Wicked Problem, Parsimonious Solution: Securing Electric Vehicle Charging Station Software

Emma Sheppard*†, Zachary Wadhams*, Dalton Arford†, Clemente Izurieta*†‡, and Ann Marie Reinhold*†

*Montana State University, Bozeman MT, USA
†Pacific Northwest National Laboratory, Richland WA, USA
‡Idaho National Laboratory, Idaho Falls ID, USA

***Abstract*—Electric vehicle charging infrastructure presents a suite of novel cyber-physical threats. Among this infrastructure, charging stations are the most vulnerable elements. The software in the charging station supply equipment is particularly vulnerable. Currently, the software is an attack surface that is largely unprotected and poorly characterized. To represent the vulnerabilities in this attack surface, we advocate for applying modern software quality assurance to characterize vulnerabilities in electric vehicle charging station software. Specifically, we advocate for the application of hierarchical software quality assurance (HSQA) to specialized electric vehicle charging station software. HSQA provides a comprehensive view of the code quality and security — from the level of individual vulnerabilities (e.g., CVEs) to high level characteristics (e.g., CIA Triad). HSQA incorporates quality and security considerations throughout the software development lifecycle. Thus, our position is that HSQA is an excellent approach for assessing electrical vehicle charging station software.**

***Index Terms*—electric vehicle, cyber-physical system, software quality, cybersecurity, charging station, power grid**

I. Introduction

Worldwide, there is a growing demand for carbon-neutral technology, with many nations moving towards the adoption of zero-emissions vehicles [1]–[4]. Consequently, electric vehicle charging infrastructure (EVCI) is rapidly growing. EVCI refers to every component required to charge an electric vehicle (EV), including the charging station (EVCS), the power supply equipment (EVSE) within the charging station, the cloud-based charging station management systems (CSMS), the power grid or operator, and the payment and authorization mechanisms [5].

EVCI creates a nexus between the EV, the cloud, and the power grid. Thus, EVCI is a complex system that qualifies as both an Industrial Internet of Things (IIOT) device and operational technology (OT), and incorporates components of industrial automation and control systems (IACS), as well as distributed energy resources (DER) [5].

Public EVCI (i.e., commercial charge points) supports the growing EV market by providing accessibility to both rural and urban areas, alleviating range anxiety and encouraging the adoption of EVs [4], [6]. The push for the public adoption of EVs will require substantial investments in public EVCI to support the growing EV market [7], [8]. This expansion of public EVCI will introduce myriad logistical challenges, such as access and reliability, and security concerns, including cybersecurity threats.

II. The Attack Surface of EVCI

As the demand for EVs has increased—and continues to increase—around the globe, manufacturers are increasing public access to EVCI. With increasing access comes an expanding attack surface[1]. This attack surface is concerning to cybersecurity researchers and original equipment manufacturers (OEMs) alike, as EVCS equipment is public facing by necessity. The attack surface of EVCI is expansive and highly varied across charging stations—depending upon the combinations of proprietary and open-source software, hardware, and protocols within the infrastructure [9]. Existing attempts to characterize this attack surface are limited. No one study encompasses every component of every EVCS due to the variation in hardware and software in use.

An EVCS contains one or more EVSEs. The EVSE is the most vulnerable element of the infrastructure because it is public facing and central to the transmission of data and power. The EVSE is the hub for the exchange of information between the EV, the EV user, the third-party application providers, the OEM, the charge point operator (CPO), and the grid operator [10]. Thus, threat modeling of the attack surface in EVCI should include a comprehensive assessment of the EVSE [10], [11].

EVSEs are sophisticated cyber-physical systems (CPS) that leverage interconnected technologies, enabling them to manage the flow of electricity from the grid to the vehicle and facilitate data exchange between users and monitoring or management systems. Given its crucial role in the core functionality of EVCI, securing the EVSE is paramount to ensuring the security of the entire infrastructure.

The attack surface of EVSEs can be broken into two categories: a physical surface, composed of hardware, and a digital surface, driven by software. With the automotive industry moving towards “software-defined vehicles,” protecting the digital attack surface is crucial [12]. Software governs key interdependent functionalities of the EVSE, making it a prime target for adversarial attacks [13]. By focusing on the software

[1] https://www.fortinet.com/resources/cyberglossary/attack-surface

that drives the EVSE, attacks can be mitigated across its interfaces. Identifying and improving software quality and security characteristics are critical for reducing the exploitability of EVCI.

Here, we explore a novel integration and assessment of EVSE software quality and security characteristics using a tried-and-true software quality assurance approach.

A. Prior Work

1) Four-Interface Threat Model: The attack surface of the EVSE can be categorized into four interfaces: EV-to-EVSE, EV operator, EVSE internet, and EVSE maintenance [10]. Each of these four interfaces are explored below.

Interface 1: The EV-to-EVSE interface is the EVSE coupling cable. This cable physically connects the EV to the EVSE for power exchange. This interface is not standardized. EVSE couplers vary in power level, power type, and underlying communication protocols, resulting in a vulnerable heterogeneous infrastructure. Vulnerabilities in this interface include malware exchange from EV to EVSE [14], charging disruptions [15], [16], privilege escalation within Vehicle-to-Grid communications [17], and security concerns with the ISO 15118 EV-to-EVSE communication protocol [18]–[21].

Interface 2: The EV operator interface authenticates charging sessions using methods like Radio Frequency Identification (RFID) tags, smartphone Near Field Communication (NFC), and credit card swipes to link the operator's billing information to the charging station. Vulnerabilities in the EV operator interface include RFID cloning [22], [23], authorization bypass mechanisms [23], and reverse-engineering of third-party applications to gain access to EVSE management portals [24]. Note that ISO 15118-20[2] recommends public key infrastructure (PKI) encryption to mitigate this attack vector [25].

Interface 3: The EVSE internet interface encompasses any vulnerability that may occur due to EVSE connection to internet services. EVSEs are required to maintain internet connectivity to transmit telemetry data, allow access for third-party management systems, and enable grid operators to access EVSE equipment [10]. EVSE communication protocols tend to be proprietary, but open-source protocols exist.

Open Charge Point Protocol (OCPP) is a common open-source protocol used for communication between the EVSE and its CSMS [26]. A benefit of current OCPP versions (2.1 and 2.0.1) is the inclusion of PKI encryption and ISO 15118 plug-and-charge functionality. However, OCPP 1.6 is more commonly used in public charging stations [27]. This older version of OCPP lacks PKI encryption and requires the use of Virtual Private Networks (VPNs) to protect the EVSE from man-in-the-middle (MITM) attacks and energy theft [28].

Attacks on this interface can target EVSE vendors, grid operator systems, and the EV [10]. Documented exploits include targeting OCPP attack vectors [23], [28], [29], intercepting billing communications [22], and detecting EVSEs on the public internet [30], [31]. Remote communications with an EVSE can allow an attacker to gain remote access to other EVSEs [32].

Interface 4: The EVSE maintenance interface is the physical, outward-facing hardware. Communications in the maintenance interface circuit boards generally occur over ethernet or serial analog and are often unencrypted [33]. Ethernet switches can be accessed if the lid to the EVSE is removed, and communications amongst components can be monitored using an ethernet cable. Outside the lid, physical ports are often left unprotected to allow vendors to monitor, update, and debug components within the EVSE, resulting in an easily exploitable attack vector. Moreover, the maintenance interface includes locally hosted web servers through which adversaries can gain access to personally identifiable information (PII) [34]. Additional hazards include unsigned firmware [24] and hard-coded credentials [35], [36].

2) CharIN EVSE Threat Model: Charging Interface Initiative e.V. (CharIN) released the most current and comprehensive characterization of the EVSE attack surface [11], enumerating several attack vectors and threat scenarios. The CharIN EVSE model includes a mapping of each scenario to the Microsoft STRIDE threat model[3] and recommends mitigations and best practices. Referenced frameworks, standards, and protocols include ISA/IEC 62443 Cybersecurity for ICAS[4], MITRE ATT&CK Framework[5], ISO 15118-2[6] and ISO 15118-20[7], OCPP[8], and ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering[9].

3) Integrating Known Threat Models for Comprehensive EVCI Security: The Four-Interface [10] and CharIN EVSE threat models [11] highlight the criticality of both software and hardware components within the EVSE. Both threat models are applicable to EVSE components across OEMs. Here, we take a position that incorporates findings from both models, addresses exploitable attack vectors, and is adaptive to emerging threats and vendor-dependent components.

III. Our Position on Securing EVSE Software

Utilizing secure-by-design principles [37], we advocate for an approach that incorporates security considerations throughout the software development lifecycle. Historically, charging stations and their software have been constructed with a "build-and-forget" mentality [11]. These practices require practitioners to shoulder the burden of maintaining externally developed software [37].

More recently, cybersecurity agencies are urging manufacturers to assume full responsibility for their software [37]. Technical experts are moving toward standardizing cybersecurity practices throughout an EVSE rather than inheriting se-

[2] https://www.iso.org/standard/77845.html

[3] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[4] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[5] https://attack.mitre.org/matrices/ics/

[6] https://www.iso.org/standard/55366.html

[7] https://www.iso.org/standard/77845.html

[8] https://openchargealliance.org/protocols/open-charge-point-protocol/

[9] https://www.sae.org/standards/content/iso/sae21434/

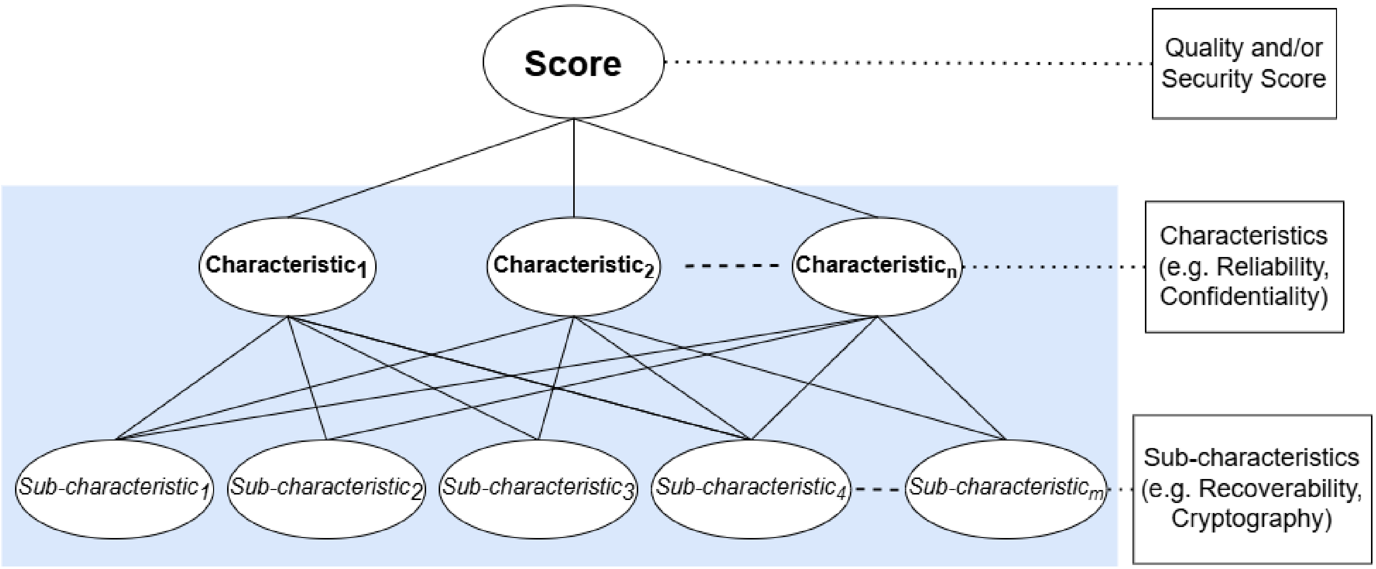

Fig. 1: A conceptual view of the upper-level architecture of an HSQA model. Includes the overall quality and/or security score, high-level characteristics, and their sub-characteristics. For more examples, see Tables I, II, and III.

curity measures from individual vendor components [11]. For instance, CharIN is pushing for EVSE software components to be secure-by-design [11]. This change from "build-and-forget" to secure-by-design is a shift from a reactive to a proactive security posture.

A proactive security posture requires protecting EVSE software. Protecting EVSE software can be achieved through quality and security evaluation methods, such as software quality assurance (SQA). SQA models—and specifically, hierarchical SQA models (HSQA)—enable the identification, prioritization, and mitigation of security issues [38]. HSQA modeling answers the calls by the U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency (DHS CISA) and CharIN for incorporation of secure-by-design principles [39], [40]. Our position is that HSQA is a promising avenue to evaluate the quality and security of EVSE software. In the following subsections, we advocate for rigorous assessment of software quality and security using HSQA to promote a more secure and resilient EVSE.

A. Quality Modeling for Software Components in the EVSE

We propose HSQA to promote the quality and security of EVSE software. We incorporate existing work in IIOT, IACS, DER, OT, and the automotive industry (e.g., ISO/IEC 33000[10] and SPICE [41]) into HSQA. HSQA allows for the generalization of quality in EVSE software.

HSQA has been employed successfully for over a decade [42], [43]. Initially, these models operationalized ISO/IEC 9126:2001[11], the precursor to ISO/IEC 25010:2011 and ISO/IEC 25010:2023[12]. The modern approach to HSQA is the Platform for Investigative software Quality Understanding and Evaluation (PIQUE) [40]. PIQUE is domain-agnostic, allowing efficient application across various software-dependent systems, including EVSE.

HSQA evaluates and scores software utilizing outputs from static analysis tools. These outputs are aggregated into increasingly abstract concepts; for example, from raw counts of CVEs[13] to high level characteristics in ISO/IEC standards [40], [44]. HSQA enables stakeholders to make informed decisions regarding software quality and security, supporting risk analysis by organizing potential software-level vulnerabilities across multiple levels of abstraction.

HSQA models are customizable by design. This customizability is an advantage because EVSE software is necessarily diverse. Diverse software is analyzed by diverse static analysis tools; e.g., C# code must be analyzed with different static analysis tools than C++ code. Yet, the information garnered from diverse tools can be integrated into HSQA models with minimal effort.

The diverse software within EVSE operate in concert and thus should not be considered in isolation. HSQA enables a single solution that can evaluate and score each software component contemporaneously. In so doing, HSQA provides a means for assessing the quality and security posture of the EVSE as a system.

Integrated assessments of software quality and security require identifying high-level quality and security characteristics specific to an EVSE. Integration is achieved by merging software quality standards (e.g., ISO/IEC 25010:2023) with EVSE cybersecurity research, standards, and best practices (e.g., [5], [45]–[50]). HSQA facilitates this merging by design (Fig. 1).

[10] https://committee.iso.org/sites/jtc1sc7/home/projects/flagship-standards/isoiec-33000-family.html

[11] https://www.iso.org/standard/22749.html

[12] https://www.iso.org/standard/78176.html

[13] https://cve.mitre.org/

Our position is: ***HSQA is an excellent approach for the assessment of EVSE software.*** *This novel application of a tried-and-true solution will increase the quality and security posture of EVSE.*

B. Counterarguments

Counterarguments to this position may include alternate ways to satisfy secure-by-design principles or evaluate the quality of EVSE software. Quality assurance and secure-by-design best practices include the use of memory-safe programming languages, vulnerability disclosures, static and dynamic application security testing (SAST/DAST), and code review for quality assurance [37]. Any implementation of these best practices aids in securing software. However, these approaches are independent and therefore do not provide a holistic perspective on software quality and security.

In contrast, HSQA leverages existing vulnerability disclosures and static analysis tools to score the quality and security of software holistically. HSQA modeling can implement published CVEs, CWEs[14], code review, and SAST/DAST. Currently, outputs from static analysis tools are the inputs to HSQA models [40]. HSQA offers a practical and scalable approach for integrating such information at multiple levels of abstraction–meeting the needs of developers and the C-Suite alike [40].

IV. Quality & Security Characteristics for EVSE

The novel application of HSQA to EVSE requires the integration of high-level quality and security characteristics from diverse sources. We propose the integration of three foundational pillars: (*I*) the ISO/IEC 25010:2023 software product quality model [51]; (*II*) the *Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report* (herein K. Harnett et al.) prepared by the U.S. Department of Transportation (DoT) Volpe Center [48]; and (*III*) cybersecurity standards relevant to power electronics delivery equipment, industrial control systems (ICS), and road vehicles, including ISA/IEC 62443 [46], IEEE 1547-3 [52], and ISO/SAE 21434:2021 [47]. Furthermore, we draw on the methods outlined in Karnouskos et al. [53] to define the ISO/IEC 25010:2023 software quality characteristics and sub-characteristics in the context of ICS and EVSE. The following proposed high-level quality and security characteristics would be implemented in a similar architecture to Fig 1.

A. Pillar I: Software Quality Standards

The ISO/IEC 25000 suite of standards provides a comprehensive framework for evaluating software product quality, with ISO/IEC 25010 – System and software quality models serving as a key component of the ISO/IEC 2501n standards for Quality Model Division[15]. ISO/IEC 25010:2023 specifies nine high-level characteristics that are essential for assessing software quality: functional suitability, performance efficiency, compatibility, interaction capability, reliability, security, maintainability, flexibility, and safety [51]. Table I outlines these high-level characteristics, their sub-characteristics, and their proposed applications to EVSE software. Definitions exactly as written in the ISO/IEC 25010:2023 Systems and software engineering (SQuaRE) Product quality model can be found in the full archived table[16].

B. Pillar II: Cybersecurity Best Practices for EVSE

K. Harnett et al. and the U.S. Naval Facilities Engineering Systems Command prepared the most current EVSE best practices for cybersecurity [48]. These best practices are based on interviews with subject matter experts, the ElaadNL-commissioned European Network for Cyber Security (ENCS) *EV Charging System Security Requirements* [56], and the U.S. National Motor Freight Traffic Association cybersecurity reports for medium and heavy-duty EVs [57]. The best practices align with the Microsoft STRIDE Threat Model, which categorizes common cyber threats and maps them to security characteristics [58], [59].

All of the STRIDE properties are important for evaluating EVSE software (i.e., authenticity, integrity, non-repudiation, confidentiality, availability, and authorization). We use the STRIDE properties as our characteristics. The following sub-characteristics are also important (Table II): design, cryptography, communication, hardening, resiliency, secure operation, logging, assurance, lifecycle and governance, and EVSE operator/utility operator communications.

C. Pillar III: Cybersecurity Standards for Road Vehicles, Industrial Automation and Control Systems, and Power Delivery Electronics

Cybersecurity standards relevant to road vehicles, industrial automation and control systems, and power delivery electronics are also important considerations for EVSE software.

Road vehicles.—The standard for road vehicle cybersecurity, ISO/SAE 21434:2021, specifies requirements for threat modeling and recommends the Microsoft STRIDE Threat Model, as well as alternate frameworks: EVITA[17], TVRA[18], and PASTA[19]. We utilize STRIDE (as opposed to EVITA, TVRA, and PASTA) because STRIDE enables parsimony across Pillars II and III and simplifies the process of mapping threat scenarios to high-level security characteristics.

Industrial automation & control systems.—The series of industrial automation and control standards governing security, ISA/IEC 62443, aligns with the confidentiality, integrity, and availability (CIA) Triad[20]. The CIA triad are thus the characteristics we employ. The sub-characteristics from ISA/IEC 62443 are highlighted in Table III.

[14] https://cwe.mitre.org/

[15] https://iso25000.com/index.php/en/iso-25000-standards/51-iso-iec-2501n

[16] https://doi.org/10.5281/zenodo.14758339

[17] https://doi.org/10.5281/zenodo.1188418

[18] https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

[19] https://threat-modeling.com/pasta-threat-modeling/

[20] https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

TABLE I: ISO/IEC 25010:2023 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model characteristics (bolded), sub-characteristics (italicized), and their proposed applications to EVSE software.

Characteristic & ***Sub-characteristics***	**Application to EVSE Software**
Functional Suitability *Functional completeness, correctness, appropriateness*	Ensures charging stations perform as expected to meet EV user needs, enhancing satisfaction and confidence in charging infrastructure.
Performance Efficiency *Time behavior, resource utilization, capacity*	Impacts the speed of vehicle charging and energy efficiency, directly affecting EV users, management system operators, and power grid load.
Compatibility *Co-existence, interoperability*	Enables communication between charging stations, EVs, the grid, and third-party applications via the cloud.
Interaction Capability *Appropriateness recognizability, learnability, operability, user error protection, user engagement, inclusivity, user assistance, self-descriptiveness*	Aids users in navigating the charging process, including use of the human-machine interface (HMI), the authentication process, and the physical interaction of charging a vehicle.
Reliability *Faultlessness, availability, fault tolerance, recoverability*	Minimizes downtime and enables fast recovery after service disruptions, ensuring continuous charging operations.
Security *Confidentiality, integrity, non-repudiation, accountability, authenticity, resistance*	Protects user data and EVSE networks, preventing malicious attacks that may compromise charging infrastructure [11], [48].
Maintainability *Modularity, reusability, analysability, modifiability, testability*	Facilitates efficient software updates and improvements, accommodating new technologies and security measures.
Flexibility *Adaptability, scalability, installability, replaceability*	Allows charging infrastructure to evolve with technological and regulatory changes, enabling compliance with new standards, i.e. NACS SAE J3400 [54], [55].
Safety *Operational constraints, risk identification, fail safe, hazard warning, safe integration*	Protects users and infrastructure from hazards like cable melting, fires, and electrical shocks, enhancing public confidence in EV adoption [45].

TABLE II: Security sub-characteristics from K. Harnett et al. [48], the corresponding requirement from the ElaadNL-commissioned ENCS *EV Charging Systems Security Requirements* [56], and their descriptions.

K. Harnett et al. Security Sub-characteristic	**ENCS Requirement**	**ENCS Description** †
Design	Future Proof Design	Prevents lack of capabilities for future security updates.
Cryptography	Cryptographic Algorithms and Protocols	Describes cryptographic algorithms, key lengths, and pseudo-random generators allowed for use.
Communication	Communication Security	Defines implementation mechanisms for end-to-end security in an EVCS.
Hardening	System Hardening	Provides hardening mechanisms for the EVCS components.
Resiliency	Resilience	Prevents issues due to misuse of the EVCS components or communication interfaces.
Secure Operation	Access Control	Defines authorization mechanisms for the EVCS components or its communication interfaces.
Logging	Logging	Defines detection mechanisms to identify security issues on an EVCS component or its communication interfaces.
Assurance	Assurance	Specifies measures vendors must take to ensure secure functioning of EVCS components.
Lifecycle and Governance	Product Lifecycle and Governance	Defines processes for secure development, manufacturing, and provisioning of EVCS components.
EVSE Operator/Utility Operator Communications	CPO and DSO Communication	Requirements for secure communications between Charge Point Operators (CPOs) and Distribution System Operators (DSOs). Useful for new server procurement or setup.

† Descriptions have been paraphrased and condensed for readability. Exact descriptions can be found in Section 1.4 of [56].

Power delivery electronics.—The cybersecurity standard relevant to power delivery electronics is the IEEE 1547-3 Guide for Cybersecurity of DERs Interconnected with Electric Power Systems. This standard combines multiple resources to define cybersecurity characteristics, including ISA/IEC 62443 [46], the NIST Cybersecurity Framework [5], the DHS US-CERT Cyber Security Evaluation Tool [60], the MITRE ATT&CK Framework, and the U.S. National Renewable Energy Laboratory DER Cybersecurity Framework [61].

Section 4.4.4.1 of IEEE 1547-3 lists many security requirements applicable to EVSE. We operationalize these requirements as HSQA characteristics (Fig. 1). This IEEE 1547-3 standard primarily utilizes the CIA Triad to map common cyberattacks to security characteristics, but includes additional important characteristics and a sub-characteristic outside of the CIA triad (Table III); the sub-characteristic of note is cryptography. The other sub-characteristics relevant to power delivery electronics are defined in ISA/IEC 62443 [49] (Table III).

TABLE III: Security frameworks (italicized), high-level characteristics (bolded), sub-characteristics (italicized), and their definitions from ISO/SAE 21434:2021, ISA/IEC 62443, and IEEE 1547-3.

Standard & *Security Framework*	**Security Characteristic/** ***Sub-characteristic***	**Definition**
ISO/SAE 21434:2021 Road Vehicles – Cybersecurity engineering *Microsoft STRIDE Threat Model*	See [59]	See [58], [59]
ISA/IEC 62443 Security for Industrial Automation and Control Systems *CIA Triad*	**Confidentiality**	Prevents unauthorized access to sensitive information.
	Integrity	Ensures the accuracy and consistency of data and system operations.
	Availability	Ensures systems function as intended without disruption over time.
	Access Control	Restricts access to devices or information to authorized users only.
	Use Control	Limits the usage of devices or data to authorized operations.
	Data Integrity	Protects communication channels from unauthorized changes to data.
	Data Confidentiality	Secures data from unauthorized access during transmission.
	Restrict Data Flow	Controls data flow to prevent exposure to unauthorized entities.
	Timely Response to Event	Ensures prompt responses to security incidents with appropriate actions.
	Resource Availability	Guarantees resources remain accessible despite potential attacks.
IEEE 1547-3 Guide for Cybersecurity of DERs Interconnected with Electric Power Systems *CIA Triad*	**Confidentiality**	Protects information from unauthorized disclosure.
	Integrity	Prevents and detects unauthorized data modification.
	Availability	Ensures systems remain operational and reliable.
	Accountability	Links actions to responsible entities for traceability.
	Authentication	Confirms the identity of communication participants.
	Authorization	Defines user permissions for data access and operations.
	Non-repudiation	Provides proof of origin for actions or commands.
	Cryptography	Uses algorithms to secure data via encryption and hashing.

† Definitions have been paraphrased and condensed for readability. Exact definitions can be found in their respective standards.

V. Developing HSQA Models from Quality & Security Characteristics

Our current research operationalizes HSQA using the quality and security characteristics described in Section 4. Developing these HSQA models for EVSE requires extending our HSQA meta-model and specifying the characteristics as "quality/security aspects" and the sub-characteristics as "product factors" [40]. However, because HSQA is a tried and true technology with an extensible meta-model, the time from model concept to minimum viable product has been short.

Operationalizing characteristics and sub-characteristics into an HSQA model is trivial. The challenge lies in ensuring the "right" characteristics and sub-characteristics are selected for inclusion in the HSQA models for EVSE software. As EVSE is relatively new, inherently complex, and a technology that operates at the nexus of multiple critical infrastructures, the characteristics and sub-characteristics identified above will almost certainly require refinement. We anticipate this refinement to be our greatest challenge. However, this challenge is one we have addressed in other domains.

Our current work targets source and compiled code in EVSEs. Because the inputs to these HSQA models are the outputs of static analysis tools, an important consideration is that models can only aggregate results for measurable characteristics. Thus, it is imperative to find static analysis tools that have the content coverage for EVSE software; if such tools are not available, tooling is a threat to the internal and content validity of HSQA outputs. These threats to validity are concerns for EVSE HSQA models because tooling that is specific to EVSE infrastructure is of limited availability. In the absence of EVSE-specific tools, we are utilizing generic tools, including SonarQube[21] for source code and CVE Binary Tool[22] for compiled code.

VI. Discussion

HSQA models for EVSE software build upon the foundation laid by the Four-Interface [10] and CharIN EVSE threat models [11]. Our work incorporates these findings and provides the foundation for integrating them into deployable HSQA models. These HSQA models consider the identification, risk, and interdependencies of vulnerabilities to EVSE software and provide a means for evaluation throughout the software development lifecycle. HSQA thus advances the evaluation of software quality and security in EVSEs.

Our position acknowledges that EVSE software quality and security are not mutually exclusive. Rather, quality and security are interrelated, and are best addressed as such. Integrating software quality characteristics with EVSE cybersecurity characteristics enhances the overall security posture of EVSEs by directly measuring attack vectors to one of the most vulnerable digital attack surfaces in EVCI.

Unlike traditional power grid and quality-of-service evaluations of EVSEs, which focus on external impacts and operational performance, HSQA delves into the integrity and robustness of the internal software components. HSQA measures code quality and security, thereby providing a holistic assessment of interdependent, complex cyber-physical software systems.

In conclusion, we return to our position that HSQA is an excellent approach for the assessment of EVSE software. As EVSEs are a prime target and comprise a large and growing attack surface, cybersecurity solutions are needed. Here, our

[21] https://www.sonarsource.com/products/sonarqube/

[22] https://github.com/intel/cve-bin-tool

position includes a solution that is secure-by-design, tried-and-true, and comprehensive. HSQA will increase the quality and security posture of EVSE by offering a parsimonious solution for mitigating a wicked problem.

Acknowledgments

This research was conducted with support from the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Department of Energy (DOE) Pacific Northwest National Laboratory (PNNL) under contract IAA# 70RSAT24KPM000022. Any opinions contained herein are those of the author and do not necessarily reflect those of DHS S&T or DOE PNNL.

The PNNL AI Incubator Large Language Model was used in this document for spell-checking and grammatical enhancements.

References

[1] The White House, "Fact sheet: President biden announces steps to drive american leadership forward on clean cars and trucks," 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/05/fact-sheet-president-biden-announces-steps-to-drive-american-leadership-forward-on-clean-cars-and-trucks

[2] ——, "Executive order on catalyzing clean energy industries and jobs through federal sustainability," 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/08/executive-order-on-catalyzing-clean-energy-industries-and-jobs-through-federal-sustainability/

[3] California Air Resources Board, "California air resources board: Zero-emission vehicle program," n.d. [Online]. Available: https://ww2.arb.ca.gov/our-work/programs/zero-emission-vehicle-program/about

[4] European Parliament, "Eu ban on the sale of new petrol and diesel cars from 2035 explained: Topics: European parliament," Mar. 2022. [Online]. Available: https://www.europarl.europa.eu/topics/en/article/20221019STO44572/eu-ban-on-sale-of-new-petrol-and-diesel-cars-from-2035-explained

[5] J. McCarthy *et al.*, "Cybersecurity framework profile for electric vehicle extreme fast charging infrastructure," Tech. Rep., Oct. 2023.

[6] F. S. Mandolakani and P. A. Singleton, "Electric vehicle charging infrastructure deployment: A discussion of equity and justice theories and accessibility measurement," *Transportation Research Interdisciplinary Perspectives*, vol. 24, p. 101072, Mar. 2024.

[7] Ormazabal. (2023) Europe needs to invest 280 billion euros in electric vehicle charging infrastructure. [Online]. Available: https://www.ormazabal.com/en-gb/europe-needs-to-invest-280-billion-euros-in-electric-vehicle-charging-infrastructure/

[8] US Department of Transportation Federal Highway Administration, "Investing in america: Biden-harris administration announces $635 million in awards to continue expanding zero-emission ev charging and refueling infrastructure," Jan. 2025. [Online]. Available: https://highways.dot.gov/newsroom/investing-america-biden-harris-administration-announces-635-million-awards-ev-charging

[9] S. Mousavi and L. Nash, "Securing electric vehicle supply equipment: Cybersecurity strategies for hyperconnected ecosystems," Oct. 2023, electric vehicle charging industry cybersecurity. [Online]. Available: https://www2.deloitte.com/us/en/pages/consumer-business/articles/electric-vehicle-charging-industry-cybersecurity.html

[10] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," *Energies*, vol. 15, no. 11, p. 3931, May 2022.

[11] M. Sharma *et al.*, "White paper of charging interface initiative e.v." CharIN, Jun. 2024. [Online]. Available: https://www.charin.global/media/pages/technology/knowledge-base/df62b1558e-1650556154/charin_white_paper_connector_test_v5.4.pdf

[12] T. Caldwell, "Council post: The state of cybersecurity of ev charging infrastructure." [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2024/08/30/the-state-of-cybersecurity-of-ev-charging-infrastructure/

[13] D. Strom, "Ev charging stations still riddled with cybersecurity vulnerabilities." [Online]. Available: https://www.darkreading.com/ics-ot-security/ev-charging-stations-still-riddled-with-cybersecurity-vulnerabilities

[14] K. Rohde, "Electric vehicle cyber research," in *Proceedings of the DOE FEMP Energy Exchange*, Tampa, FL, USA, Aug. 2017.

[15] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of ccs electric vehicle charging," *arXiv*, Feb. 2022.

[16] K. Rohde, "A distributed auto charger attack on the grid," in *Proceedings of the S4*, Miami, FL, USA, Apr. 2019.

[17] S. Dudek, "Examining log4j vulnerabilities in connected cars and charging stations," Trend Micro. [Online]. Available: https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html

[18] R. Falk and S. Fries, "Securely connecting electric vehicles to the smart grid," *Intl Journal on Advances in Internet Technology*, vol. 6, 2013.

[19] ——, "Electric vehicle charging infrastructure security considerations and approaches," in *Proceedings of INTERNET*, Jun. 2012, pp. 58–64.

[20] K. Bao, H. Valev, M. Wagner, and H. Schmeck, "A threat analysis of the vehicle-to-grid charging protocol iso 15118," *Computer Science - Research and Development*, vol. 33, no. 1–2, pp. 3–12, Sep. 2017.

[21] S. Lee, Y. Park, H. Lim, and T. Shon, "Study on analysis of security vulnerabilities and countermeasures in iso/iec 15118 based electric vehicle charging technology," in *2014 International Conference on IT Convergence and Security (ICITCS)*. IEEE, Oct. 2014, pp. 1–4.

[22] M. Dalheimer, "Ladeinfrastruktur für elektroautos: Ausbau statt sicherheit (charging infrastructure for electric cars: Expansion instead of security)," in *Proceedings of the 34th Chaos Communication Congress*, Leipzig, Germany, Dec. 2017, pp. 27–30.

[23] A. Friedland, "Security and privacy in the current e-mobility charging infrastructure," in *Proc. of the DeepSec*, vol. 31, Vienna, Austria, 2016.

[24] "Cyber security research and development: Cyber assessment report of level 2 ac powered electric vehicle supply equipment," INL, Tech. Rep. INL/MIS-18-45521, May 2018.

[25] B. Sorokanich, "What is plug & charge?" Capital One Auto Navigator, Oct. 2023. [Online]. Available: https://www.capitalone.com/cars/learn/finding-the-right-car/what-is-plug-charge/2734

[26] Open Charge Alliance, "Open charge point protocol." [Online]. Available: https://openchargealliance.org/protocols/open-charge-point-protocol/

[27] L. R. Saposnik and D. Porat, "Hijacking ev charge points to cause dos," 2023. [Online]. Available: https://www.saiflow.com/blog/hijacking-chargers-identifier-to-cause-dos/

[28] C. Alcaraz, J. Lopez, and S. Wolthusen, "Ocpp protocol: Security threats and challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, Sep. 2017.

[29] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing security in ocpp: Protection against man-in-the-middle attacks," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, Feb. 2018, pp. 1–5.

[30] R. Varriale, R. Crawford, and M. Jaynes, "Risks of electric vehicle supply equipment integration within building energy management system environments: A look at remote attack surface and implications," in *Lecture Notes in Networks and Systems*. Springer International Publishing, Aug. 2021, pp. 163–173.

[31] O. Shezaf, "Who can hack a plug? the infosec risks of charging electric cars," in *Proceedings of the Hack in the Box*, Amsterdam, The Netherlands, 2013, pp. 10–11.

[32] C. Vasquez, "Vulnerabilities could let hackers remotely shut down ev chargers, steal electricity," Feb. 2023. [Online]. Available: https://cyberscoop.com/hack-electric-vehicle-chargers/

[33] B. Anderson and J. Johnson, "Securing vehicle charging infrastructure," in *Proceedings of the 2021 DOE Vehicle Technologies Office Annual Merit Review*, Washington, DC, USA, Jun. 2021, pp. 21–25.

[34] G. Master, "Security of ev & back-end systems (evse)," Aug. 2022. [Online]. Available: https://medium.com/@grand_Master/security-of-ev-back-end-system-evse-ea903f854aeb

[35] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers & Security*, vol. 112, p. 102511, Jan. 2022.

[36] "Schneider electric security notification: Evlink city/parking/smart wallbox charging stations," 2021. [Online]. Available: https://www.se.com/au/en/download/document/SEVD-2021-194-06/

[37] "Shifting the balance of cybersecurity risk: Principles and approaches for security-by-design and -default," Cybersecurity and Infrastructure Security Agency. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

[38] "Software quality assurance - software engineering," GeeksforGeeks. [Online]. Available: https://www.geeksforgeeks.org/software-engineering-software-quality-assurance/

[39] "Cisa: 2023-2027 strategic technology roadmap," Cybersecurity and Infrastructure Security Agency. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/22-1116%20LAYOUT%20-%20STRv5_FINAL_508c.pdf

[40] C. Izurieta, D. Reimanis, E. O'Donoghue, K. Liyanage, A. R. Manzi Muneza, B. Whitaker, and A. M. Reinhold, "A generalized approach to the operationalization of software quality models," *PeerJ Computer Science*, vol. 10, p. e2357, 2024.

[41] "Automotive spice ver. 3.1, process assessment model," VDA QMC Working Group 13 / Automotive SIG, Nov. 2017.

[42] S. Wagner *et al.*, "Operationalised product quality models and assessment: The quamoco approach," *Information and Software Technology*, vol. 62, pp. 101–123, Feb. 2015.

[43] M. G. Siavvas, K. C. Chatzidimitriou, and A. L. Symeonidis, "Qatch - an adaptive framework for software product quality assessment," *Expert Systems With Applications*, vol. 86, pp. 350–366, May 2017.

[44] A. M. Reinhold, B. Boles, A. R. Manzi Muneza, T. McElroy, and C. Izurieta, "Surmounting challenges in aggregating results from static analysis tools," *Military Cyber Affairs*, vol. 7, Issue 1, Article 6, 2024.

[45] B. Carlson, "Consequence-driven cybersecurity for high-power charging infrastructure," DOE Vehicle Technologies Program, Tech. Rep. INL/MIS-19-53414, Jun. 2017. [Online]. Available: https://www.energy.gov/eere/vehicles/articles/cybersecurity-consequence-driven-cybersecurity-high-power-charging

[46] "Isa/iec 62443 series of standards - isa," International Society of Automation. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[47] "Iso/sae21434: Road vehicles - cybersecurity engineering," Society for Automotive Engineering International, Aug. 2021. [Online]. Available: https://www.sae.org/standards/content/iso/sae21434/

[48] K. Harnett, G. Watson, and G. Brown, "Government fleet and public sector electric vehicle supply equipment (evse) cybersecurity best practices and procurement language report," Volpe National Transportation Systems Center, Cambridge, MA, USA, 2019. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/43606/dot_43606_DS1.pdf

[49] "Ieee 1547.3-2023: Ieee guide for cybersecurity of distributed energy resources interconnected with electric power systems," IEEE Standards Association. [Online]. Available: https://standards.ieee.org/ieee/1547.3/10173/

[50] "Upstream security global automotive cybersecurity report 2024," Upstream Security Ltd., Herzliya, Israel, 2024. [Online]. Available: https://upstream.auto/reports/global-automotive-cybersecurity-report/#

[51] "Iso/iec 25010:2023 systems and software engineering — systems and software quality requirements and evaluation (square) — product quality model," International Standards Organization. [Online]. Available: https://www.iso.org/standard/78176.html

[52] "From bugs to breaches: The software quality problem in security," Aptori. [Online]. Available: https://aptori.dev/blog/from-bugs-to-breaches-the-software-quality-problem-in-security

[53] S. Karnouskos, R. Sinha, P. Leitao, L. Ribeiro, and T. I. Strasser, "Assessing the integration of software agents and industrial automation systems with iso/iec 25010," in *2022 IEEE 20th International Conference on Industrial Informatics (INDIN)*, Jul. 2018, pp. 61–66.

[54] T. Krisher, "Tesla's ev plug is closer to becoming the industry standard following a move by an automotive group," AP News. [Online]. Available: https://apnews.com/article/tesla-electric-vehicle-charging-plug-standard-01ed6050d8ddfbbe2d27b83ddf0b9943

[55] "Sae j3400 charging connector · joint office of energy and transportation," Joint Office of Energy and Transportation. [Online]. Available: https://driveelectric.gov/charging-connector

[56] European Network for Cyber Security, "Ev charging systems security requirements," 2017. [Online]. Available: https://elaad.nl/wp-content/uploads/2022/05/security-requirements-for-charge-points-8-2017.pdf

[57] National Motor Freight Traffic Association, "Medium and heavy duty electric vehicle and charging infrastructure cyber security baseline reference document," Virginia, USA, May 2018. [Online]. Available: https://nmfta.org/wp-content/media/2022/11/MDHDEV-CI-Cyber-Security-v1-2-1-complete.pdf

[58] "Microsoft threat modeling tool threats," Microsoft, Aug. 2022. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[59] Microsoft, "Uncover security design flaws using the stride approach," 2006. [Online]. Available: https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[60] Cybersecurity and Infrastructure Security Agency (CISA), "Cyber security evaluation tool (cset): Cisa," 2025. [Online]. Available: https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset

[61] Electrify America, "About electrify america." [Online]. Available: https://www.electrifyamerica.com/about-us/