chain is vital for success in cybersecurity.

Unified codes and standards will support a secure future for EV charging

Moving forward, advancing cybersecurity in our increasingly connected world will require industries and standards organizations to identify a unified global criterion for assessing products.

Across every industry, connected devices and software must be validated with global standards that can be applied to any application. It's essential for all of us—businesses, communities and governments—to work together to share best practices and pioneer a collection of global cybersecurity standards.

At Eaton, we're partnering with organizations within our industry, academia and beyond to support a more cybersecure world. And our experts are helping advance cybersecurity by leading and participating in the organizations developing cybersecurity standards, including supporting the first ever automotive cybersecurity standard—ISO/SAE 21434 and ongoing efforts to provide more guidance. Already, the auto industry and suppliers are rapidly adopting the ISO/SAE 21434 standard.

We believe this deep level of collaboration is an integral aspect of our proactive and consistent enterprise-wide approach to cybersecurity. We also believe industry codes and standards are essential.

We're actively collaborating with renowned standards and industry leaders to accelerate the development of measurable cybersecurity criteria that will serve as a platform for trusted connections for decades to come.

For example, in 2020 we became the first company to have our product development processes certified for cybersecurity by both the International Electrotechnical Commission (IEC) and global safety science organization UL. We also helped develop and endorse adoption of UL 2900 [3] and IEC 62443 cybersecurity standards creating measurable cybersecurity criteria for connected devices, associated systems and development processes.

These types of certifications underscore Eaton's leadership in providing customers with confidence that its connected solutions comply with proven industry guidelines.

How we incorporate cybersecurity into EV charging networks

Following our SDL, we proactively incorporate cybersecurity into multiple levels of the design behind our EV Chargers. This all starts with the most stringent threat modeling and penetration testing for our designs and communications protocols.

We comply with the industry's Open Charge Point Protocol (OCPP), which is governed by the Open Charge Alliance (OCA) and formally certifies products for compliance. The cybersecurity aspect of OCPP defines an end-to-end security design architecture, with implementation guidelines for both charging devices and management software. By applying Eaton's comprehensive cybersecurity approach, customers can have robust solutions that extend beyond OCPP.

On the hardware side, we integrate cybersecurity at every level, including ports, communications modules and third-party controllers. Additionally, we continuously monitor vulnerabilities reported against our software components in our EV chargers.

Going one step further, we design our chargers to accept authentic and trusted firmware. To prevent intrusion, we integrate novel code that knows how to reject potentially harmful firmware uploads.

8 essential cybersecurity best practices for EV charging

Cybersecurity needs to be a foundational capability and function. Secure-by-design principles need to be applied not only during the entire product development process but also throughout deployment. That includes employing secure maintenance practices, like updating EV charging firmware prior to deploying the technology and applying firmware updates and software patches regularly.Our approach hinges on the ability to constantly evaluate connected systems when new technologies are applied to understand the associated risks and ways to reduce vulnerability.

The following provides basic tips for the deployment and maintenance of EV charging solutions to help minimize cybersecurity risks across commercial and fleet applications. This is not a comprehensive guide but intended to complement your existing cybersecurity programs.

1. **Keep track of software and hardware assets** in your environment. This is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component.

   Additionally, new providers should incorporate EV chargers into business continuity and disaster recovery plans by backing up and securely storing important device configuration and network details. This includes periodically reviewing and, where possible, exercising these plans.

2. **Conduct a risk assessment to identify and assess** reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system and device and its environment. This should be conducted periodically and in accordance with applicable technical and regulatory frameworks like IEC 62443 and NIST Standards.

3. **Physical security is essential.** An attacker with unauthorized physical access can cause serious disruptions. Physical security is an important layer of defense.

   EV chargers present a unique challenge in this area, as they need to be placed in publicly accessible areas. Therefore, manufacturers need to account for this factor in their enclosure designs and installers should provision for CCTV monitoring of the chargers.

   Chargers with the capability to freely connect removable media may be exposed to physical security threats. You should not connect removable media unless the origin of the media is known and trusted. Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

   Cyber risks can also creep into devices, systems, software and services if supply chains do not perform cybersecurity due diligence

4. **Harden third-party commercial off-the-shelf operating systems or platforms** that are used to run Eaton EV charging hardware and/or software. Our hardware and software are designed for interoperability and is Open Charge Point Protocol (OCPP) compliant. As you deploy other OCPP-compliant technologies, it is important to take heed of industry best practices. This includes installing all security updates made available by the manufacturer, changing default credentials upon first login, disabling or locking unused built-in accounts, and limiting use of privileged generic accounts. You should also change default SNMP community strings, restrict SNMP access using access control lists and disable unneeded ports and devices.

5. **Network communications need to be configured securely.** Segmentation of networks, denying traffic between segments except what is specifically allowed and restricting communications to host-to-host paths is essential. Open only those ports that are required for operations and protect the network communication using protection and intrusion detection systems. Further, all logs should be protected, retained (for a reasonable time) and reviewed.[4]

   Further, it is important to continually scan for vulnerabilities. Any known critical or high-severity vulnerabilities on third-party component libraries used to run applications should be remediated first. Adequate malware defenses also need to be deployed to protect your EV chargers and related software applications.

6. **Strict management and validation of remote access is vital for maintaining control over security.** Connecting EV chargers to a network is essential for monitoring, access control, collecting payments and more. Remote access to this network should be stringently and actively managed to prevent intrusion.

7. **Take heed of best practices for secure system development when you develop and host an application on your chargers.** Security vulnerabilities in these applications may expose the underlying device to an attack. Ensure that you select trustworthy suppliers who understand the importance of cybersecurity and have a robust cybersecurity program that follows the NIST Cybersecurity Framework or is third-party certified by UL 2900, IEC 62443, ISO/SAE 21434 or other widely recognized industry standards.

8. **Sensitive information stored in your devices should be adequately protected through the deployment of your organizational security practices.** Data privacy needs to be a primary consideration—from storing data to processing it and when it comes time to decommission chargers. For example, data should be purged from devices before they're disposed (see NIST SP 800-88 guidelines for additional information).

Building secure EV charging networks for today and the future

Whether the objective is to disrupt operations or create an entry point to higher value business assets, the tools and the techniques used for unauthorized network access are becoming increasingly sophisticated. These threats must be considered when developing EV charging infrastructure that depends on network connectivity to simplify system deployment, effective operation, and ongoing maintenance and management.

As EV adoption surges and more states begin to require charging infrastructure across new and retrofit construction projects, it is a necessity to have a robust cybersecurity program in place that addresses people, processes and technology.

It is important to address evolving cyber threats proactively using a best-in-class, standardized defensive approach with an unwavering focus on the malware, spyware and ransomware present across the globe. Ensuring the security of your EV charging hardware and software assets is critical to maintaining the safety and uptime of operations and your reputation—because a vulnerability on these critical pieces of energy infrastructure not only puts the availability of that equipment at risk, but potentially provides access to higher value targets on the primary IT network.

For manufacturers, this means adopting a proven secure development approach to help support a secure future for EV charging by managing cybersecurity risks in products through the entire product life cycle. And for owners and operators, it is critical to select products and suppliers backed by trusted third-party accreditations that give EV charging network users confidence they are plugging into a system that is built to be secure by design

The electric revolution is here. Although we're in the early stages of EV adoption, we all have a responsibility to safely and securely build out the infrastructure needed to support and accelerate the future of electric transportation.

About Eaton's Cybersecurity services

Eaton offers a suite of cybersecurity assessment and life-cycle management services to help identify vulnerabilities and secure your operational technology networks. These services can help you complete the recommended remediation and mitigation actions and strengthen your overall network security. More information about these services is available at **Eaton.com/cybersecurityservices**

About Eaton

Eaton is an intelligent power management company with 2022 revenues of $20.8B that is dedicated to improving the quality of life and protecting the environment for people everywhere. By capitalizing on the global growth trends of electrification and digitalization, we're accelerating the planet's transition to renewable energy and helping to solve the world's most urgent power management challenges. 2023 marks Eaton's 100th anniversary of being listed on the New York Stock Exchange.

For more information, visit **Eaton.com**

References

1 Department of Transportation

2 Eaton cybersecurity services

3 UL 2900

4 Cybersecurity considerations for electrical distribution systems

For more information, visit

Eaton.com/evchargers
Eaton.com/cybersecurity
Eaton.com/cybersecurityservices

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP191002EN / SMC
Rev.01
September 2023

Follow us on social media to get the latest product and support information.

Powering Business Worldwide