

Utilities & Platform Requirements



Carolyn Weiner
Program Director
EVCAN



EV Charging Accessibility Network

Utilities and Platform Requirements

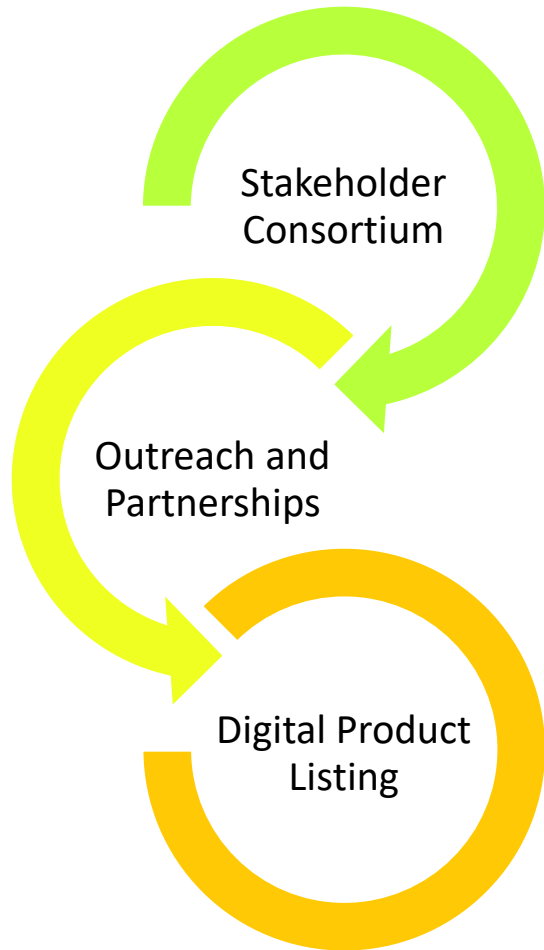
May 12, 2026



We are a 501c3 nonprofit organization with deep roots in energy efficiency and decarbonization

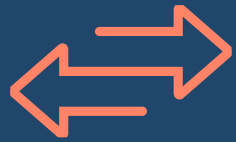


Our Approach



- Mobilize Utility leaders around a common set of technical requirements.
- Through strategic partnerships and manufacturer engagement, collect and publish vetted, unbiased product information and performance data.
- Create a digital, qualified product solution and educational resources to accelerate access to safe, reliable, and accessible EV charging solutions.

Building a shared language on performance expectations



Encourage broad market interoperability



Smart energy management in station operations



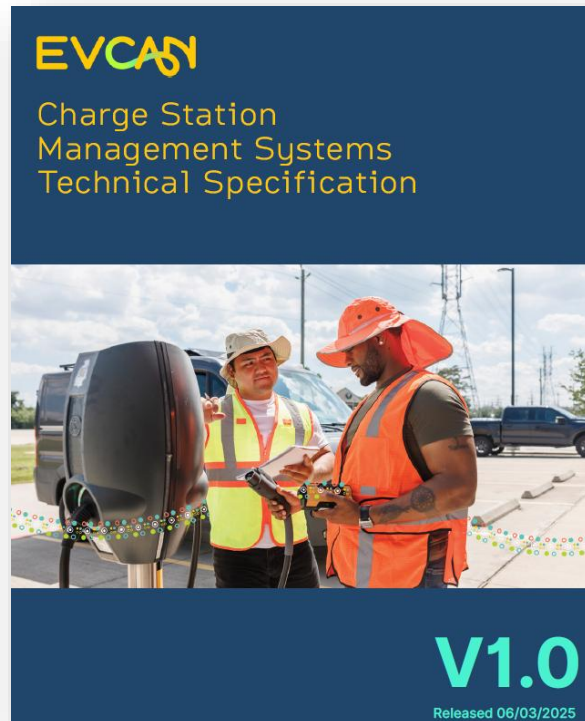
Consistent data reporting practices



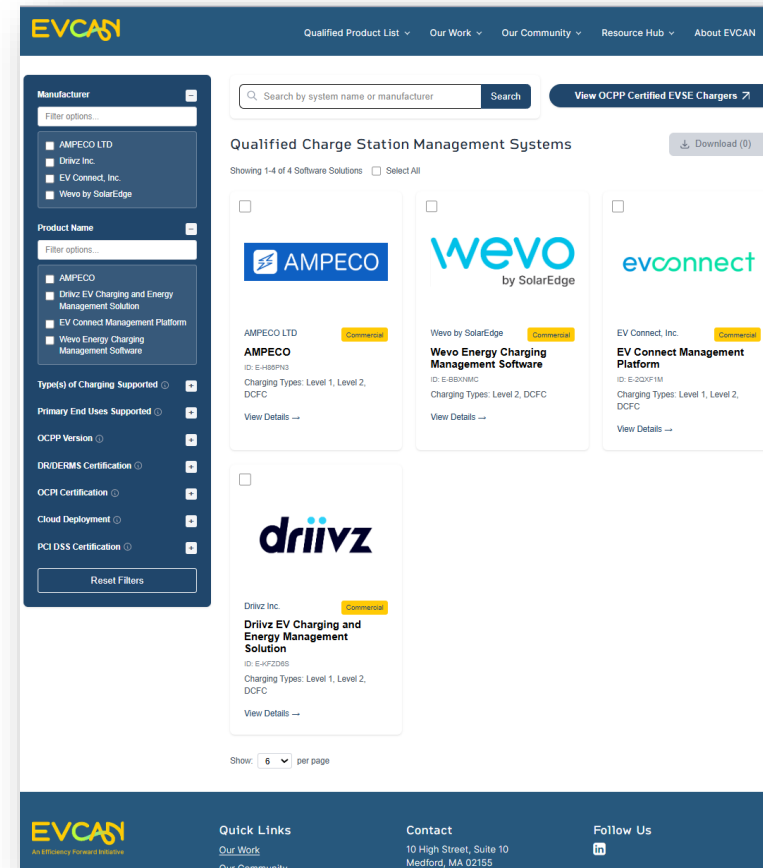
Transparent uptime and reliability

Two Main Resources

Technical Specification for Charge Station Management Systems




Qualified Product List (QPL)




How the Qualified Product List will be used


- ❑ 'Preferred' Reference
- ❑ Equipment Requirement



Fleet/MDHD EV charging programs

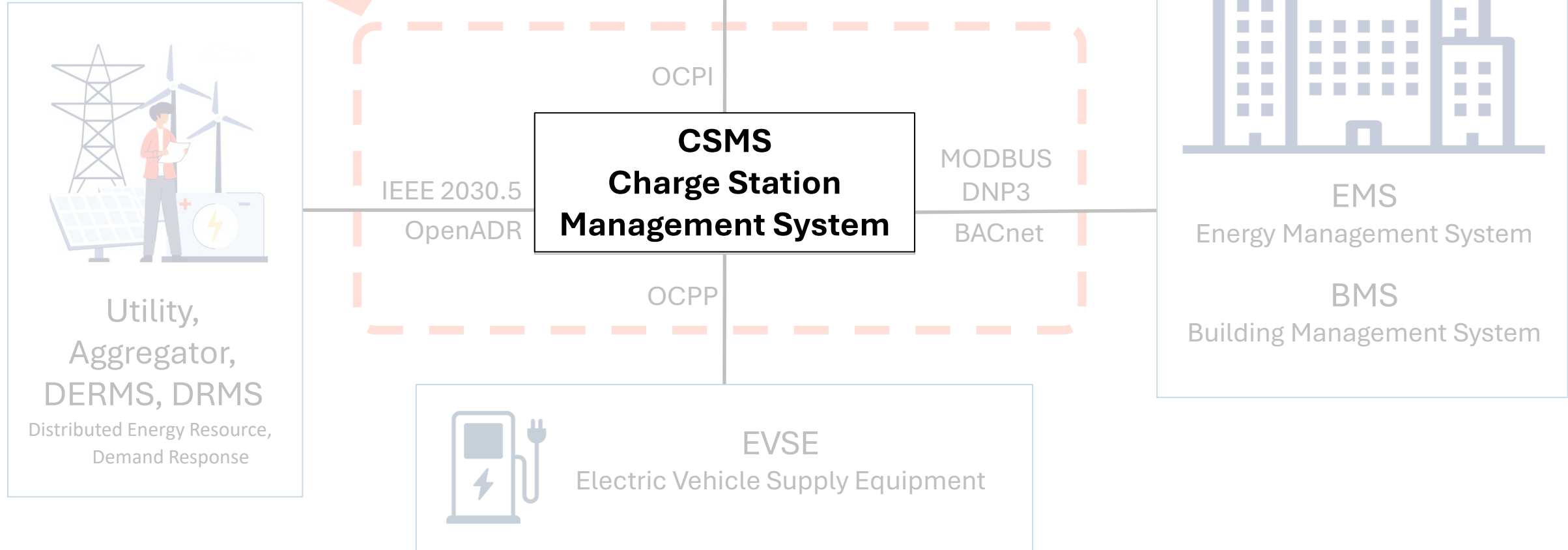


EV energy management or commercial managed charging program



Reference for State/Local agency procurement

Scope of Specification



Cybersecurity Standards Recognized by EVCAN



Standard	Process (all)	Cloud Services (if used)	Payment (if used)
ANSI/UL 2900-1	Y		
ANSI/ISA/IEC 62443-4-1	Y		
ANSI/CSA T200	Y		
SOC 2	Y	Y	
ISO/IEC 27001	Y		
ISO/IEC 27017		Y	
FedRAMP		Y	
CSA STAR		Y	
PCI DSS			Y

Why so many certifications?





ANSI/ISA/IEC 62443

ISA/IEC 62443 Family of Standards

General	ISA-62443-1-1 Terminology, concepts, and models	ISA-62443-1-2 Master glossary of terms and abbreviations	ISA-62443-1-3 System security conformance metrics	ISA-TR62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	ISA-62443-2-1 Establishing an IACS security program	ISA-62443-2-2 IACS security program ratings	ISA-TR62443-2-3 Patch management in the IACS environment	ISA-62443-2-4 Security program requirements for IACS service providers	ISA-TR62443-2-5 Implementation guidance for IACS asset owners
System	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-3-2 Security risk assessment for system design	ISA-62443-3-3 System security requirements and security levels		
Component	ISA-62443-4-1 Product security development lifecycle requirements	ISA-62443-4-2 Technical security requirements for IACS components			

p.5, ISAGCA Quick Start Guide FINAL.pdf from www.ISA.org/ISAGCA

SOC 2 (Service Organization Controls) AICPA (American Institute of Certified Public Accountants)



A screenshot of the AICPA website page titled "SOC for Service Organizations". The page features a navigation bar with "AICPA.org", "Store", "My Account", and "Become a Member" buttons. Below the navigation is a search bar and a menu with categories like "Topics", "Career Guidance", "CPE & Learning", "Certifications", "News & Advocacy", and "Membership". The main content area includes a breadcrumb trail: "AICPA > Topics of Interest Overview > Financial Reporting Center (FRC) > Assurance and Advisory > SOC for Service Organizations". The title "SOC for Service Organizations" is prominently displayed, followed by social media sharing icons for Facebook, Twitter, LinkedIn, Email, and Print. A descriptive paragraph states: "SOC for Service Organizations are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service." Below this text are three circular logos for "AICPA SOC" with the URL "aicpa.org/soc4so". Under each logo is a label: "CPAs" (with a calculator icon), "Users & User Entities" (with a photo of a woman working on a laptop), and "Service Organizations" (with a calculator icon).

SOC 1 and SOC 2 Reports

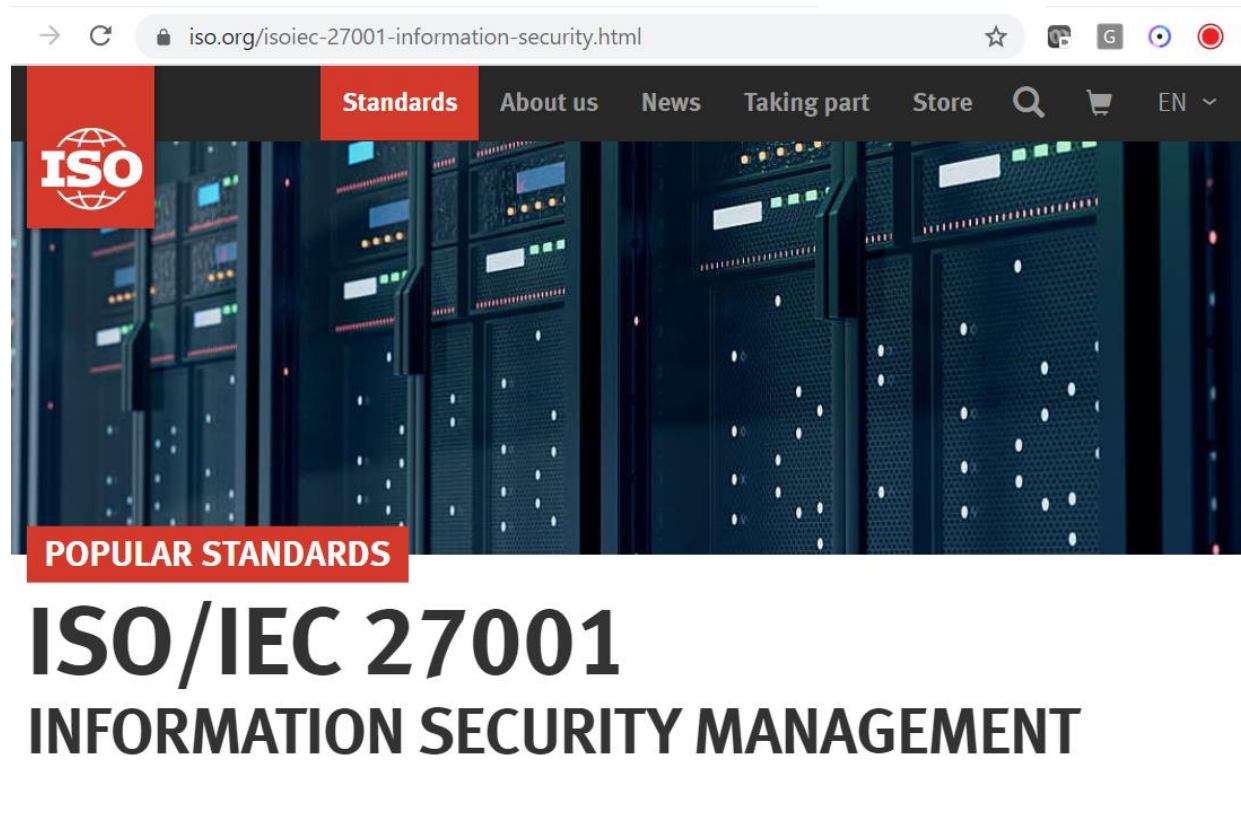
- Type I describes a vendor's systems
- Type II tests the operational effectiveness of those systems



<https://www.imperva.com/learn/data-security/soc-2-compliance/>

ISO/IEC 27001

Global Standard for Information Security Management Systems



<https://www.iso.org/isoiec-27001-information-security.html>

ISO management system 3-stage external audit

1. Preliminary informal review
2. Formal test against standard
3. Ongoing (for 27001, annual or more frequently)



ISO/IEC 27017 for cloud services (providers & customers)



<https://www.iso.org/standard/43757.html>

The screenshot shows a web browser window with the URL [iso.org/standard/43757.html](https://www.iso.org/standard/43757.html). The page features a navigation bar with links for Standards, About us, News, Taking part, Store, a search icon, a shopping cart icon, and language options (EN). The main content area displays the ISO logo, a breadcrumb trail (ICS > 35 > 35.030), and the title **ISO/IEC 27017:2015**. Below the title is the subtitle: **Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services**. A grey box at the bottom of the page contains the text: **THIS STANDARD WAS LAST REVIEWED AND CONFIRMED IN 2021. THEREFORE THIS VERSION REMAINS CURRENT.**

Cybersecurity Standards Recognized by EVCAN



Standard	Process (all)	Cloud Services (if used)	Payment (if used)
ANSI/UL 2900-1	Y		
ANSI/ISA/IEC 62443-4-1	Y		
ANSI/CSA T200	Y		
SOC 2	Y	Y	
ISO/IEC 27001	Y		
ISO/IEC 27017		Y	
FedRAMP		Y	
CSA STAR		Y	
PCI DSS			Y

EVCAN Qualified Product List / Product Details

The screenshot shows the EVCAN website's 'Qualified Product List' page. At the top, there is a navigation bar with the EVCAN logo and menu items: 'Qualified Product List', 'Our Work', 'Our Community', and 'Resource Hub'. Below the navigation is a search bar with the placeholder text 'Search by system name or manufacturer' and a 'Search' button. A button labeled 'View OCPP Certified EVSE Chargers' is also present. The main content area is titled 'Qualified Charge Station Management Systems' and includes a 'Download (0)' button. It displays three product cards, each with a manufacturer logo, name, ID, charging types, and a 'View Details' link. The third card, for 'EV Connect, Inc.' and 'EV Connect Management Platform' (ID: E-2QXF1M), is highlighted with a yellow circle. The other two cards are for 'AMPECO LTD' (ID: E-H86PN3) and 'Wevo by SolarEdge' (ID: E-BBXNMC).



The screenshot shows the 'EV Connect Management Platform' product details page. The page title is 'EV Connect, Inc. EV Connect Management Platform'. There is a navigation bar with 'Overview' selected. The main content area is divided into two columns. The left column lists features: 'Communication Interfaces', 'Cybersecurity' (highlighted with a yellow circle), 'Monitoring and Control of EVSE', 'Energy Management', 'Data Analytics and Reporting', and 'Operations, Safety, and Reliability'. The right column contains the 'evconnect' logo and a 'Visit Product Website' link. Below this is a 'Product Information' section with a table of details:

Product Information	
Manufacturer	Technical Specifications Version
EV Connect, Inc.	v1.0
Product Name	Listing Status
EV Connect Management Platform	Active
Type(s) of Charging Supported	Date Qualified
Level 1, Level 2, DCFC	Aug 25, 2025
Primary End Uses Supported	Product ID
Commercial Residential Multifamily	E-2QXF1M
Public Fleet	

At the bottom of the page, there is the EVCAN logo with the tagline 'An Efficiency Forward Initiative' and a 'Print this Page' button.

EV Connect Management Platform

[Overview](#)[Communication Interfaces](#)[Cybersecurity](#)[Monitoring and Control of EVSE](#)[Energy Management](#)[Data Analytics and Reporting](#)[Operations, Safety, and Reliability](#)

Cybersecurity Features

As the EV infrastructure grows and becomes increasingly interconnected, cyber threats become more likely. Cyber threats can include unauthorized access, data breaches, and operational disruptions. Currently, no comprehensive cybersecurity standard exists for CSMS. EVCAN has divided required cybersecurity controls into three groups: Process, Cloud, and Payment. All qualifying systems must meet the requirement for Process standards and may qualify under Cloud and/or Payment if the system architecture matches the definition of those two groups.

Use of Cloud Services

✓ Deploys using Cloud Services

Cybersecurity related to Cloud Services:

✓ SOC2

Security Certifications

Cybersecurity related to Processes:

✓ SOC2

Cybersecurity related to Payment Services

✓ Payment Card Industry Data Security Standard Certification (PCI-DSS)



Power Through Connection

Thank You!

Carolyn Weiner
Program Director
cweiner@evcan.org

