DOCKETED	
Docket Number:	19-AB-2127
Project Title:	Implementation of AB 2127 Electric Vehicle Charging Infrastructure Assessments
TN #:	240941
Document Title:	EPRI Comments on ISO 15118 Charger Communications and Interoperability Nov 10 2021 Workshop
Description:	N/A
Filer:	System
Organization:	EPRI
Submitter Role:	Public
Submission Date:	12/15/2021 12:14:44 PM
Docketed Date:	12/15/2021

Comment Received From: Mark Duvall
Submitted On: 12/15/2021
Docket Number: 19-AB-2127

EPRI Comments on ISO 15118 Charger Communications and Interoperability Nov 10 2021 Workshop

Additional submitted attachment is included below.

December 15, 2021

California Energy Commission
Re: Docket No. 19-AB-2127
1516 Ninth Street
Sacramento, California 95814-5512

Submitted to on-line portal:
https://efiling.energy.ca.gov/EComment/EComment.aspx?docketnumber=19-AB-2127

Re: Comments on ISO 15118 Charger Communication and Interoperability Workshop on Nov 10, 2021, and the Staff Proposal

EPRI smart grid cybersecurity and Electric Vehicle infrastructure subject matter experts have been engaged in assessing the cybersecurity aspects of the EV charging infrastructure since 2014, starting with EPRI leadership of the National Institutes of Standards and Technology (NIST) Smart Grid Interoperability Panel (SGIP)[1] V2G Domain Expert Working Group. The workgroup comprising of domain experts across key stakeholder communities analyzed each of the VGI communication protocols for their inclusion in the NIST Catalog of Standards, that adhere to NIST cybersecurity requirements for the smart grid. Later, during the first iteration of California multi-agency VGI Working Group, the issue of comparative assessment of cybersecurity capabilities of the standards was raised. EPRI created an internal effort to raise the profile of this research area internally, which culminated in EPRI being awarded $2M by the DoE Vehicle Technologies Office FOA 1919 award for EV infrastructure cybersecurity, to define, test, recommend and democratize the knowledge of safeguarding EV infrastructure cybersecurity, including extreme fast charging, but also encompassing the entire ecosystem from the utility, the cloud providers, the EVSEs and the EVs as well as the networks and customer payment systems. An assessment application 'Integrated Grid Security Risk Management' is about to go online where anyone will be able to configure their system and identify risks related to grid stability, equipment reliability, financial and equipment/vehicle safety, in addition to obtaining a list of best practices on mitigation approaches that can be operationalized. EPRI is currently working with NIST to create an EV infrastructure Cybersecurity Profile that will be available for the practitioners to implement in the next 12-18 months.

During the Nov 10, 2021 workshop, EPRI experts put questions in the Q&A regarding cybersecurity. In this letter, we are following up with more specific recommendations for the CEC to address charging station (EVSE)[2] cybersecurity based on our experience working with USDOE and the National Institutes of Standards and Technology (NIST) on this topic. Specifically, we discuss the cybersecurity threat and solutions for both vehicle grid integration (VGI) and payment systems and consider the entire communications pathway from the EV to

[1] NIST Smart Grid Interoperability Panel (SGIP) activity was the result of the Smart Grid Interoperability Roadmap that EPRI led to create for the NIST in the early 2010s, as one of the actions stimulated by the EISA. The Roadmap identified the need to create the Catalog of Standards.

[2] Electric Vehicle Supply Equipment

the electric grid operator.[3] We also discuss our concerns regarding lack of harmonization between ISO and SAE standards and what this means for the CEC staff's proposal.

The cybersecurity threat is almost constantly in the newspapers. Recent high-profile examples – malicious code inserted (e.g., Target Stores)[4] or malicious chips added by the original manufacturer[5] are well known. In addition, White House executive orders have been issued to address the cybersecurity threat to critical infrastructure, including utilities.[6] Cybersecurity is also included as one of the guiding principles of the National EV Charging Initiative, which was recently developed in collaboration with over 30 organizations.[7]

Cybersecurity is an issue for the grid and the EV and for consumers. Examples of threats include:

- Identity thefts and fraud by compromising charging accounts to steal electricity, identity theft, or payment information.
- Destabilizing the grid and potentially causing major damage to infrastructure by taking control of a large number of chargers or a few high-power chargers and turning them all on or off at once, or if V2G capable, instructing a bunch of EVs to discharge power all at once.
- Destabilizing the grid by EVSEs requesting a lot of power when it is not actually needed, bringing too much power to a grid area.
- Sending excess power to the EVs causing them to overcharge, causing battery damage, and creating a fire hazard.
- Denial of service attacks by locking people out of charging, for example along a major highway. This could be a bigger threat once most transportation transitions to electric and could even be used in conjunction with shutting off charging operations during emergency response events etc.

For both payment systems and VGI there are many communication pathways. One way to think about the complexity of managing and mitigating against cybersecurity risks is to consider the communication pathways of two-party systems versus three-party systems[8]. It can be relatively more manageable to secure a two-party system over multi-party systems as the two parties can negotiate clearly defined business-to-business (B2B) procedural and technical security requirements. However, even in this case, as shown with the recent attacks, each party must ensure they are fulfilling their cyber security responsibilities, including ensuring that the systems they own are hardened according to the latest cyber security best practices and come from trusted original equipment manufacturer and software developers, who have established secure supply-chain and code development practices that prevent injection of malicious code or hardware backdoors. Thus, securing a three-party system can be very difficult due to

[3] Both utilities and the California Independent System Operators have a role with the electric grid.

[4] https://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/.

[5] https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/ [sans.org] and https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies [bloomberg.com]

[6] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity and Executive Order on Improving the Nation's Cybersecurity | The White House

[7] Principles — The EV Charging Initiative - A national collaboration to meet and exceed 500,000 charging stations nationwide page 9.

[8] Multi-party transactions are characterized by how many parties engage during an information exchange. Good examples of two-party transactions are: grid signaling that concerns the EV charging, originating at the grid and terminating at the EV, or, a payment transaction that originates at the EVSE, and terminates at the payment provider or clearinghouse server. A three-party transaction may be where the grid signal meant for the EV originates at the utility, lands at the EVSE, is translated and relayed to the EV.

complexities involved with establishing trusted processes and technical controls across a multi-party system. An example of a three-party system is when the EV sends signals to a cloud aggregator / server farm who then decrypts, opens, translates a protocol into a new protocol, encrypts and sends it to the grid operator. This interception and translation of communications involves a highly complex chain-of-trust that introduces multiple points of potential vulnerabilities that can be subject to Man-in-the-Middle (MitM) attacks. To protect against this, the owners of server farms constantly work and spend money on physical and cybersecurity and adhere to industry standards such as ISO 27001 or, for cloud service providers, FedRAMP. For example, quarterly penetration testing, cameras, locks and constant auditing among others are involved in these datacenter cybersecurity processes. While this solution is feasible for a few server farms, it can be prohibitively expensive for millions of EVSE that are eventually needed across a wide geographical footprint. And even with costly security, cloud aggregators / server farms can still be vulnerable, and newspapers often report on breaches found by major institutions.

The security complexity of a three-party system is evidential in the ISO 15118 / plug and charge system where the valuable data is exchanged from the EV to the EVSE to the grid using two protocols that need to be translated at the EVSE. There is a point of entry for an MitM attack at the EVSE when the EVSE decrypts signals from the EV and re-encrypts those signals (into a different protocol) to be sent out. This problem exists for both payment data, where customer financial information can be breached, and grid signals because both types of data are decrypted and re-encrypted at the EVSE. When the information is decrypted, it may be subject to an MitM attack by insertion of malicious code, tampering of data, or misuse of the information, potentially by a malicious chip or code due to vulnerabilities within processes of the original manufacturer software developer, or installer.[9]

Further, cybersecurity vulnerabilities can possibly exist even with security chips in the EVSE. Using a security module is helpful in a two-party system. For example, encrypting data between the EVSE and the EV or between the EVSE and the payment system or grid operator protects the data on the communication path and ensure the protection of sensitive cryptographic materials. However, in a three-party system, security modules which have not been developed with an adequate hardware architecture which includes a trusted execution environment (TEE) to protect data inside the EVSE when the communication protocol has been decrypted can be subject to MitM. To date, the industry has yet to establish specific hardware security standards and use cases for these security modules. Furthermore, security modules are also subject to the same supply-chain vulnerabilities as with any other system hardware. This is where parties in the supply chain (e.g., non-trusted original equipment chip manufacturers, software developers, installers, repair people or other parties) may be subject to threat agents who establish malicious access and footholds even before the EVSE is operational.[10]

Cybersecurity recommendations for the CEC to address

In general, we believe that cybersecurity is an addressable problem. System architectures or manufacturers, developers and installers that don't meet current standards can improve. For example, a protocol can be made routable creating a two-party system rather than a three-party

[9] An EVSE could have code inserted by a hacker, an employee, or during a software upgrade that collects all the EV information decoded into the open (from the ISO 15118 decryption) and forwards it to an undisclosed server. That information could be used by other EVs to obtain energy or avoid payment by using the stolen identity. A real-life example are the Target and Solar Winds attacks mentioned previously.

[10] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

system. Any CEC regulation or incentive program that touches the VGI and payment communications between the EV and grid or EV and the payment processor should be designed at the start to be physically and cyber secure, and this applies to much more than the ISO 15118 staff proposal.

We recommend that the CEC should conduct a systemic cyber security review. As part of this, the CEC should conduct a detailed cybersecurity workshop looking at both two-party and three-party systems and the various approaches that can be used to address the various physical and cyber security threats. Recommended expert entities to speak at such a workshop include:

- SCE has a new detailed cybersecurity plan for EVSE that was submitted to the CPUC that we believe is a nation leading example.
- A detailed presentation on MitM and EVSE was presented publicly to many utilities, agencies, automakers and other stakeholders in December 2021[11]
- Representation from the Payment Card Industry and/or CARB on PCI security standards for Apple, Google, and Samsung Pay or other methods allowed by CARB's EVSE payment regulation
- Representation from other state agencies, NIST, and USDOE.
- EPRI has a presentation on its work on EVSE cybersecurity for USDOE and, in a few weeks, will publicly release its new EVSE cybersecurity assessment tool requested by USDOE.
- Other industry experts including standards development organizations.

NIST, part of the US Department of Commerce, was directed to improve cybersecurity for critical infrastructure by a Presidential Executive Order.[12] Standards that cybersecurity industry experts recommend include NIST SP-800-161,[13] NIST IR 7629 Revision 1 paragraph 6.5.1, and NIST SP-800-53. A cybersecurity expert review and accompanying workshop would be able to identify a complete package of recommendations, not only on ISO 15118 but other pathways for VGI and payment communications and help the CEC in its many endeavors.

EPRI would like to conclude with the emphasis on the concept of *Due Care & Due Diligence,*[14]where *due care* is performing the most prudent actions to meet known industry cybersecurity best practices and standards and *due diligence* is gathering all the necessary information so that the best decision-making activities can take place. The concept of due care & due diligence is a cybersecurity (CISSP) ethical responsibility akin to the Hippocratic oath for medical professionals.

It can be argued that the selection of a particular protocol for one part of the EV Charging Ecosystem without the understanding and analysis of the wider implications it has for other systems and stakeholders (e.g., the grid, customers, EV owners) may be considered a failure to exercise *due diligence* for the following reasons:

[11] At SCE's Vehicle-to-Grid Technical Advisory Board call in December 2021.

[12] For more information https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics.

[13] The National Institute of Standards and Technology (NIST), part of the US Department of Commerce, was directed to improve cybersecurity for critical infrastructure by a Presidential Executive Order. See here for more information https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics.

[14] (https://resources.infosecinstitute.com/certification/due-care-vs-due-diligence-cissp/)

- EPRI's recently completed DoE sponsored research (DE-EE0008452)[15] has identified a multitude of cyber security risk & consequence scenarios that have grid reliability, data privacy, and safety implications. The recommendation from this effort was to ensure adequate mitigation against the identified security issues through key architectural, protocol, and technology decisions that are thoroughly vetted and designed appropriately in conjunction with appropriately designed and implemented cybersecurity certification processes that guide successful implementations.
- CEC, under EPIC 16-079, sponsored research to perform cybersecurity evaluation of IEEE 2030.5[16], but not all protocol candidates for EVSE, including ISO 15118, have undergone the same independent security evaluation with the same metrics. The same security testing, performed against all candidate protocols, would ensure that the best-of-breed protocol is selected.
- Regarding MiTM attacks, any protocol translation likely requires decryption, potential exposing data for exfiltration and tampering and overall is a break in the chain-of-trust. Multiple protocols likely mean multiple PKI ecosystems[17], potentially introducing significant management overhead for all stakeholder to comply with more than one set of PKI requirements. This also introduces complexity from an incident response standpoint – if a set of certificates have to be revoked for a fleet of EVSEs, there is no guarantee that all stakeholders will be informed across a multiple PKI ecosystem.
- Finally, EPRI emphasizes the need for secure-by-design and also the major cost ramifications for "rip-and-replace". As we've seen in the telecom industry, the FCC had to invest $1.9B to Huawei/ZTE equipment due to the national security risks expressed by the security intelligence community[18], meaning this is a major concern, only to be exacerbated as the EV charging infrastructure across light, medium, and heavy-duty segments proliferates exponentially in the coming decade. The time to safeguard its cybersecurity is now.

Concerns regarding lack of harmonization of ISO and SAE standards on VGI and payment

In the US, EVSE are built to be compliant with SAE J1772 (*SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler*) which includes both AC only and combined coupler system standards. EPRI would like to express concern for CEC's proposal to mix use of SAE and IEC/ISO standards where those standards were not co-developed. As is detailed following, harmonization efforts between SAE and IEC/ISO are active, but this may not be as effective or the same as the co-development of documents as has been done, for example, with DC charging between SAE J1772 and SAE J2847/2 (*Communication Between Plug-in Vehicles and Off-Board DC Chargers*). While all of the issues below can be addressed and harmonized, there is uncertainty that the SAE and ISO standards can be harmonized in the timeframe that the CEC staff envisions in the staff proposal posted and presented on November 10.

Below are examples of some our specific concerns:

- The SAE J1772 document makes no reference to ISO 15118.

[15] https://www.energy.gov/sites/default/files/2021-06/elt206_chhaya-ghatikar_2021_o_5-20_1258pm_LR_TM.pdf

[16] https://www.epri.com/research/products/000000003002019255

[17] Exploring the Public Key Infrastructure in the ISO15118 ecosystem, ELAAD NL, 2018, https://www.elaad.nl/uploads/files/Exploring_the_PKI_for_ISO_15118_in_the_EV_charging_ecoystem_V1.0s2.pdf, Figure 6, page 34, accessed on December 10, 2021

[18] https://www.cnbc.com/2021/07/13/fcc-finalizes-program-to-rip-and-replace-huawei-zte-equipment-in-us.html

  - Normative references in SAE J1772 for digital communications are to SAE J2847/1 (*Communication for Smart Charging of Plug-in Electric Vehicles using Smart Energy Profile 2.0*) for AC Charging, and SAE J2847/2 for DC charging.
  - There is no active effort underway to tightly align SAE J1772 with ISO 15118 requirements. Failure to carefully review and ensure alignment leaves open potential interoperability issues.
- SAE J2847/1 and SAE J2847/3 (*Communication for Plug-in Vehicles as a Distributed Energy Resource*s) are based on IEEE 2030.5 (the smart energy profile). This is better aligned with the requirements of California Rule 21 in comparison to ISO 15118 particularly for support of export of AC power from an electric vehicle.
- Considerable work has been done and is being done on SAE J3072 (*Interconnection Requirements for Onboard, Utility-Interactive, Inverter Systems*) supporting SAE J2847/1, SAE J2847/3 and IEEE 1547 requirements to allow for AC power export from an electric vehicle in compliance with California Rule 21 requirements. ISO 15118 does not have proper support for AC vehicle to grid operation under Rule 21.
- CEC's proposal reads: "AC chargers must continue supporting pulse-width modulation control using IEC 61851 …". The normative behavior of the pilot signal (pulse-width modulation control) for SAE J1772 is contained in that document with no reference to IEC 61851 or any other external document.
- The timing and operation of the use of digital communications for AC charging has not been fully detailed in SAE J1772. This relates to how a charge station would transition from attempting digital communication to reverting back to use of the pilot PWM to determine charging behavior. This should be addressed to confirm interoperability for digital communications in support of AC charging. This need is independent of the selected protocol (SAE J2847/1 or ISO 15118-2 or ISO 15118-20).
- Continuous efforts to harmonize SAE documents with ISO 15118 and IEC related standards have been undertaken, but they are always a work in progress due to document update cycles. Specifying documents vaguely (like ISO 15118 or J1772) without specifying which specific document for IEC and ISO (dash number) and what version for IEC, ISO and SAE (either by date or edition) may lead to implementation and interoperability issues.
- After publication of ISO 15118-20 it is anticipated that ISO will turn attention to updating ISO 15118-2. Should CEC enforce use of the ISO documents, effort will be needed to ensure SAE J1772 remains aligned and interoperable with these updates.
- It was implied that all DC charging implementations used today are built on ISO 15118. That statement is incorrect. The underlying operation of DC charging is built on DIN 70121 which was used as the basis for SAE J2847/2 and ISO 15118-2. DIN 70121 has been updated more recently than ISO 15118-2. The SAE J2847/2 implementation has remained better aligned with DIN 70121 due to more frequent updates being implemented for SAE J2847/2. Through active harmonization efforts between SAE and DIN, DC chargers and electric vehicles that use SAE J2847/2 or DIN 70121 should work interchangeably. SAE J2847/2 is not harmonized with ISO 15118-2 Plug-and-Charge.

Thank you for the opportunity to share our expertise. If you have any questions, please do not hesitate to contact either Mark Duvall or Matt Wakefield at the contact numbers listed below.

Sincerely,

Matt Wakefield

Matt Wakefield
Director, Research and Development
ICCS
EPRI
mwakefield@epri.com
Office: (865) 218-8087

MDuvall

Mark Duvall
Director, Research and Development
Electrification & Customer Solutions
EPRI
mduvall@epri.com
Office: (650) 855-2152