SANDIA REPORT
SAND2024-12438
Printed Aug 2024

Assessment and Coordination of EVSE Cybersecurity Standards

Khalid Ansari[†], Robert Brulles [‡], Ryan Cryar[††], Dana Hatic[††], Myungsoo Jun[††], Christopher Lamb[‡], Sherry Mitchell[‡], Yulia Moiseyenko[‡‡], Anuj Sanghvi[††], Sean Tsikteris[†‡], Eirini Eleni Tsiropoulou[†‡], Roland Varriale[‡‡]

[†] FM Approvals, [††] National Renewable Energy Laboratory, [‡] Sandia National Laboratories,
[‡‡] Argonne National Laboratory, [†‡] University of New Mexico

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185
Livermore, California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods

National Nuclear Security Administration

ABSTRACT

Cybersecurity certification programs for Electric Vehicle Supply Equipment (EVSE) are fragmented due to no single certification covering all aspects of the device and additionally the existence of multiple programs and under different levels of regulation. These devices are also confronted by the intricate assembly of product software, firmware, and hardware. Devices contain both logical and physical interfaces. These multifaceted devices have vulnerabilities at many levels and interconnect with other potentially vulnerable systems including the electric vehicle, the cloud where data and payment information are stored, and the electric grid and electric grid equipment including utilities. Of the EVSE certification programs that are found, none are directly for the cybersecurity of EVSE. Many standards are for safety, specifically battery safety, some are cybersecurity standards for other types of equipment and can be modeled for EVSE. In specific, ISA/IEC 62443 is found to be significantly in line with EVSE security needs and will be used in future testing to certify EVSE and help guide the project to demonstrate where gaps exist, where strengths lie in the standard and how this can be used to lead the certification efforts in harmonizing EVSE cybersecurity standards. In addition, there are multiple efforts that are currently seeking to build EVSE standards or revise existing standards to address gaps. This effort is seeking to establish a cybersecurity program for EVSE that will inform customers and help increase the level of security across products and state EVSE procurements to achieve consistency across different jurisdictions.

This page intentionally left blank.

ACKNOWLEDGEMENT

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract TL0104040-5900-4219040-41393.

This page intentionally left blank.

CONTENTS

Acknowledgement . . . . **v**

List of Figures . . . . **ix**

List of Tables . . . . **xi**

List of Abbreviations . . . . **xii**

1. Introduction **1**

2. Analysis Process **3**

3. Standards Reviewed **7**

3.1. UL 2941: Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources 7

3.1.1. General Requirements 7

3.2. UL 2900 8

3.2.1. UL 2900: Objectives 9

3.2.2. UL 2900: Product Capabilities 9

3.2.3. UL 2900: Requirements 9

3.2.4. UL 2900: Risk Management 10

3.2.5. UL 2900: Software Composition 10

3.2.6. UL 2900: Software Weaknesses 11

3.2.7. UL 2900: Software Vulnerabilities 11

3.3. IEEE 2030.5-2018 IEEE Standard for Smart Energy Profile Application Protocol . . 11

3.3.1. IEEE 2030.5: Objectives 12

3.3.2. IEEE 2030.5: Technology Areas 12

3.3.3. IEEE 2030.5: Security 14

3.4. IEEE 1547.3 22

3.4.1. 5.2 Risk Assessment and Management 24

3.4.2. 5.3 Communication Network Engineering 25

3.4.3. 5.4 Access Control 25

3.4.4. 5.5.2 Security for Data at Rest 26

3.4.5. 5.5.3 Security for Data in Transit 26

3.4.6. 5.6 Security management 26

3.4.7. 5.7 Coping and Recovering 27

3.5. ISA/IEC 62443 28

3.5.1. IEC 62443-3-3: System Security Requirements and Security Levels 28

3.5.2. IEC 62443-4-1 Product Security Development Lifecycle Requirements 33
3.5.3. IEC 62443-4-2 Technical Security Requirements for IACS Components . . . 39
3.6. SunSpec Cybersecurity Certification Requirements 44
3.6.1. SunSpec Requirements for Test Procedure 46
3.6.2. SunSpec Requirements SAE J3072 Implementation using the IEEE 2030.5 protocol 48
3.6.3. SunSpec Blockchain Cybersecurity Requirements 51
3.7. ISO 15118-20 Road Vehicles – Vehicle to grid communication Interface – Part 20: Network and application protocol requirements 54
3.7.1. ISO 15118-20: Security Concept 54
3.7.2. ISO 15118-20: Other Relevant Sections 58
3.8. ANSI Roadmap 62
3.8.1. ANSI Roadmap of Standards and Codes for Electric Vehicles at Scale 62
3.9. State Requirements 63

4. Identified Gaps 65
4.1. NIST CSF Profile 65
4.2. Identified Gaps 66

5. Conclusion 77

References 79

Appendices 81

A. Standards Not Selected 81

B. EVSE Ecosystem Lifecycle 83

LIST OF FIGURES

Figure 3-1. ACL Attributes, IEEE 2030.5-2018 15
Figure 3-2. Resource authentication process 18
Figure 3-3. Security LogEvents 21
Figure 3-4. Cybersecurity requirements, threats, and attack vectors 23
Figure 3-5. IEEE 1547.3 scope visualized with corresponding sections 24
Figure 3-6. The ISA/IEC 62443 Series. 29
Figure 3-7. SunSpec Cybersecurity Certification Requirements – An Overview. 45
Figure 3-8. PEV and EVSE Interaction following the IEEE 2030.5 protocol. 51
Figure 3-9. Communication among EVCC, SECC, and SA. 54
Figure 3-10. Document overview 55

Figure 4-1. NIST CSF Core Structure. 66
Figure 4-2. NIST CSF Core Structure. 67
Figure 4-3. Gap Matrix by Color. 68

Figure B-1. EVSE Ecosystem 84
Figure B-2. Summary of Coverage. 85
Figure B-3. Summary of Coverage. 86

This page intentionally left blank.

LIST OF TABLES

Table 3-1. Standard’s objectives 13
Table 3-2. Technology areas covered by IEEE 2030.5 14
Table 3-3. Device credentials 15
Table 3-4. Resource access scenarios and protocols 16
Table 3-5. Port-based request handling 16
Table 3-6. Elements of the cipher suite 19
Table 3-7. Superset test cases that should be validated along with their purpose (part 1). . . . 47
Table 3-8. Superset test cases that should be validated along with their purpose (part 2). . . . 48
Table 3-9. Main Actors Involved in DER Device Security with Different Colors. 52
Table 3-10. Main Use Case Scenarios. 52
Table 3-11. Trusted vs. Untrusted networks 56
Table 3-12. Protection of cryptographic keys 57

Table 4-1. Table of Gaps 75

Abbreviation	Definition
ACL	Access Control List
ANSI	American National Standards Institute
BEV	Battery Electric Vehicle
CA	Certificate Authority
CP	Certificate Policy
CPM	Certificate Provisioning Mode
CPM4PE	Certificate Provisioning Mode for Private Environment
CRL	Certificate Revocation List
CSA	Component Security Assurance
CSO	Charging Station Operator
CSP	Cloud Service Providers
DOE	Department of Energy
DER	Distributed Energy Resource
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DNS-SD	DNS Service Discovery
DNSSEC	Domain Name System Security Extensions
DRBG	Deterministic Random Bit Generator
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Energy Management Systems
eMSP	eMobility Service Provider
EPRI	Electric Power Research Institute
ESI	Energy Services Interface
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment
EXI	Efficient XML Interchange
HAN	Home Area Network
HSM	Hardware Security Modules
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IACS	Industrial Automation and Control Systems
IACSSA	IACS Security Assurance
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol

IPsec	Internet Protocol Security
ISA	International Society of Automation
ISO	International Organization for Standardization
LFDI	Long Form Device Identifier
MTU	Maximum Transfer Unit
NDP	Neighbor Discovery Protocol
NIST	National Institute of Standards and Technology
NRBG	Mon-deterministic Random Bit Generator
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OOI	Outline of Investigation
PDU	Protocol Data Unit
PE	Private Environment
PHEV	Plug-in Hybrid Electric Vehicles
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
PLC	Power Line Communication
PnC	Plug and Charge/Park and Charge
PQC	Post-Quantum Cryptograph
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RNG	Random Number Generation
SA	Secondary Actor
SCVP	Server-Based Certificate Validation Protocol
SDP	SECC Discovery Protocol
SECC	Supply Equipment Communication Controller
SFDI	Short Form Device Identifier
SL	Security Levels
SLAAC	Stateless Auto Address Configuration
SOC	Systems and Organization Controls
SBOM	Software Bill of Materials
SPDLC	Secure Product Development Life Cycle
Sub-CA	Subordinate Certificate Authority
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Diagram Protocol
URI	Uniform Resources Identifier
V2G	Vehicle-to-Grid
V2GTP	V2G Transfer Protocol
VAS	Value Added Service

WADL	Web Application Description Language
WLAN	Wireless Local Area Network
XML	Extensible Markup Language
XSD	XML Schema Definition
Zero-RTT	Zero Round-Trip Time

1. INTRODUCTION

With the rapid expansion of electric vehicles (EVs) across the globe, the integration of electric vehicle supply equipment (EVSE) into our infrastructure presents both unprecedented opportunities and critical cybersecurity challenges. The Biden Administration's National Standards Strategy for Critical and Emerging Technology underscores the urgency of harmonizing standards to safeguard these pivotal components of our transportation and energy sectors. Despite the exponential growth in EV adoption, there remains a pressing need for cohesive cybersecurity standards specifically tailored to EVSE.

Recent incidents highlight the vulnerabilities within the automotive and mobility sectors, with a staggering 295 cybersecurity incidents reported in 2023 alone [1]. As EVSE networks expand, so too does their attractiveness to malicious actors seeking to exploit potential entry points into the power grid. This threat is compounded by the forecasted proliferation of EV chargers, projected to increase by 8.4% in just the third quarter of 2023 [2]. By 2030, the United States anticipates requiring 28 million EV charging ports to support an estimated 33 million EVs, underscoring the critical need for robust cybersecurity measures [3].

Amidst this backdrop, various standards bodies and organizations are diligently developing frameworks to enhance the security posture of EVSE technologies. Initiatives led by entities like the Department of Energy (DOE), National Institute of Standards and Technology (NIST), International Electrotechnical Commission (IEC), International Organization for Standardization (ISO), SunSpec, and others are pivotal in advancing the dialogue and implementation of cybersecurity protocols across the industry. This paper aims to critically review these evolving standards and their applicability to a voluntary certification program for EVSE cybersecurity.

By examining the current landscape of standards and conducting a comprehensive gap analysis against the NIST Cybersecurity Framework Profile (CSF), this research seeks to elucidate opportunities for bolstering cybersecurity practices within the EVSE sector. Ultimately, the adoption of a unified certification standard nationwide would constitute a significant stride towards ensuring the integrity and resilience of EVSE infrastructure against emerging cyber threats.

Section 2 of this paper delves into the Analysis Process, exploring the foundational principles shaping EVSE cybersecurity standards. Section 3 provides an in-depth review of standards from multiple organizations, while Section 4 presents the findings of our gap analysis. Finally, Section 5 offers concluding insights and recommendations for advancing EVSE cybersecurity in an era defined by technological convergence and heightened cyber risks.

This page intentionally left blank.

2. ANALYSIS PROCESS

This section describes the standards we have selected and why they are the most applicable for evaluation. To begin, the team put together a list of standards and then proceeded to identify those that are most applicable to cybersecurity for EVSE. The processes used to evaluate these standards consisted of a general review and discussion of the applicability to EVSE in section 3. The tables below lists the initial compilation of standards gathered from a much larger list that included other EVSE adjacent standards (see Appendix A) . The standards that were excluded were standards that govern EVs, batteries, and other electrical and technical requirements. Those selected are listed in the table below along with a short description of the standard.

Some additional research was done to map the selected standards to the EVSE ecosystem to get an idea of what areas of the EVSE ecosystem has coverage, by which standards, and at what point in the lifecycle. An explanation of the EVSE ecosystem lifecycle and the results of this research are in Appendix B.

Standard	Description
ISO 15118	Road Vehicles – Vehicles to Grid Communication Interface: This standard specifies the communications between EVs and the power grid, including charging stations.
ISO 15118-20	2nd generation network layer and application layer requirements. This part outlines communication standards between EVs and EVSE. This standard focuses on facilitating bidirectional power transfer and defines communication messages and sequences. It specifies requirements for wireless communication in both conductive and wireless charging scenarios. The document also details the communication process between the electric vehicle communication controller (EVCC) and the supply equipment communication controller (SECC).

Standard	Description
SunSpec	Cybersecurity Certification Requirements
SunSpec	SunSpec Requirements SAE J3072 Implementation using the IEEE 2030.5 protocol
SunSpec	Blockchain Cybersecurity Requirements

Standard	Description
ISA/IEC 62443 Industrial Communication Networks	Network and System Security. This family of standards defines requirements and process for implementing and maintaining electronically secure industrial automation and control systems (IACS).
ISA/IEC 62443-3-3:2013	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in ISA/IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C(capability). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(Target), for a specific asset.
ISA/IEC 62443-4-1:2018	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. This standard applies to supplier's development lifecycles processes for products used in industrial automation and control systems including EVSE. It defines a secure development life-cycle (SDL) for the purpose of developing and maintaining secure products. This life-cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. These requirements apply to the developer and maintainer of the product, but not to the integrator or user of the product.
ISA/IEC 62443-4-2:2018	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components. This standard provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in ISA/IEC 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C(Capability).

Standard	Description
IEEE 1547.3:2018	The standard provides guidelines and technical specifications for the interconnection of distributed energy resources (DERs) with the electric power grid. This standard is the most recent version of the IEEE 1547 standard. Key features of the standard include technical requirements, grid support functions, communication and control, safety, protection, and testing.
IEEE 2030.5-2018	IEEE Standard for Smart Energy Profile Application Protocol
ANSI Electric Vehicle Standards Panel (EVSP) - Roadmap of Standards and Codes for Electric Vehicles at Scale	It is not a standard. It is a roadmap for the standard developing organizations. The roadmap's focus is on light-duty, on-road plug-in EVs that are recharged via a connection to the electrical grid, as well as the supporting charging infrastructure needed to power them. Medium and heavy-duty EVs are also covered, as is wireless charging. A total of 37 standardization gaps are identified with corresponding recommendations across the topical areas of vehicle systems, charging infrastructure, grid integration, and cybersecurity.
UL 2900 Series	This standard applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware.
UL 2941	Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources

Table 2 Summarizes the standards and their purposes.

This page intentionally left blank.

3. STANDARDS REVIEWED

This section provides a detailed study of the selected standards reviewed. Each of the standards listed in the tables from the previous section are given their own subsection here. These standards are examined and then in the next section analyzed for gaps, with the exception of the ANSI Roadmap and the NEVI State Requirements, which are provided as additional context.

3.1. UL 2941: Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources

The standard applies to cybersecurity evaluation for network connected inverter-based resources and parts of inverter-based resource (IBR) systems that provide software-based and firmware-based controls, including, but not limited to such devices as inverters, monitoring, and controller devices. It describes the minimum cybersecurity requirements that IBR equipment shall support.

The outline does not contain the methods of validation of these requirements and requirements regarding functional testing of a product, which means the standard contains no requirements to assess that the product functions as designed. The standard is written in a way that the choice of implemented technology is at the manufacturer's decision.

3.1.1. General Requirements

UL 2941, as outlined at the start of the standard, specifies the requirements that vendors shall account for cybersecurity of network connected inverter-based resources and parts of inverter-based resource (IBR) systems. The standard provides requirements in 11 areas starting from Section 5 through Section 15 in the document that manufacturers or vendors shall follow.

Section 5 of UL 2941 is titled "Access Control, User Authentication and User Authorization," and outlines the requirements for vendors to observe to secure confidence in identification and authentication of users and processes. The section has 22 mandatory and 7 conditional requirements. Requirements for Cryptography is presented in Section 6. Cryptography includes key generation, key exchange, encryption methods, versioning, negotiation, and policies used in cryptographic practices for securing information. Detailed cryptographic methods are outlined in Annex C. It includes 8 mandatory, 8 conditional, and 1 optional requirement regarding cryptography.

Section 7 describes requirements for Sensitive Data Management to protect from data exfiltration and unauthorized access while helping to ensure the integrity of the device. The section has 13 mandatory and 1 conditional requirements. Most of them deal with encryption of data with sensitive or critical information. Requirements for Security Management are specified in Section 8. Security management covers the implemented features that facilitate the configuration and maintenance of the cybersecurity functions and the protection of the device. In total 25 requirements (9 mandatory and 16 conditional) are specified for security management.

UL 2941 assigns Section 9 for Risk Management that the device vendor shall conduct per release of a new device model or firmware update to reduce the risks of backdoors, bots, malware, or any other form of malicious behavior. It specifies 7 mandatory requirements. Section 10 of UL 2941 presents requirements for Documentation because documentation provided along with the device is an important source of information. It describes security features and interfaces that shall be implemented in the device.

Section 11 of UL 2941 is dedicated to requirements for Monitoring. Monitoring enables real-time intervention and alarms when anomalous events are detected. Logging of events is important to be able to assess threats, analyze errors and overall functioning of the device. Investigation and monitoring of logs can lead to an early discovery of malicious logins and other anomalous events. A total of 13 mandatory requirements for Logging are specified in Section 12 of UL 2941.

Product management requirements, which are specified in Section 13, are related to the cybersecurity design choices made by the vendor such as penetration testing, security firmware updates, software updates, device updates, product decommissioning, etc. Compliance of integrity mechanisms for product management is specified in Annex D1.3. Security functions in DER are often required to have accurate timing because malicious time sources can manipulate the device time and data resulting in system inaccuracy, non-sequential logging, and erroneous operation. Section 14 specifies 3 mandatory requirements for Time Synchronization of the device.

The last section of UL 2941 presents requirements for Physical Anti Tamper. Since physical access to the device grants the malicious user access to the interfaces and HMI of the device, any unprotected interface or HMI allowed action increases the attack surface and therefore the risk of intrusion. This section specifies the cybersecurity requirements for physical accesses to the device such as console port, HMI, and USB ports.

3.2. UL 2900

UL 2900-1, with its official title *ANSI//CAN//UL 2900-1:2023 Software Cybersecurity For Network-Connectable Products, Part 1: General Requirements*, applies as an approved American National Standard and a National Standard of Canada. The standard offers guidance on testing and evaluating network-connectable products for cybersecurity vulnerabilities while referencing prior frameworks and standards regarding weaknesses involved in cyber communications protocols and processes. It outlines requirements for security risk controls in product architecture and design, as well as methods for evaluating and testing products for vulnerabilities. The standard does not include requirements for a product’s functional testing or hardware. In the context of EVSE, UL 2900 is important for considering future integration of distributed charging infrastructure and cybersecurity resilience.

3.2.1. UL 2900: Objectives

The primary objective of this standard is to enhance security around communications protocols and trust mechanisms. UL 2900 invites transparency from vendors and covers roles, responsibilities, and authorities for the risk management process of such network-connectable products. In identifying key information for vendors to provide, UL 2900 enhances mechanisms for vendors to demonstrate a product's capability with respect to managing vulnerabilities, software weaknesses, and malware. Restricting guidance to evaluations of products for software vulnerabilities, rather than functional testing of a product or the hardware contained therein, UL 2900 can accommodate a variety of EVSE configurations and structures while maximizing cybersecurity risk controls.

3.2.2. UL 2900: Product Capabilities

UL 2900 deeply probes the process of design and subsequent connectivity and communication capabilities of software products. In accounting for all manner of use of software products, the standard asks vendors to lay out on the table any and all potential vulnerabilities and the ways in which software is designed to manage risk. For software incorporated into EVSE, these connections, interfaces, and communications protocols are critical to maintaining resilience and compatible operations. The following section details the requirements outlined within UL 2900 as they pertain to software product design, use, and testing, before introducing the relevance and requirements for EVSE.

3.2.3. UL 2900: Requirements

The foundations of UL 2900, detailed at the beginning of the standard, explain the documentation vendors must provide to account for fundamental functions and components of a software product. UL 2900 offers a section on documentation of a product, its design, and its use, which covers a wealth of functions for which a product may be incorporated into EVSE. The guidance aims to account for every possible function a product can execute, as well as possible interfaces and communications protocols each supports, including remote, local, and wireless interfaces, as well as external file inputs.

Section 4 of UL 2900, titled "Documentation of Product, Product Design and Product Use," outlines requirements for vendors to provide specific information about their products, including all functions and configurable interfaces that support remote, local, and wireless communication protocols. It makes a request that vendors account for all software components in a product—including contents or libraries, source code, and build configuration parameters—to ensure proper product deployment and function. Further, this section requests visibility into when and how third-party libraries are used within software. Section 5 requires vendors to provide a security risk analysis and corresponding design documentation for evaluation.

In section 6, UL 2900 outlines all the requirements product vendors must meet regarding how it documents security considerations, product effectiveness for intended functions and configurations, as well as the communication protocols and external interfaces the product will use. The idea is that such documentation is a model of best practices in the spirit of NIST CSF and SP800-53. This documentation should offer requirements and recommendations for the software product's use, configuration, and authentication and authorization, in addition to how to evaluate efficacy and risk associated with the product's use. Section 7, "Risk Controls," dictates compliance for product vendors with security risk controls detailed across additional sections of UL 2900, including circumstances in which a vendor should document and justify any deviation from the requirements within a risk assessment or analysis.

Under section 8, UL 2900 lays out the specifics around access control, user authentication, and user authorization, requiring vendors to provide clear documentation of the ways in which software cybersecurity protocols are implemented. This includes time-out protocols configurable at a user level, cryptographic compliance, role and privilege differentiation, and account management. These requirements are further extended under section 9, "remote communication," which requires verification that a software product can provide "integrity and authenticity" of data communicated over remote interfaces. UL 2900 provides security functions requirements in Annex C of the document.

The remainder of the baseline requirements dictate management of sensitive data using separate cryptographic keys for each "service, operation, or function" and document the processes in accordance with the risk management provisions of UL 2900. Finally, a vendor must ensure software products allow for security updates and patches, with stipulations for verification of authenticity and storage of security-related events. At end-of-life, a vendor may follow NIST SP 800-00 guidance on decommissioning products.

3.2.4. UL 2900: Risk Management

Section 12 of UL 2900 provides vendors guidance on how to conduct their risk management process through the design phase of a software product, including developing a security risk analysis plan, using a classification scheme for the risks identified in the process, and documenting the risk evaluation method for known vulnerabilities or weaknesses.

Other sections of the standard refer back to section 12 to provide guidance on acceptable and unacceptable types of weaknesses, vulnerabilities, and risks contained in software products.

3.2.5. UL 2900: Software Composition

In terms of explicating a product's software composition, vendors must, under UL 2900, execute a Software Composition Analysis to be able to provide a software bill of materials (SBOM). Prior to delivering a software product, a vendor must also verify the product's compliance with malware detection and inspection in accordance with section 14, otherwise, a vendor should provide justification and documentation for not using a malware detection tool, per compliance requirements in section 12.

Further, under section 15, a vendor must ensure software products continue to operate as intended, even when there are invalid or unexpected inputs on any of its connected interfaces. This malformed input testing requirement simulates product configuration based on a vendor's recommended documentation, with inspection intended to verify that only the authorized external interfaces appear in the product.

Section 16 describes the requirements for structured penetration testing, or the process by which vendors check software products for exploitable pathways that compromise its designed functionality. The idea is to enhance resilience so any malfunction may be corrected to a product's previous state. The goal of the penetration test is to find and exploit flaws based on the following conditions:

- "Circumvent the risk controls and security configuration of the product;
- Attempt to engage the product in a denial of service;
- Attempt to access and authenticate on the product via unauthorized means;
- Attempt to exploit vulnerabilities acceptable in the risk analysis;
- Attempt to elevate privilege on the product."

3.2.6. UL 2900: Software Weaknesses

UL 2900 requires vendors to conduct analysis for software weaknesses to ensure a product does not contain weaknesses that are deemed unacceptable in section 12 of the standard. Analysis must be conducted using static source code analysis, as well as static binary and bytecode analysis.

3.2.7. UL 2900: Software Vulnerabilities

This final section of UL 2900 dictates that static analysis should be conducted on all binary and bytecode provided by the vendor of a software product, unless exceptions can be justified as required in section 12 of the standard. Compliance should be verified with the evaluation of all available code for "all known vulnerabilities applicable to the product published in the National Vulnerability Database," available through NIST. Ideally, known vulnerabilities should be eliminated, unless a vendor can prove the impacts present a low enough risk.

3.3. IEEE 2030.5-2018 IEEE Standard for Smart Energy Profile Application Protocol

IEEE 2030.5, officially titled *IEEE 2030.5-2018 IEEE Standard for Smart Energy Profile Application Protocol*, is also known as SEP 2.0 (Smart Energy Profile 2.0). IEEE 2030.5 is an internationally recognized open standard for smart energy communications that was primarily designed to facilitate the communication between various smart grid and home area network devices, often referred to as the Internet of Things (IoT).

By leveraging IoT principles, IEEE 2030.5 offers consumers diverse methods to control their energy consumption and production. The standard utilizes TCP/IP to define application layer functions that enable the exchange of information, including time of day pricing, load control, demand response, and energy usage, thereby integrating devices such as smart thermostats, meters, plug-in electric vehicles, electric vehicle supply equipment (EVSE), smart inverters, smart appliances, and energy management systems (EMS). By establishing a framework to support these applications, IEEE 2030.5 ensures a secure, interoperable, and plug-and-play ecosystem for various grid-connected devices, fostering seamless collaboration and interoperability across different devices and systems.

The IEEE 2030.5 standard includes three essential documents for compliance:

1. IEEE Std 2030.5: The primary standard document.
2. IEEE 2030.5 XML Schema Definition (XSD): Schema file(sep_wadl.xml) provided in the supplemental materials.
3. IEEE 2030.5 WADL: Web Application Description Language file (sep_wadl.xml) included in the supplemental materials.

All IEEE 2030.5 devices must comply with these documents to ensure standard adherence.

3.3.1. IEEE 2030.5: Objectives

To enhance the efficiency, functionality, and security of energy management infrastructure, the IEEE 2030.5 standard has several key objectives. The primary objective of the standard is interoperability which ensures seamless communication among diverse devices and systems. Therefore, different devices, regardless of manufacturer or underlying technology, can effectively work together. The features of zero configuration and automated discovery significantly enhance interoperability objectives. They enable devices to automatically find and configure themselves with other devices on the network, eliminating the need for manual setup and ensuring that new devices can seamlessly integrate into the existing system.

Another objective of the IEEE 2030.5 standard is scalability which enables support of a wide range of devices and applications, from small residential setups to large industrial installations. The standard also incorporates security features such as encryption, authentication, and authorization to protect against cyber threats. Lastly, this standard offers flexibility and aims to allow the integration of new technologies and devices over time. This ensures the protocol remains adaptable to future advancements in smart grid technology. Below, Table 3-1 summarizes the objectives.

3.3.2. IEEE 2030.5: Technology Areas

IEEE 2030.5 covers a wide range of technology areas that are important for smart grid communication and energy management.

Objectives
Interoperability
Scalability
Security
Flexibility

Table 3-1. Standard's objectives

In Section 4, the standard addresses the flexibility of the protocol, general rules, and best practices, ensuring that communication protocols can adapt to various smart grid setups. It includes specifications for WADL (Web Application Description Language) and the use of Uniform Resources Identifiers (URIs), which are necessary for defining how resources are accessed and interacted with.

IEEE 2030.5 addresses data models aimed at standardizing data representation for consistent information exchange. Section 9 specifically defines standardized data models and schemas for a variety of smart grid devices. It encompasses essential functions such as time, power status, network status, log events, configuration, and device information.

In Section 5: Application Support, the standard outlines the framework for message handling. This includes the use of TCP, URI encoding, HTTP headers, HTTP response codes, application payload syntax, and content negotiation. These provisions aim to ensure reliable and efficient communication among devices.

IEEE 2030.5 includes a detailed section on various security attributes, including device credentials, authentication and authorization context, cipher suits, default security policies, registration, security log events. and certificate management. These clauses are designed to greatly enhance secure communications.

The standard also addresses device and resource management to facilitate the monitoring and control of connected devices and resources. This includes functions such as device capabilities, self-device functions, and device function sets, along with function set assignments, subscription/notification, and response function sets. These provisions enable efficient management of devices and resources.

The demand response and load control function set within the smart energy resources section of the standard enables utilities and energy providers to implement demand response programs. This involves communicating with customer devices to manage and reduce energy usage during peak periods, thus maintaining grid stability.

The standard includes provisions for integrating and managing Distributed Energy Resources (DERs) such as solar panels and energy storage systems. These are addressed within the distributed energy resource function set.

IEEE 2030.5 covers support for electric vehicles through function sets for metering, pricing, messaging, billing prepayment, and flow reservation. These provisions enable effective communication between EVs, EV supply equipment (EVSE), and grid operations, supporting smart charging and vehicle-to-grid integration.

Another aspect covered by the standard is the incorporation of manufacturer-specific proprietary extensions. This allows manufacturers to introduce unique requirements, thus enhancing flexibility. The standard includes provisions for xmDNS/DNS-SD, URIs, resources, and device capabilities to support these extensions.

Below are the key technology areas covered by the IEEE 2030.5 standard:

Technology Area	Explanation
Communication Protocols	Ensures flexible and robust communication among devices
Messaging Framework	Provides a protocol for message handling
Security	Provides security features to protect data and ensure secure communication
Device and Resource Management	Facilitates effective management of devices and resources
Demand Response and Load Control	Enables demand response programs and load control functionalities
DER Integration	Integration and management of various DERs
EV Support	Provides communication and management for EVS and EVSE
Manufacturer-Specific Proprietary Extensions	Allows for specific extensions by manufacturers to meet unique needs

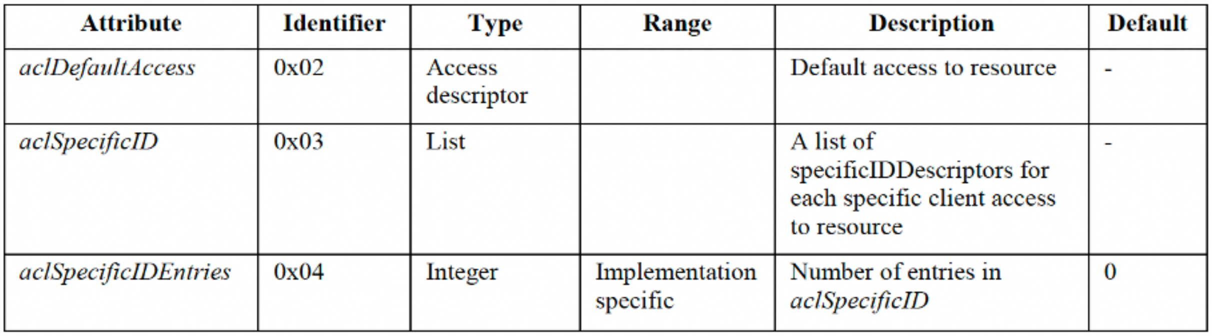
Table 3-2. Technology areas covered by IEEE 2030.5

3.3.3. IEEE 2030.5: Security

As mentioned earlier, the IEEE 2030.5-2018 standard includes a detailed section on security, which outlines essential mechanisms to ensure the integrity, confidentiality, and availability of smart grid communications. Section 6 covers various security aspects, such as device credentials, authentication, and authorization contexts to manage resource access. It specifies the supported encryption cipher suites, defines default security policies, and offers guidelines for device registration and certificate management. Additionally, emphasis is placed on logging security events to enable effective monitoring and incident response. The key provisions include the following:

Section 6.2.3 Access control List (ACL) attributes.

Access Control List (ACL) attributes represent data used to determine whether a particular client can access a resource. ACLs enforce granular access control based on criteria such as client identity. While conceptually, every resource has an ACL, in practice, only resources with complex access policies may need detailed ACL data. ACLs are used to grant or revoke privileges, with default configurations denying access unless explicitly granted. Initial ACL settings are defined by the security policy, with dynamic inheritance for subordinate resources. ACLs are a valuable security measure commonly integrated into EVSE implementations. Sections of this part can likely be repurposed for EVSE implementation, as they should translate effectively. The table below outlines ACL attributes as defined by the IEEE 2030.5 standard. These attributes will require adjustment to align with EVSE-specific attributes and characteristics.



Attribute	Identifier	Type	Range	Description	Default
aclDefaultAccess	0x02	Access descriptor		Default access to resource	-
aclSpecificID	0x03	List		A list of specificIDDescriptors for each specific client access to resource	-
aclSpecificIDEntries	0x04	Integer	Implementation specific	Number of entries in *aclSpecificID*	0

Figure 3-1. ACL Attributes, IEEE 2030.5-2018

Section 6.3 Device credentials

Section 6.3 of the standard addresses device credentials, which consists of three key elements per device, including short form device identifier (SFDI), long form device identifier (LFDI), and Personal Identification Number (PIN).

Credentials per Device
Short Form Device Identifier (SFDI)
Long Form Device Identifier
Personal Identification Number (PIN)

Table 3-3. Device credentials

In Section 6.3.2, the certificate fingerprint is discussed. The SFDI and LFDI are derived from the certificate fingerprint, which is generated by applying a SHA256 operation to the entire DER-encoded certificate. This fingerprint serves as a unique identifier and is openly used to derive the SFDI and LFDI, but it is not confidential and does not lead to the generation of further keying material. Therefore, this mechanism is not considered trustworthy and should not be used when applying to EVSE systems. An example of such a certificate fingerprint is provided in IEEE 2030.5-2018 for illustrative purposes:

3E4F-45AB-31ED-FE5B-67E3-43E5-E456-2E31-984E-23E5-349E-2AD7-4567-2ED1-45EE-213

Other clauses in Section 6.3 discuss the parameters and components of SFDI, LFDI, and PIN. Section 6.3.4 provides detailed information on LFDI, noting its use for “when a globally unique identity is required.” However, the algorithm used is not cryptographically secure nor sufficient to provide this level of assurance. An attacker could intercept the non-confidential certificate and derive the SFDI and LFDI. Therefore, the assessment that this provides adequate cryptographic security cannot be supported.

Section 6.4 Resource access authentication and authorization context

This section of the IEEE 2030.5 standard outlines the authentication and authorization process for network and application layer communications. Once authenticated and authorized to join a network, a node can engage in network layer communication. However, for application layer communication, clients and servers "MAY" be required to undergo additional application layer authentication. Similarly, registration with utility or third-party service providers "MAY" also be necessary for explicit device and user authorization at the application layer. The use of "MAY" introduces flexibility but may weaken security assurance, suggesting consideration of stronger language such as "SHALL" or "SHOULD" for clearer and more consistent security requirements.

The section also discusses HTTPS and HTTP application layer connections. Thus, resource access requiring application layer authentication, data confidentiality, and integrity checking must occur through HTTPS (HTTP over TLS 1.2). If a request is made to the HTTPS port, authentication is mandatory and will be initiated if not already done, after which the request is evaluated against the Access Control List (ACL). For HTTP requests, authentication is not required, but the request is still evaluated against the ACL. Authentication authorization is determined by the ACL settings, which consider the level of client authentication and may use a Local Registration List for device-specific authorization. Tables below represent HTTPS and HTTP details discussed in the Section 6.4.

Scenario	Protocol Used	Authentication Required	Action Upon Request
Resource access requiring application layer authentication, data confidentiality, and integrity checking	HTTPS (HTTP over TLS 1.2)	Yes	Authentication initiated or already done. Request evaluated against ACL
Resource access NOT requiring application layer authentication, data confidentiality, and integrity checking	HTTP	No	Request passed to ACL. Client considered unauthenticated

Table 3-4. Resource access scenarios and protocols

Port Used	Considered Request Type	Authentication Required	Action Upon Request
HTTPS Port	HTTPS Request	Yes	Authentication initiated or already done. Request evaluated against ACL with ancillary information from secure session
HTTP Port	HTTP Request	No	Request passed to ACL. Client considered unauthenticated

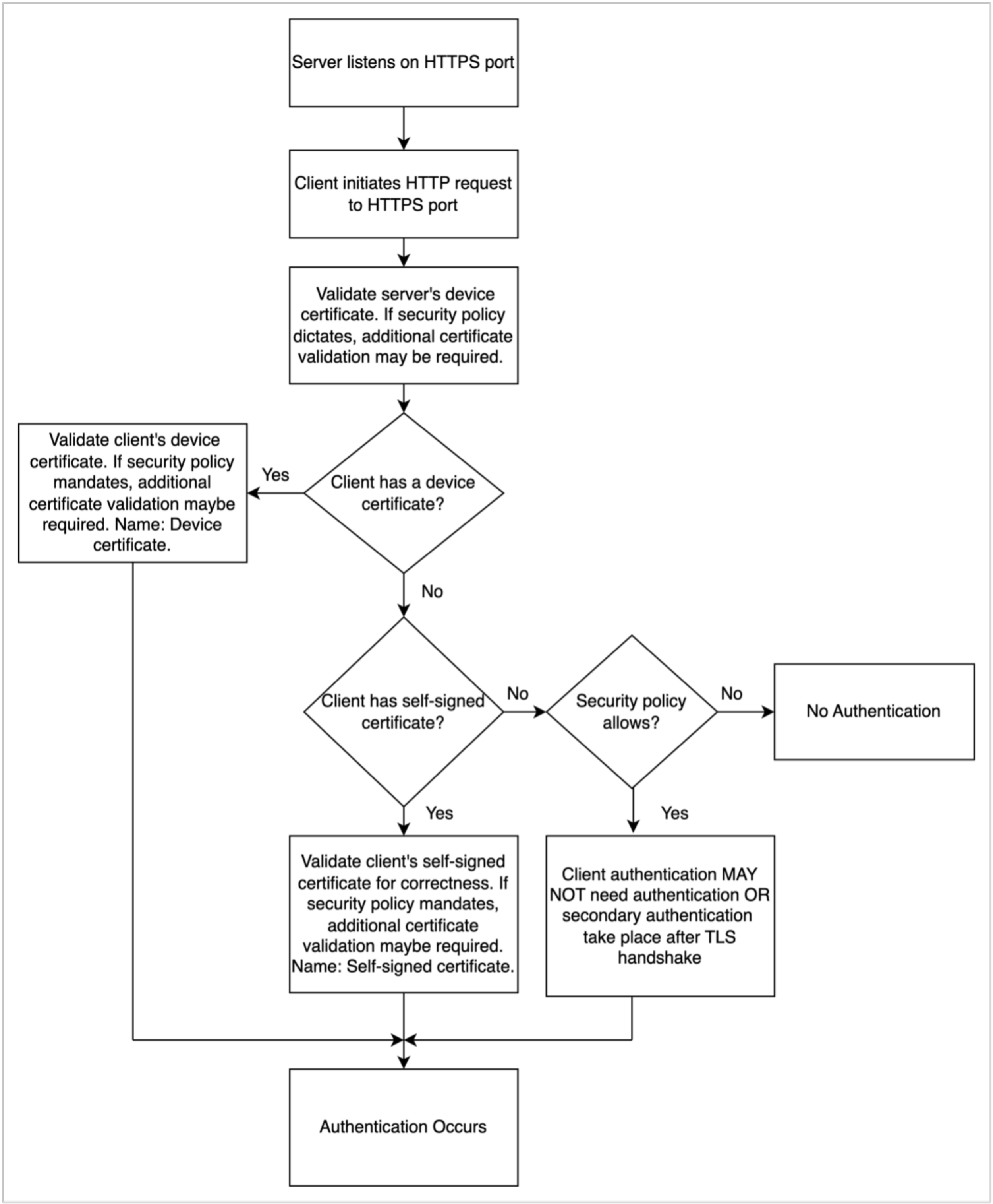
Table 3-5. Port-based request handling

Section 6.5 Resource access authentication

Section 6.5 describes the resource access authentication process, which is applicable only to HTTPS connections. While it is possible to implement authentication over HTTP transaction, this method is not covered by the IEEE 2030.5-2018 standard, leaving HTTP-based authentication out of scope. This exclusion presents potential security risks as relying only on HTTPS without addressing HTTP could create vulnerabilities. The lack of guidance on the HTTP authentication process is considered a gap in the standard.

For HTTPS communications, the authentication process follows TLS (IETF RFC 5246) requirements. While IETF RFC 5246 specifies the TLS protocol version 1.2, Section 6.5 does not mention the TLS version. Previous sections of the standard specify TLS version 1.2 or higher for secure communication. To enhance clarity and ensure the use of a more secure protocol, the TLS version should be specified if this section is applied to EVSE systems applications.

The use of TLS (IETF RFC 5246) requires all servers to present a device certificate during the TLS handshake. The process involves the server listening on the HTTPS port, the client initiating an HTTP request, and mutual authentication via device certificates. If no TLS session is in place, a TLS handshake occurs between the server and the client. If the client does not have a certificate and the security policy permits, client authentication may be skipped or secondary client authentication may occur. The following figure represents the detailed steps of the resource authentication process.



Server listens on HTTPS port
Client initiates HTTP request to HTTPS port
Validate server's device certificate. If security policy dictates, additional certificate validation may be required.
Client has a device certificate?
Yes
Validate client's device certificate. If security policy mandates, additional certificate validation maybe required. Name: Device certificate.
No
Client has self-signed certificate?
No
Security policy allows?
No
No Authentication
Yes
Validate client's self-signed certificate for correctness. If security policy mandates, additional certificate validation maybe required. Name: Self-signed certificate.
Yes
Client authentication MAY NOT need authentication OR secondary authentication take place after TLS handshake
Authentication Occurs

Figure 3-2. Resource authentication process

Overall, this section is well-suited for EVSE systems as it requires only minor modifications to effectively tailor it to the specific operational and security needs of EVSE systems.

Section 6.6 Resource access authorization

Section 6.6 of the IEEE 2030.5-2018 standard outlines the process for resource access authorization. Normally, preauthorization for resources is established during client registration. If the security policy permits, authorization may occur immediately after authentication based on implicit rules, allowing requests to complete even if the client is unregistered. For clients using self-signed certificates, preauthorization based on the SFDI must be completed, and authorization is granted if the SFDI matches the one presented during registration.

This section requires significant modification as it relies on the SFDI (Short Form Device Identifier) and LFDI (Long Form Device Identifier) constructs of the IEEE 2030.5-2018 standard. Despite this reliance, it remains an important area for ensuring secure resource access particularly in the context of EVs and EVSE.

Section 6.7 Cipher suites

IEEE 2030.5-2018 mandates the use of a single cipher suite that provides a security level of 128 bit, specifically TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite (IETF RFC 7251), which utilizes the elliptic curve secp256r1. Each element of the cipher suite is explained in the following table:

Element	Description
TLS	TLS version 1.2
ECDHE	Key exchange algorithm Elliptic Curve Diffie-Hellman Ephemeral used to establish a shared secret between the client the sever. Keys are temporary and used only for the duration of the session.
ECDSA	Elliptic Curve Digital Signature algorithm. Used for signature authentication and integrity verification.
WITH	
AES_128	Advanced Encryption Standard with 128-bit key. An encryption algorithm with 128 key size in bits denoting the strength of the encryption.
CCM_8	Counter with CBC-MAC Mode (CCM) using an 8-byte authentication tag used for message authentication and confidentiality.

Table 3-6. Elements of the cipher suite

The use of a single cipher suite prevents weak protocol downgrade attacks and promotes interoperability, one of the main objectives of the standard. Key requirements are divided into server and client requirements. Therefore, server requirements mandate all devices acting as servers must support Elliptic Curve Cryptography (ECC), while devices acting as clients must support ECC cipher suites to validate ECC certificates and be capable of requesting an ECC certificate. The section also mentions that devices can support additional cipher suites, but these suites should maintain cryptographic strength at least equivalent to the mandatory cipher suite.

This part of the standard can be applied to EVs and EVSE. Additionally, considering the inclusion of Post-Quantum Cryptography (PQC) suites, which provide security resistant to attacks from quantum computing attacks, is also advisable.

Section 6.8 Default security policy

This section outlines that service providers can create security policies by balancing regulatory requirements and risk assessments. These policies may trade off ease of data access with information assurance, utilizing TLS, ACLs, and other security controls to meet different needs. The implementation of these policies falls outside the scope of the standard, but the standard does provide default security policies for each function set to facilitate certification testing. Policy attributes include the following items:

· Functions set: reflects the functionsImplemented attribute in DeviceInformation

· aclDefaultAccess AuthType: reflects the default access control settings

· Device certificate need: specifies if a device certificate is needed

· Device registration: specifies if registration is required

The default policies ensure that servers support necessary measures during certification testing and can support additional policies as needed. This section is crucial for EVs and EVSE and should be implemented accordingly.

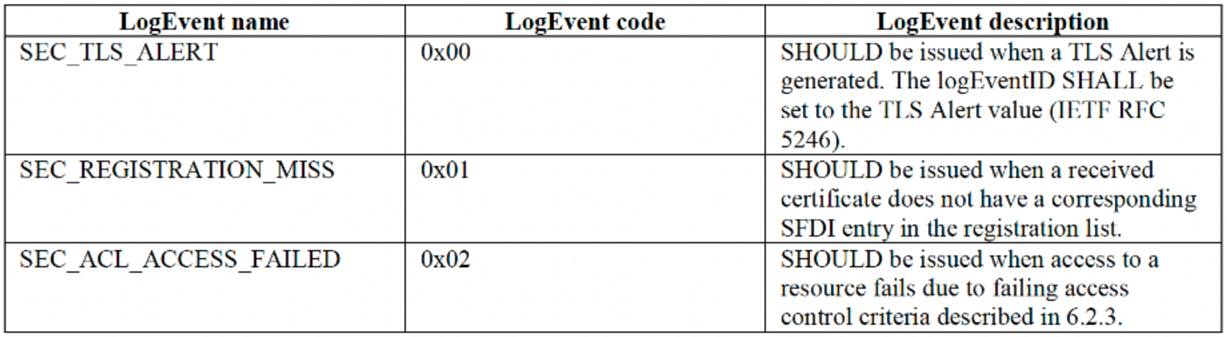
Section 6.9 Registration

Section 6.9 has two subsections including 6.9.1 Introduction and 6.9.2 EndDeviceList. Subsection 6.9.1 outlines the registration process for clients using a device certificate with and EndDevice server. The process involves providing the clients SFDI and optionally, a PIN to the server that manages the resource. Registration can be completed in advance through a service provider or on-demand by presenting the client's SFSI to the premises owner for authorization. Clients register through an EndDevise resource on an energy services interface (ESI), managed by a utility, premises owner, or trusted third party. This section may be too perspective for EVSE, as it seems to be more a business operation tasks rather than a cybersecurity task.

Subsection 6.9.2 EndDeviceList specifies that clients must use DNS service discovery (DNS-SD) to locate HAN services and resolve the URI of the EndDeviceList for registration and authentication. The EndDeviseList is used to register a device with a utility, premises owner, or service provider program. Registration configures the server's aclLocalRegistrationList with the client's SFDI, optionally a PIN, and required device types. This enables the server to authenticate the client based on the SFDI and device certificate. This procedure seems very prone to DNS poisoning unless the Domain Name System Security Extensions (DNSSEC) is used. It may not be necessary to EVSE.

6.10 Security LogEvents

Section 6.10 of the IEEE 2030.5-2018 standard defines specific LogEvents related to security. These events include SEC_TLS_ALERT, SEC_REGISTRATION_MISS, and SEC_ACL_ACCESS_FAILED. Below is the table provided by the standard that explains each LogEvent item.



LogEvent name	LogEvent code	LogEvent description
SEC_TLS_ALERT	0x00	SHOULD be issued when a TLS Alert is generated. The logEventID SHALL be set to the TLS Alert value (IETF RFC 5246).
SEC_REGISTRATION_MISS	0x01	SHOULD be issued when a received certificate does not have a corresponding SFDI entry in the registration list.
SEC_ACL_ACCESS_FAILED	0x02	SHOULD be issued when access to a resource fails due to failing access control criteria described in 6.2.3.

Figure 3-3. Security LogEvents

While this section is crucial for EVSE, providing essential logging for security-related events, it is relatively brief in this standard and requires further expansion to fully address EVSE needs.

6.11 Certificate Management

Section 6.11 of the IEEE 2030.5-2018 standard specifies the public-key infrastructure (PKI) used in the IEEE 2030.5 certificate management system, known as Manufacturing PKI. This PKI issues certificates to devices during application installation, such as at the time of manufacture. These certificates are used for authenticating devices during deployment, redeployment, and ongoing operations over TLS. The standard anticipates the market will implement multiple Manufacturing PKIs as required. The standard also describes optional certificates for specific device classes like energy services interfaces (ESIs) and web portals. There are six classes of certificates in an IEEE 2030.5 system:

1. Device certificates: Issued during manufacturing for operational use.

2. Device test certificates: Issued during manufacturing for testing.

3. Additional certificates: Optional TLS server certificates for devices like ESIs.

4. Generic client certificates: Issued by non-IEEE 2030.5 Certificate Authorities (CAs) to non-native entities.

5. Generic server certificates: Issued by non-IEEE 2030.5 Certificate Authorities (CAs) to non-native entities.

6. Self-signed client certificate for non-native entities: Self-generated and self-signed by customers or software.

This part of the standard is important for application in EVSE. However, additional details are needed to clarify how it relates to or differs from EVSE PKI. The rest of this section of the standard is dependent on specific deployment and implementation details, which will vary based on the particular requirements and configurations of the IEEE 2030.5 applications in use.

3.4. IEEE 1547.3

IEEE 1547.3 Std developed in 2007 did not adequately meet present security needs and hence a revision of the IEEE 1547.3 was undertaken. IEEE 1547.3 is a guide for cybersecurity of DERs interconnected with electric power systems and is targeted towards utilities, DER owner/operators, aggregators, manufacturers/integrators supporting DER interconnections, and other DER stakeholders. The document, referred to as a guide, is a non-binding document intended for stakeholders in this space to have a resource for recommendations that can be testable upon interconnection. This guide is intended to be complementary to the IEEE 1547-2018 standard for interoperability requirements. As such its scope is limited to that of the DER device as well as it's connection within this ecosystem. IEEE 1547.3 cybersecurity guidance entails securing the information infrastructure surrounding DERs and the respective stakeholders. Some key stakeholders that IEEE 1547.3 include the following:

1. Operators of the Grid (DER operators, independent/transmission system operators, utility planners)
2. Entities with financial interests (DER owners, aggregators, retail energy providers, energy markets)
3. Utility regulators
4. Support services
5. DER manufacturers

These stakeholders have different roles and responsibilities for managing or operating DER equipment and is the basis for several threat vectors. Some of the tactics, techniques, and procedures are described in the figure as mapped from the MITRE ATT&CK framework.

IEEE 1547.3 lacks coverage on NIST CSF's Govern category and insufficiently addresses governance controls that need to be embedded within organizational processes. Also, there are specific elements of the NIST CSF categories of Identify, Protect, Detect, Respond, and Recover that are insufficiently addressed.

The guide begins by describing the importance of cyber physical security, and the fundamentals in order to understand why the recommendations are recommendations. This is broken up into "components of cybersecurity, cybersecurity concepts for cyber-physical power systems, cybersecurity as a continuous process, rationale for defense-in-depth and end-to-end cybersecurity, risk management, and managing cybersecurity: security levels and maturity scoring" [4].

The document then describes cybersecurity for the DER domain and why it is essential to grid resiliency, along with the fundamentals of the power systems impacts. This is the transition into the core of the document, described through the recommendations.

The scope of the document is broken into 3 different categories:

1. Operator and Aggregator Recommendations
2. DER Communications Recommendations

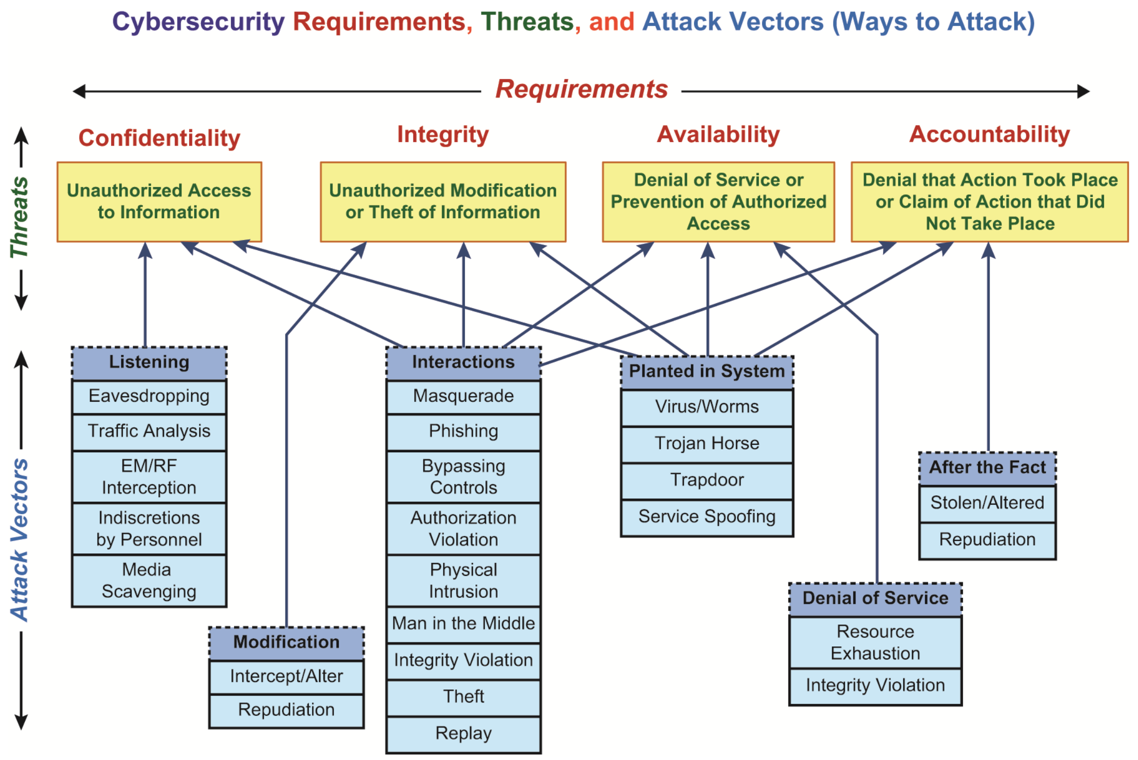


Figure 3-4. Cybersecurity requirements, threats, and attack vectors

3. DER recommendations

Each of the different scope categories has different recommendations that are applicable to that specific area. While some of the scopes have overlapping recommendations, some of them exist at a different level. Such as within the communications recommendations, patch management is one of the categories in which it only applies to that specific scoping.

The Operator and Aggregator Recommendations are split up into 6 categories:

- 5.2 Risk Assessment and Management
- 5.3 Communication Network Engineering
- 5.4 Access Control
- 5.5.2 Security for Data-at-Rest
- 5.6 Security Management
- 5.7 Coping and Recovering

The DER Communications Recommendations are split up into 5 categories:

- 5.2 Risk Assessment and Management
- 5.3 Communication Network Engineering
- 5.5.3 Security for Data in Transit

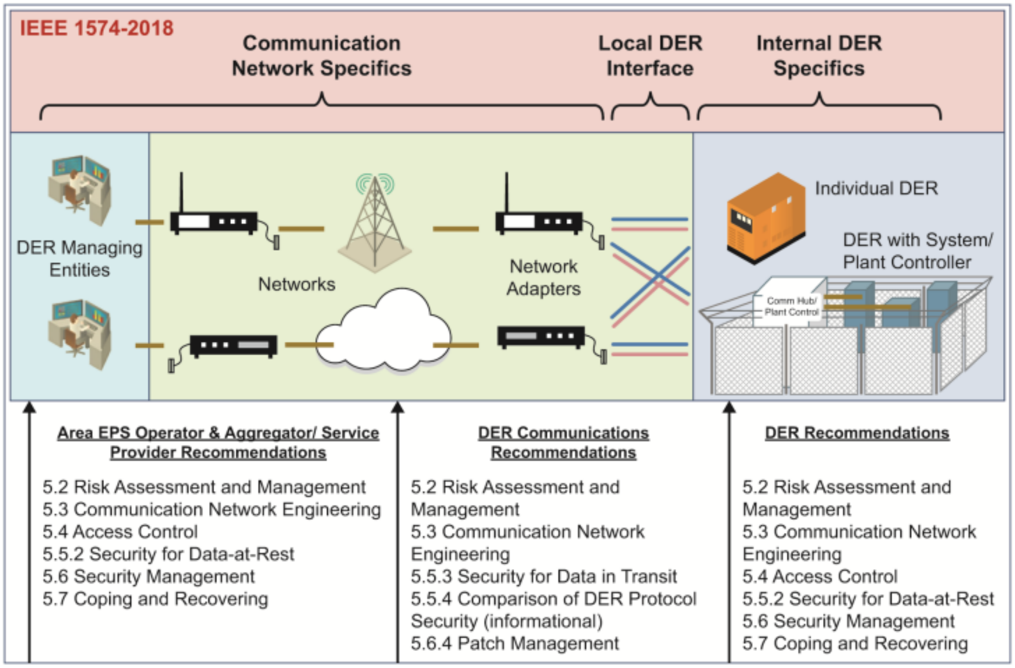

IEEE 1574-2018
Communication Network Specifics
Local DER Interface
Internal DER Specifics
DER Managing Entities
Networks
Network Adapters
Individual DER
DER with System/ Plant Controller
Comm Hub/ Plant Control
Area EPS Operator & Aggregator/ Service Provider Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.4 Access Control
5.5.2 Security for Data-at-Rest
5.6 Security Management
5.7 Coping and Recovering
DER Communications Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.5.3 Security for Data in Transit
5.5.4 Comparison of DER Protocol Security (informational)
5.6.4 Patch Management
DER Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.4 Access Control
5.5.2 Security for Data-at-Rest
5.6 Security Management
5.7 Coping and Recovering

Figure 3-5. IEEE 1547.3 scope visualized with corresponding sections

- 5.5.4 Comparison of DER Protocol Security (informational)
- 5.6.4 Patch management

Finally, the DER Recommendations are:

- 5.2 Risk Assessment and Management
- 5.3 Communication Network Engineering
- 5.4 Access Control
- 5.5.2 Security for Data-at-Rest
- 5.6 Security Management
- 5.7 Coping and Recovery

These sections are further described in the following subsections.

3.4.1. 5.2 Risk Assessment and Management

In the Risk Assessment and Management recommendations, the section focuses around the assessment of the risk and management of those risks to ensure a mature ecosystem. The key activities within the section focus around the cross organization assessment of potential threats such as what are the potential inadvertent threats, and the deliberate threats in order for those threats to be mitigated and managed as much as possible. The section also outlines the key activity of establishing risk management processes, timelines, acceptable risks, responsibilities, and cybersecurity events in the event of risks becoming actionable.

3.4.2. 5.3 Communication Network Engineering

In the Communication Network Engineering section, the document focuses on the communication network design and security of the interactions with the stakeholders and the DER. The activities described within this section, determine what network topologies are documented, data exchanges are documented, internal communications and external communications are isolated, and critical assets are isolated from other systems. Additionally, there are recommendations focused around the management of the security boundaries of networks, where the communications are protected, and data leaks are protected.

Network traffic monitoring follows within this section in order to protect against intrusions and leaks. Recommendations encompass logging, as well as detailing a baseline for what the network traffic monitoring should have.

Network security equipment contains recommendations that are specific to protecting the equipment from network intrusion. This includes the disabling of ports and services which are not in active use, strict access control implementations complying with 5.4, and hardware boundaries.

The last two sub sections within network engineering are physical access to networks and cloud computing. Physical access describes the recommendations in order to protect unused physical ports, or disabling the physical ports through software if possible. Cloud computing recommendations are more generalized through the hosted solutions and issues to be considered that is outlined in the later sections.

3.4.3. 5.4 Access Control

Access control is the section that describes the recommendations for user access as well as system access. The user access recommendations require authentication, authorization, accountability and non-repudiation in order to have a cohesive and strong access control mechanism. The same recommendations hold true for system level access controls. However, System access control recommends that the system authentication be performed as close to the end system as possible.

The section then details access management recommendations, where it was recommended default passwords be changed upon installation, and that multiple users are supported by the system. In addition, the section details that a secure interface should be provided for updating user accounts include passwords, and that any changes are logged.

Recommendations then get more specific for the Role Based Access Control (RBAC) sub-section within access control. The guide details that RBAC be the specific implementation of access control implemented for the systems. Both users and systems are assigned one or more roles only necessary to complete the required tasks, for the concept of least privilege. All of the entities within the system must verify the requesting system or user has the required roles that of which they are trying to access, if not the system requires that it be logged.

RBAC implementation also requires that there be multiple roles associated with the following rights:

- Reading DER information and data
- Writing control settings
- Any additional functions be documented

3.4.4. 5.5.2 Security for Data at Rest

Security for data at rest is hosted within the data security section, which covers software including databases, applications, services, and firmware. The security for data at rest requires that any access be authorized through RBAC with the proper assigned roles. This data that is at rest, including any non-volatile storage of sensitive data, must also be encrypted utilizing mechanisms that are not deprecated according to the latest NIST 800-130 guidance. When the time has come for the device to be decommissioned, a standard operating procedure must also take place to ensure that the entire device is sanitized of any data that has been stored on the device.

3.4.5. 5.5.3 Security for Data in Transit

Security for data in transit is the next section within the data security section. Data in transit contains more strict recommendations due to the possibility of additional attack vectors. This section recommends that in addition to utilizing authentication of the source of the data and the recipient, that RBAC methods must be utilized to authorize any function over the data. The section also identifies that X.509 certificates be utilized, TLS 1.3 implemented if possible while understanding TLS 1.2 being easier to implement, and key management is performed as well. Finally, the guide provides recommendations on detailing the timestamp of the data must be applied, and verified upon receipt that it is within a timely manner, and that any sessions that fall outside of a session time period be timed out and terminated.

3.4.6. 5.6 Security management

Security management details recommendations on management of the ecosystems security aspects such as lifecycle management, supply chain management, patch management, security event logging, and data backups.

Under lifecycle management, the guide puts emphasis on the asset's lifecycle where all asset inventories include the physical devices, firmware installed, software versions, externally managed services and that the hardware/software and security upgrades be noted in the asset inventories. The guide also recommends that assets must all include a secure identity that is associated with them, and documented within these inventories.

Operating system management is a separated recommendation from regular software lifecycle management, such that any operating system on the devices must be within the vendors supported window, and that any that are outside the vendor version support window be recommended for decommissioning after being isolated. The decommissioning process is then required to note any assets or software within the assets inventory that are being decommissioned or disposed.

The guide includes a specific section under security management for supply chain management, where vendors and assets are continually assessed. Additionally, any language associated with suppliers or agreements must include proper language for supply chain risk management.

Patch Management is one of the largest sub-sections within security management. The guide recommends that the device and its supported systems support updates, remote updates, and automated updates. These updates must be verified they are from the correct source and that the integrity of the patch has not been tampered. This includes that the update be supplied by the supplier with proof of the supplier's identity. The supplier of the patch, must include details such as the fixes within the patch, and any security management done within the patch such as risk mitigation. Any suppliers of these patches must apply a patch to the device and its supported systems within 60 days of a vulnerability being discovered to ensure timely delivery of a mitigation to said vulnerability. Suppliers are also recommended to supply a software bill of materials (SBOM) to the customer in a machine readable format to ensure supply chain transparency. Patches must also be agreed on by the supplier and customer on a specified window of time.

The next sub-section details the recommendations for security event logging, for monitoring during a possible security event. The guide recommends that the system at a minimum must log:

- Login attempts both successful and unsuccessful
- Any malicious code found
- Logging failures
- Settings changes
- Updates
- RBAC access changes

All logs must be timestamped, keeping in line with secure timekeeping practices, and all logs must be protected with the necessary permissions with roles.

Data backups is the final set of recommendations within the security management section. Data backups are recommended to be done on a periodic basis and stored in an offline location. These backups must also include snapshots of field device configurations.

3.4.7. 5.7 Coping and Recovering

The coping and recovering section provides recommendations for the recovery of security events. The section is broken up to pre-event recommendations, during-event recommendations, and post-event recommendations.

In the pre-event recommendations, the focus is on primarily documenting and realizing potential risks and their associated strategies. A baseline of the current systems architectures, and other configurations is recommended to be documented to ensure that after the event it can be restored to its original state. Incident response plans are also recommended developed at this stage, along with any key stakeholder agreements be put in place for management during and after an event.

In during-event recommendations, the focus is on following the documented procedures and contacting the proper authorities. The guide recommends that governmental organizations are contacted if appropriate during the event with request for assistance if needed. During said event, any information is coordinated with the agreed stakeholders in the pre-event recommended procedures. Any logs must also be collected and stored during the security event for post-event dissection and analysis.

In post-event recommendations, the focus is around restoring and updating to original states if necessary. Any information that is collected during the event is recommended to be disseminated to the proper stakeholders or authorities. Additionally, reporting mechanisms are utilized to show what happened, what has been done, and any additional actions being taken to prevent similar events from happening. Finally, it is recommended an analysis and inventory on any affected assets, and upon agreement from all external stakeholders the security event is closed.

3.5. ISA/IEC 62443

ISA/IEC 62443 series of standards, also referred to as IEC 62443 standards, define requirements and processes for implementing electronically secure industrial automation and control systems (IACS). The focus of this analysis was limited to those parts of IEC 62433 standards (3-3, 4-1, and 4-2) that provide a common set of requirements to enable product suppliers in designing and delivering secure and reliable IACS devices and systems. Other parts not analyzed here address governance and security program management for the end-user and service provider among other topics.

An overview of the set of IEC 62443 standards can be seen in Figure 3.6 [5] below.

3.5.1. IEC 62443-3-3: System Security Requirements and Security Levels

IEC 62443-3-3 plays a pivotal role in securing industrial automation and control systems (IACS). As a part of the extensive IEC 62443 series, it outlines specific guidelines to bolster the cybersecurity of IACS. This standard zeros in on system security requirements and security levels, presenting a structured approach to deploy cybersecurity practices in industrial settings. Its goal is to shield critical infrastructure from emerging cyber threats. IEC 62443-3-3 covers essential aspects such as network segmentation, access control, data integrity, and incident response, providing a solid framework to defend industrial systems against cyber risks.

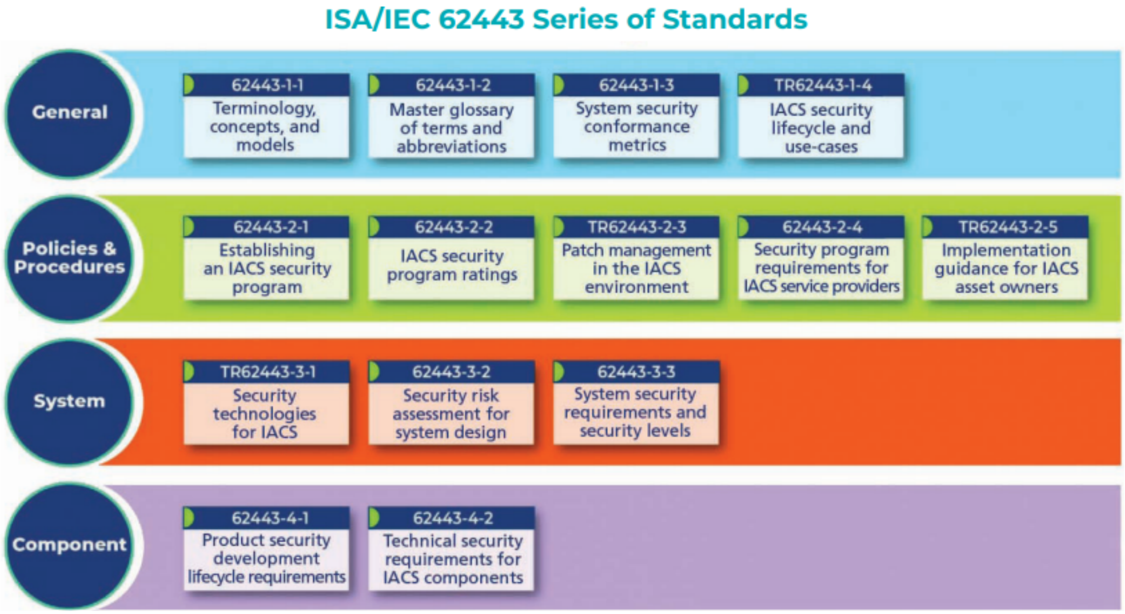

ISA/IEC 62443 Series of Standards
General
62443-1-1
Terminology, concepts, and models
62443-1-2
Master glossary of terms and abbreviations
62443-1-3
System security conformance metrics
TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
62443-2-1
Establishing an IACS security program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

Figure 3-6. The ISA/IEC 62443 Series.

3.5.1.1. Security Levels

Both IEC 62443-3-3 and IEC 62443-4-2 define four distinct security levels (SLs) to measure and implement the cybersecurity posture of Industrial Automation and Control Systems (IACS). Each level addresses different threat scenarios and prescribes specific measures to mitigate risks.

Security Level 1 (SL1) provides basic protection against casual or accidental breaches, targeting attackers with minimal motivation and resources. Measures include basic user authentication, simple access controls, basic logging, and minimal encryption. SL1 is suitable for non-critical systems with limited external connectivity.

Security Level 2 (SL2) defends against intentional but basic attacks using simple means and low resources. Measures include stronger authentication (e.g., two-factor authentication), role-based access control (RBAC), enhanced logging, basic network segmentation, firewalls, and improved encryption. SL2 is appropriate for systems with moderate risk, such as small industrial control systems with moderate external exposure.

Security Level 3 (SL3) provides robust protection against sophisticated attacks using moderate resources. Measures include advanced authentication (e.g., biometrics), fine-grained access control, comprehensive logging and monitoring, strong network segmentation, demilitarized zones, IDS/IPS, end-to-end encryption, and regular security assessments. SL3 is ideal for critical systems with high exposure, such as power plants and large manufacturing facilities.

Security Level 4 (SL4) ensures the highest protection against highly sophisticated attacks using extensive resources. Measures include multi-factor authentication, granular access controls, advanced security monitoring, rigorous network segmentation, multiple firewalls, comprehensive IDS/IPS, full data encryption, continuous security assessments, threat intelligence integration, and secure product development lifecycle. SL4 is suitable for high-stakes environments like national critical infrastructure.

Security Level	Threat Actors	Typical Measures	Use Cases
SL1	Casual attackers	Basic user authentication, simple access controls, basic logging, minimal encryption	Non-critical systems, limited external connectivity
SL2	Basic intentional attackers	Stronger authentication, RBAC, enhanced logging, basic network segmentation, improved encryption	Moderate-risk systems, small industrial control systems
SL3	Motivated attackers	Advanced authentication, fine-grained access control, comprehensive logging, strong network segmentation, end-to-end encryption	Critical systems, large manufacturing facilities
SL4	Highly sophisticated attackers	Multi-factor authentication, granular access controls, advanced security monitoring, rigorous network segmentation, full data encryption	National critical infrastructure, military installations

3.5.1.2. Foundational Requirements

The IEC 62443-3-3 standard sets foundational requirements for securing Industrial Automation and Control Systems (IACS), emphasizing the importance of Identification and Authentication Control (IAC) and Use Control (UC) to ensure entities are properly identified, authenticated, and granted access only to authorized functions and data, utilizing mechanisms like Multi-factor Authentication (MFA), Role-Based Access Control (RBAC), and Access Control Lists (ACLs). System Integrity (SI) and Data Confidentiality (DC) protect against unauthorized modifications and access, employing antivirus software, application whitelisting, encryption, and secure communication protocols. Restricted Data Flow (RDF) controls information flow within IACS zones through network segmentation and unidirectional gateways, while Timely Response to Events (TRE) and Resource Availability (RA) ensure operational resilience by implementing intrusion detection systems, incident response teams, redundancy, and backup solutions. This comprehensive framework addresses a wide spectrum of security threats, ensuring the integrity, confidentiality, and availability of IACS components and data.

Foundational Requirement	Objective	Key Measures
Identification and Authentication Control (IAC)	Ensure proper identification and authentication of entities	User and device authentication, MFA, secure identity management
User Control (UC)	Ensure access control for authenticated entities	RBAC, ACLs, access monitoring and logging, regular access rights review
System Integrity (SI)	Protect and verify system integrity	Malware protection, integrity verification, patch management, continuous integrity monitoring
Data Confidentiality (DC)	Protect sensitive information from unauthorized access	Data encryption, secure communication protocols, data masking, least privilege access
Restricted Data Flow (RDF)	Control and restrict information flow within and between IACS zones	Network segmentation, conduits, data diodes, network traffic monitoring
Timely Response to Events (TRE)	Detect and respond to security events promptly	IDS/IPS, SOC/Incident response team, incident response plans, SIEM systems
Resource Availability (RA)	Maintain system availability and operational continuity	Redundancy, failover mechanisms, backup and recovery, resource management

3.5.1.3. System Wide Security Measures

System-wide security measures are comprehensive controls and practices applied across an entire IACS to enhance overall security. These measures integrate various components, processes, and practices to create a cohesive security posture. A critical aspect of these measures, is network segmentation and zoning where the objective is to divide the IACS network into distinct zones and control data flow between them to minimize the risk of unauthorized access and contain potential breaches. Key measures include creating security zones based on different levels of trust and security requirements, defining and controlling communication paths using firewalls, routers, and gateways, and implementing demilitarized zones (DMZs) to isolate critical systems from external networks. Additionally, firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are deployed to protect the IACS network from external and internal threats by filtering traffic and detecting or preventing malicious activities. Secure communication protocols are essential to ensure the confidentiality and integrity of data transmitted within the IACS, using strong encryption algorithms and mutual authentication between devices. Access control mechanisms are implemented to restrict access to IACS resources to authorized users and devices only, utilizing role-based access control (RBAC), multi-factor authentication (MFA), and the principle of least privilege. Continuous security monitoring and incident response are facilitated by Security Information and Event Management (SIEM) systems, real-time monitoring tools, and a well-defined incident response plan integrated with threat intelligence feeds.

Security Measure	Objective	Key Measures
Network Segmentation and Zoning	Minimize risk and contain breaches	Zones, conduits, DMZs
Network Traffic Monitoring	Filter traffic and detect/prevent malicious activities	Firewall, IDS/IPS
Secure Communication Protocols	Ensure confidentiality and integrity of data	Encryption, authentication, secure protocols
Access Control Mechanisms	Restrict access to authorized users and devices	RBAC, MFA, least privilege
Incident Detection and Response	Detect and respond to security incidents	SOC analysis, incident response playbooks/plans, threat intelligence
Physical Security	Protect against physical tampering and damage	Access controls, surveillance, environment controls
Backup and Recovery	Ensure data and system availability and integrity	Regular backups, off-site storage, recovery testing

To reduce the attack surface, system hardening involves eliminating unnecessary services and applying regular security patches and secure configurations. Physical security measures include implementing physical access controls, surveillance, and environmental controls to protect hardware from tampering and damage. Finally, robust backup and recovery processes ensure the availability and integrity of data and systems, with regular backups stored in secure off-site locations and frequent recovery testing to verify their effectiveness.

A comprehensive security posture is essential for IACS. By properly integrating various security measures, these systems effectively mitigate risks and enhance the overall security of IACS environments.

3.5.1.4. Assessment and Compliance

The assessment process aims to evaluate the security of IACS to ensure they comply with metrics defined in security levels (SLs) and foundational requirements (FRs). This begins with an initial assessment, which involves identifying the IACS components, zones, and conduits to be evaluated. A baseline security assessment is conducted to establish the current security posture by identifying existing controls, vulnerabilities, and threats. Following this, a gap analysis compares the current security status with the required security levels and foundational requirements to identify deficiencies. The process continues with a risk assessment that identifies potential external and internal threats to the IACS, analyzes vulnerabilities within the components, and evaluates the likelihood and impact of these threats exploiting the identified vulnerabilities. Risks are then prioritized based on their severity. Finally, the security controls assessment verifies the effectiveness of existing controls against the required standards, incorporating security testing, including penetration tests, to confirm the implementation and efficacy of these controls. The compliance process ensures that IACS meet the specified security levels and foundational requirements through a structured framework. This involves defining compliance criteria, including specific security levels (SL1 to SL4) for different IACS components and zones based on risk assessments, and ensuring adherence to foundational requirements as explained in 3.3.1.2. Implementation entails deploying necessary security controls to address identified gaps and developing policies and procedures to support these controls. Comprehensive documentation of security controls, policies, procedures, and assessment results is maintained, and audit trails ensure all security activities, changes, and incidents are logged and traceable. Ongoing compliance involves continuous monitoring of the IACS to promptly detect and respond to security incidents, regular audits to verify adherence to IEC 62443-3-3 requirements, and periodic reassessments to accommodate changes in the threat landscape and system modifications. Certification by third-party assessors provides independent validation of compliance, with compliance reports prepared for stakeholders. Benefits of this rigorous assessment and compliance process include enhanced security through the mitigation of security gaps, adherence to industry regulations, effective risk management, and continuous improvement of security controls and practices.

3.5.2. IEC 62443-4-1 Product Security Development Lifecycle Requirements

IEC 62443-4-1 is a critical component of the IEC 62443 series, concentrating on the secure development lifecycle of IACS. This standard outlines a detailed framework of practices and processes aimed at creating secure products from the ground up. It encompasses security considerations from the initial design phase to deployment and ongoing maintenance. By prioritizing secure software development and system engineering, IEC 62443-4-1 ensures that security measures are integrated throughout the entire product lifecycle. This method not only reduces vulnerabilities but also bolsters the overall cybersecurity defenses of industrial systems, which in turn safeguards critical infrastructure against potential cyber threats.

3.5.2.1. Security Management

Proper security management should focus on establishing a framework to ensure the security of IACS throughout their lifecycle. This involves establishing clear security policies and objectives aligned with organizational goals and regulatory requirements, and assigning specific roles and responsibilities to ensure accountability. Implementing a comprehensive risk management process and conducting regular security reviews and audits help identify, assess, and mitigate potential security risks while verifying compliance and evaluating control effectiveness.

Security Management	Requirement	Rationale and Supplemental Guidance
SM-1	Document and enforce a general product development/maintenance/support process.	Ensure well-defined, proven processes. Examples: ISO 9001, ISO/IEC 27034.
SM-2	Identify roles and personnel responsible for each required process.	Assign responsibilities within the organization. Use tools like a RACI matrix.
SM-3	Identify products (or parts) to which this document applies.	Apply processes to appropriate products with correct detail. Criteria: market intent, security requirements, risk.
SM-4	Provide security training and assessment programs for relevant personnel.	Ensure personnel have adequate expertise. Training should be role-specific.
SM-5	Identify applicable parts of this document for a selected project.	Justify scoping with documented security analysis. Examples: no software, no external interfaces.
SM-6	Provide an integrity verification mechanism for scripts, executables, and important files.	Ensure files have not been altered. Methods: cryptographic hashes, digital signatures.
SM-7	Protect the product during development, production, and delivery.	Ensure no unauthorized alterations or disclosures. Apply ISO/IEC 27001 and ISO/IEC 27002 controls.
SM-8	Protect private keys used for code signing from unauthorized access or modification.	Ensure private keys are secure.
SM-9	Identify and manage security risks of externally provided components.	Address supply chain security. Maintain an inventory of third-party components. Refer to ISO/IEC 27036-3.
SM-10	Ensure third-party developed components conform to requirements.	Applies to subcontracted components with security implications. Use threat modeling.
SM-11	Verify that products or patches are not released until security issues are addressed.	Ensure no unresolved security issues. Use vulnerability scoring systems like CVSS.
SM-12	Verify completion of all applicable security-related processes before release.	Ensure key security practices are executed.
SM-13	Continuously improve the SDL.	Improve SDL rigor over time. Review and enhance processes periodically.

This table highlights the key activities involved in security management according to IEC 62443-4-1, which collectively contribute to a proactive security posture, minimizing vulnerabilities and enhancing the overall security resilience of the system.

3.5.2.2. Specification of Security Requirements

The specification of security requirements should focus on identifying and defining the necessary security measures for IACS. This process begins with the identification of necessary security requirements based on the system's context, including its operational environment, potential threats, and regulatory demands. It is crucial to define the security functionality and assurance levels needed to protect the system adequately, ensuring that these requirements provide a comprehensive security framework. All security requirements must be clearly defined and testable, allowing for effective verification and validation throughout the system's lifecycle.

Activity	Description
Requirement Identification	Identify all necessary security requirements based on the system context, including threats, environment, and regulatory needs.
Functionality and Assurance	Define the necessary security functionality and assurance levels for the system to ensure comprehensive protection.
Testable Requirements	Ensure all security requirements are clearly defined and testable, facilitating effective verification and validation processes.

This table outlines the key activities involved in specifying security requirements which emphasize a systematic approach to identifying, defining, and verifying security needs to ensure integrity, availability, and confidentiality of IACS.

3.5.2.3. Secure Design

Promote secure design that emphasizes the integration of security measures during the design phase of IACS. This involves applying core design principles such as least privilege, defense in depth, and secure by design to ensure minimal necessary access and multiple defensive strategies. Threat modeling identifies potential security threats and vulnerabilities, allowing proactive mitigation. Implementing risk mitigation involves deploying tailored security controls. Layered security provides multiple lines of defense, ensuring system protection even if one layer is compromised. This comprehensive approach helps build resilient systems capable of withstanding various security challenges.

Activity	Description
Design Principles	Apply principles such as least privilege, defense in depth, and secure by design to ensure robust security foundations.
Threat Modeling	Conduct threat modeling to identify potential security threats and vulnerabilities proactively.
Risk Mitigation	Implement security controls to effectively mitigate the risks identified during threat modeling.
Layered Security	Design security mechanisms in layers to provide multiple lines of defense against potential threats.

This table outlines the key activities involved in secure design according to IEC 62443-4-1, highlighting a systematic approach to integrating security measures from the design phase to build resilient and secure industrial control systems.

3.5.2.4. Secure Implementation

The Security Implementation Review (SI-1) process ensures that implementation reviews are conducted to identify, characterize, and resolve security-related issues in the secure design implementation. This includes verifying that security requirements are met, secure coding standards are followed, and static code analysis (SCA) is performed to detect security coding errors. The process also involves reviewing the implementation's traceability to defined security capabilities and examining threats and their potential to exploit implementation interfaces, trust boundaries, and assets. The rationale emphasizes the importance of comprehensive security reviews to ensure the implementation adheres to secure design principles and best practices. Manual and automated reviews are used to verify requirements, adherence to best practices, and identify security vulnerabilities and non-conformities in the code.

The Secure Coding Standards (SI-2) process mandates the incorporation of periodically reviewed and updated security coding standards in the implementation processes. These standards include avoiding exploitable constructs, banned functions, and insecure design patterns, using automated tools, following secure coding practices, validating inputs crossing trust boundaries, and proper error handling. The rationale highlights the necessity of providing developers with guidance to avoid common implementation pitfalls that could lead to security issues. The product supplier maintains and follows a list of security best practices based on industry standards and lessons learned, ensuring these practices remain current and relevant.

3.5.2.5. Security Verification and Validation Testing

Proper security verification and validation testing ensure effective protection for IACS. Comprehensive security test plans and regular penetration testing identify and address potential weaknesses. Requirement validation confirms that security measures meet specified requirements and mitigate risks. Detailed test documentation tracks testing activities and results, ensuring rigorous evaluation and continuous improvement of system security.

Activity	Description
Test Plans	Develop comprehensive security test plans covering all aspects of the system to ensure thorough testing.
Penetration Testing	Perform regular penetration testing to identify and address potential security weaknesses, simulating real-world attack scenarios.
Requirement Validation	Perform regular penetration testing to identify and address potential security weaknesses, simulating real-world attack scenarios.
Test Documentation	Maintain detailed records of all security testing activities and results to track testing processes, findings, and corrective actions.

This table summarizes the key activities involved in security verification and validation testing, emphasizing the importance of thorough planning, proactive testing, requirement validation, and meticulous documentation in ensuring system security.

3.5.2.6. Security-related Processes in the Maintenance Phase

The maintenance phase is crucial for the continued security of IACS. Timely application of security updates and patches protect against new vulnerabilities, while continuous threat monitoring addresses emerging threats. Up-to-date security documentation and ongoing training programs keep personnel informed about the latest practices and potential threats. These processes collectively ensure ongoing security throughout the system's operational life.

Activity	Description
Security Updates	Ensure timely availability and application of security updates and patches to protect against newly discovered vulnerabilities.
Threat Monitoring	Continuously monitor for new threats and vulnerabilities that may affect the system, enabling proactive risk management.
Documentation Maintenance	Keep security documentation up to date with the latest information and practices, ensuring clear guidance for managing system security.
Training and Awareness	Provide ongoing security training and awareness programs for personnel to keep them informed about the latest security practices and potential threats.

This table summarizes the key activities involved in the maintenance phase according to IEC 62443-4-1, emphasizing the importance of timely updates, continuous monitoring, documentation maintenance, and ongoing training in sustaining system security.

3.5.2.7. Management of Security-related Issues

Effective management of security-related issues ensures that security threats are promptly identified, managed, and resolved. Establishing a process for handling security issues that encompasses identification, reporting, and resolution procedures to ensure a swift response to potential threats. Vulnerability tracking involves continuously monitoring and managing vulnerabilities from discovery through to resolution, ensuring issues are addressed systematically and efficiently. Prompt and clear communication with stakeholders to ensure relevant parties are informed about security issues and their resolutions. Maintaining detailed incident records is also crucial, providing a comprehensive log of all security incidents and the actions taken to resolve them, which is valuable for future reference and continuous improvement of security practices.

Activity	Description
Issue Handling	Establish a process for handling security issues, including identification, reporting, and resolution to ensure swift response and management.
Vulnerability Tracking	Track and manage vulnerabilities from discovery through to resolution ensuring systematic and efficient handling of security threats.
Stakeholder Communication	Communicate security issues and their resolutions to relevant stakeholders promptly to maintain transparency and foster collaboration.
Incident Records	Maintain a detailed log of all security incidents and the actions taken to resolve them, providing a valuable reference for future security improvements.

This table outlines the key activities involved in managing security-related issues according to IEC 62443-4-1, highlighting the importance of structured processes, continuous tracking, effective communication, and comprehensive documentation in maintaining and improving system security.

3.5.2.8. Documentation Requirements

Proper documentation is a fundamental requirement of IEC 62443-4-1, ensuring that all aspects of security are thoroughly documented and maintained. This includes detailed documentation of all security policies, procedures, and guidelines, providing a clear framework for managing system security. Maintaining comprehensive records of all security-related activities and decisions is essential for traceability and accountability. Ensuring that security documentation is accessible to all relevant personnel fosters a culture of security awareness and adherence to established practices. Regular review and updating of security documentation are necessary to reflect changes, improvements, and emerging threats, ensuring it remains current and effective. This systematic approach to documentation helps maintain robust security practices and supports continuous improvement in managing security risks.

Activity	Description
Security Documentation	Document all security policies, procedures, and guidelines in detail, providing a clear framework for managing system security.
Activity Records	Maintain comprehensive records of all security-related activities and decisions to ensure traceability and accountability.
Accessibility	Ensure that security documentation is accessible to all relevant personnel, promoting security awareness and adherence to best practices.
Review and Update	Regularly review and update security documentation to reflect changes, improvements, and emerging threats, ensuring it remains current and effective.

This table outlines the key activities involved in documentation requirements that highlighting the importance of detailed documentation, comprehensive records, accessibility, and regular updates in maintaining and improving system security.

3.5.3. IEC 62443-4-2 Technical Security Requirements for IACS Components

IEC 62443-4-2 covers detailed technical security requirements for IACS components. This standard focuses on defining security capabilities for individual IACS components, such as controllers, sensors, and communication devices, ensuring the necessary security features to protect against cyber threats. The standard outlines the security capabilities that IACS components should have to mitigate risks and achieve the desired security levels. While IEC 62443-4-2 similarly defined security controls, its scope targeted the individual components as opposed to the systems as done in IEC 62443-3-3.

3.5.3.1. Identification and Authentication Control

Identification and Authentication Control (IAC) is critical for securing Industrial Automation and Control Systems (IACS) components. This control ensures that all entities (human users, software processes, devices) are uniquely identified and authenticated before accessing the system, preventing unauthorized access and protecting against cyber threats. It includes managing user accounts and authenticators, securing the lifecycle of identifiers, and controlling wireless access, ensuring only authorized entities can interact with the system to maintain its integrity and security.

IAC Requirement	Description
IAC-1: Human users identification and authentication	Enforces unique identification and authentication for all human users.
IAC-2: Software process and device identification and authentication	Ensures unique identification and authentication for software processes and devices.
IAC-3: Account management	Controls the creation, use, and deletion of user accounts.
IAC-4: Identifier management	Manages the creation, distribution, and deletion of identifiers.
IAC-5: Authenticator management	Implements mechanisms to manage authenticators (e.g., passwords, tokens).
IAC-6: Wireless access management	Controls and manages wireless access to the IACS.
IAC-7: Permitted actions without identification or authentication	Defines and controls actions that can be performed without identification or authentication.

In conclusion, IAC is essential for maintaining the integrity and security of IACS components by ensuring that only authorized entities can access and interact with the system.

3.5.3.2. Use Control

Identification and Use Control (UC) is essential for managing and regulating the actions of authenticated users and processes within IACS. This control ensures that once entities are authenticated, their activities are closely monitored and restricted to pre-defined permissions, preventing unauthorized use of system resources. It includes mechanisms for session management, such as locking and termination, and controls the execution of actions without prior identification or authentication. By defining and enforcing these controls, UC helps maintain system integrity and prevents potential misuse or exploitation of the IACS.

UC Requirement	Description
UC-1: Session lock	Implements mechanisms to lock sessions after a period of inactivity to prevent unauthorized access.
UC-2: Session termination	Ensures that sessions are terminated after a specified period and/or manually to maintain security.
UC-3: Remote session termination	Provides mechanisms for the remote termination of sessions to enhance control over access.
UC-4: Permitted actions without identification or authentication	Defines and controls actions that can be performed without identification or authentication.
UC-5: Unsuccessful login attempts	Limits the number of unsuccessful login attempts to protect against brute-force attacks.
UC-6: User Controlled policies	Allow users to manage their own access policies within defined security parameters.

These requirements collectively ensure that authenticated entities can only perform authorized actions, thereby protecting the IACS from unauthorized access and potential security breaches.

3.5.3.3. System Integrity

System Integrity (SI) is focused on ensuring the integrity and trustworthiness of Industrial Automation and Control Systems (IACS) components. This control category emphasizes protecting the system from unauthorized modifications and ensuring that all system components operate as intended. It includes measures to verify the integrity of software, firmware, and information, safeguard the boot process, and ensure the authenticity of code and data.

System Integrity (SI)	Description
SI 1	Protect against casual or coincidental manipulation.
SI 2	Protect against manipulation by someone using sophisticated means with moderate resources and IACS-specific skills.
SI 3	Protect against manipulation by someone using sophisticated means with moderate resources and IACS-specific skills.
SI 4	Protect against manipulation by someone using sophisticated means with extended resources and high motivation.

The purpose of ensuring component integrity is to protect against unauthorized manipulation or modification. Components undergo multiple testing cycles, including unit and system testing, before production to ensure they perform as intended. Once operational, asset owners are responsible for maintaining integrity based on risk assessments. Physical asset integrity must be preserved in both operational and non-operational states, such as during production, storage, or maintenance. Similarly, logical asset integrity must be maintained during transit and at rest, such as during network transmission or when residing in a data repository.

These requirements are designed to ensure that the IACS components remain secure, reliable, and resistant to unauthorized modifications, thereby maintaining system integrity and stability of the control system.

3.5.3.4. Data Confidentiality

Data Confidentiality (DC) focuses on protecting sensitive information within Industrial Automation and Control Systems (IACS) from unauthorized access and disclosure. This control category encompasses the implementation of processes and technologies to safeguard data both at rest and in transit. It includes measures such as encryption, secure communication protocols, and stringent access controls to ensure that only authorized entities can access or modify sensitive data.

DC Requirement	Description
DC-1: Information protection processes	Implements processes to protect sensitive information from unauthorized access and disclosure.
DC-2: Protection of stored information	Ensures that stored information is encrypted or otherwise protected to prevent unauthorized access.
DC-3: Protection of transmitted information	Protects information during transmission using secure communication protocols to prevent interception or tampering.
DC-4: Cryptographic key management	Manages cryptographic keys securely to ensure that encryption and decryption processes are effective and protected from compromise.
DC-5: Data integrity during transmission	Ensures that data remains intact and unaltered during transmission between system components.

These requirements are designed to ensure that the IACS components remain secure, reliable, and resistant to unauthorized modifications, thereby maintaining the overall data confidentiality and stability of the control system.

3.5.3.5. Restricted Data Flow

Restricted Data Flow (RDF) is focused on controlling and limiting the flow of data within IACS to prevent unauthorized access and ensure secure communication pathways. This control category involves implementing measures to segment networks, enforce data flow policies, and restrict communication channels to only those necessary for operational purposes which helps to minimize the risk of data breaches, prevent lateral movement by attackers within the network, and ensure authorized access to sensitive information.

RDF Requirement	Description
RDF-1: Network Segmentation	Implements network segmentation to separate critical systems and limit data flow to necessary segments.
RDF-2: Data flow enforcement	Enforces policies and mechanisms to control and restrict data flow within the IACS.
RDF-3: Controlled interfaces	Ensures that interfaces between different network segments are controlled and monitored to prevent unauthorized data flow.
RDF-4: Secure communication channels	Uses secure communication channels to protect data flow between system components.
RDF-5: Data integrity during transmission	Ensures that data remains intact and unaltered during transmission between system components.

These requirements are designed to ensure that the IACS components remain secure, reliable, and resistant to unauthorized modifications, thereby maintaining the overall security and stability of the control system.

3.5.3.6. Timely Response to Events

Timely Response to Events (TRE) is focused on the capability of Industrial Automation and Control Systems (IACS) to detect, respond to, and recover from security incidents and anomalies in a timely manner. This control category encompasses mechanisms for continuous monitoring, logging of security events, and prompt incident response to mitigate potential threats and minimize damage. By ensuring a timely response to security events, TRE helps to maintain the operational integrity and security of IACS, enabling quick identification and addressing of issues before they can escalate into significant security breaches or system failures.

TRE Requirement	Description
TRE-1: Audit Logging	Implements mechanisms for logging security-related events to ensure traceability and accountability.
TRE-2: Continuous monitoring	Continuously monitors the system for security events and anomalies to enable prompt detection and response.
TRE-3: Incident response capability	Establishes and maintains incident response capabilities to address security incidents effectively and efficiently.
TRE-4: Security event detection	Ensures the system is capable of detecting and reporting security events in a timely manner.
TRE-5: Recovery from security events	Implements processes for recovering from security events to restore normal operations swiftly.

These requirements ensure that IACS components are equipped with the necessary tools and processes to detect, respond to, and recover from security incidents, thereby maintaining the resilience and security of the system.

3.5.3.7. Resource Availability

IEC 62443-4-2 outlines the requirements for ensuring the availability of industrial automation and control system (IACS) components against degradation or denial of essential services (DoS). The standard defines four security levels (SLs) to categorize the robustness of components under various conditions. SL 1 ensures reliable operation under normal conditions, preventing DoS from casual or coincidental actions. SL 2 extends this reliability to abnormal conditions, safeguarding against entities with low resources and generic skills. SL 3 further enhances protection to include extreme conditions, defending against entities with moderate resources and IACS-specific skills. Finally, SL 4 provides the highest level of security, ensuring reliable operation under all conditions and preventing DoS from highly motivated entities with extensive resources and specialized skills.

CR Number	RA Requirement	Supplemental Guidance	Requirement Enhancements
CR 7.1	Maintain essential functions during DoS.	Ensure safe operations during DoS.	Mitigate effects of flooding DoS events.
CR 7.2	Limit resource use by security functions.	Prevent lower-priority processes from interfering.	None
CR 7.3	Support backup operations without affecting normal operations.	Ensure recovery from failures or misconfigurations.	Validate integrity of backups before restoration.
CR 7.4	Recover to a secure state after disruption.	Reinstall patches, reestablish configurations, load secure backups.	None
CR 7.6	Support recommended network and security configurations.	Monitor and control configuration changes.	Generate machine-readable security settings report.
CR 7.7	Restrict unnecessary functions, ports, protocols, and services.	Reduce risk by disabling non-essential functions.	None
CR 7.8	Support control system component inventory.	Augment overall component inventory.	None

3.6. SunSpec Cybersecurity Certification Requirements

The **SunSpec Cybersecurity Certification** has identified and organized the cybersecurity requirements in the following main categories considering the software, the device, and authentication aspects [6].

1. **Software Updates/Product Support:** The Distributed Energy Resources (DER) devices must (i) support updating mutable security and operational software components, including the operating system, boot loader, applications, libraries, etc.; (ii) provide a mechanism for users to read the current software version; (iii) support remote updates, communicating with a remote server at least once per day to download and install software updates; (iv) support automated updates to streamline the update process; (v) verify the authenticity and integrity of software updates before installing them; and (vi) meet the same security requirements as remote updates in the case that the DER devices support local updates.

2. **Device Communications:** The DER devices must (i) implement secure communication protocols (TLS 1.2 or higher, IPSec Version 2 or higher, or SSH-2) for all communications accessing the public Internet; and (ii) reject deprecated security technologies identified by NSA and IETF to prevent vulnerabilities.

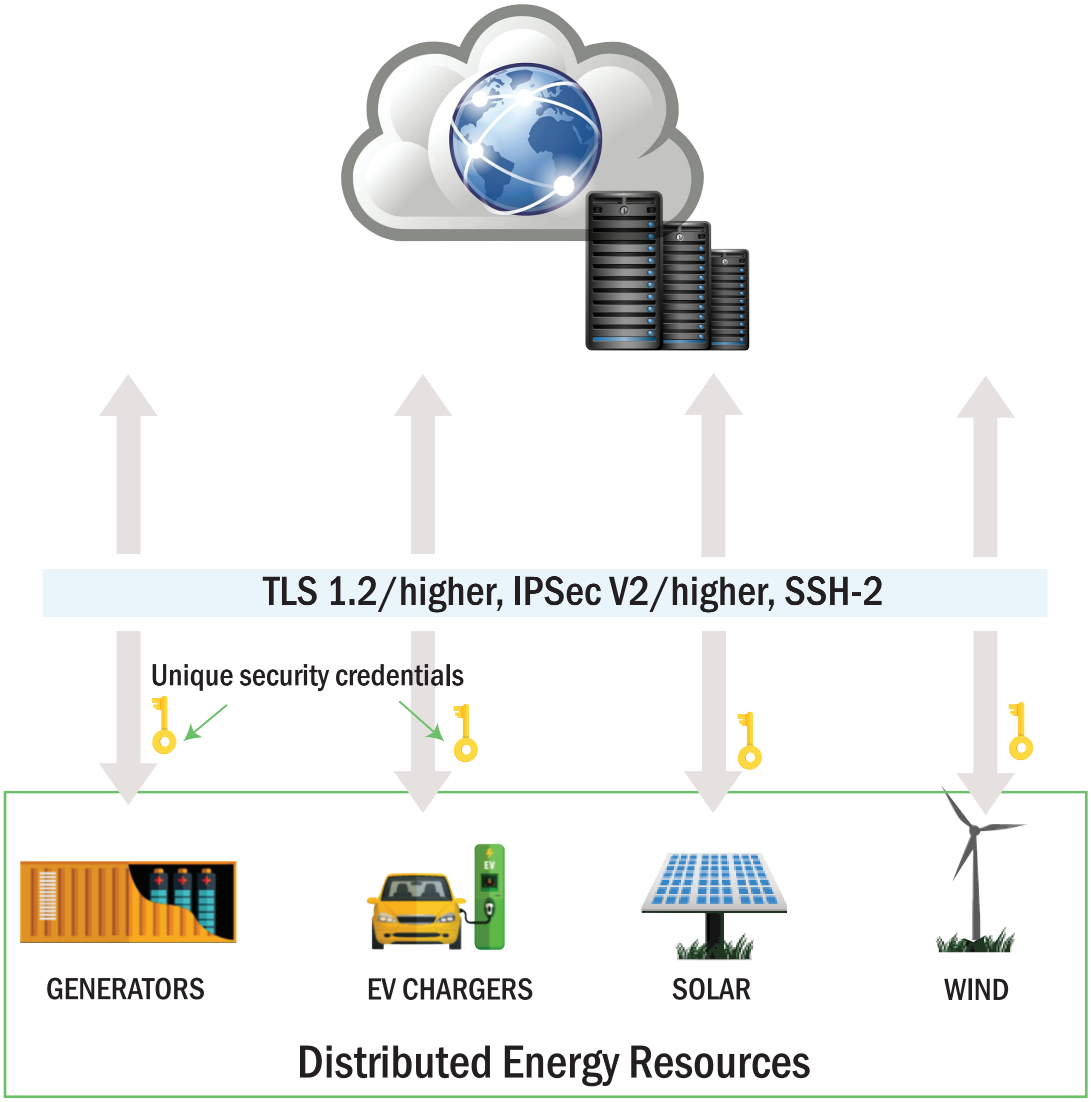

TLS 1.2/higher, IPSec V2/higher, SSH-2
Unique security credentials
GENERATORS
EV CHARGERS
SOLAR
WIND
Distributed Energy Resources

Figure 3-7. SunSpec Cybersecurity Certification Requirements – An Overview.

3. **Authentication:** Regarding the authentication of the DER devices, the SunSpec Alliance (i) requires each user to have unique security credentials for access levels or accounts; (ii) mandates secure authentication mechanisms for all electronic access, locally or remotely; (iii) requires automatic logout after a period of inactivity (iv) allows authorized users to set session timeout periods; (v) enforces strong password requirements or provides a strength meter; (vi) requires users to create new passwords if defaults are shared or displayed; (vii) implements account lockouts after consecutive failed login attempts; (viii) prevents storage or display of unencrypted passwords; and (ix) supports at least one admin account without brute force prevention.

4. **Device Security:** Regarding the device security, the SunSpec Alliance (i) removes or disables unnecessary interfaces and ports before device transfer; and (ii) supports a "factory reset" option for end-of-life or repurposing.

5. **Logging:** The logging requirements include secure storage, timestamps, resolution, accuracy, configuration, security events, remote logs, incident reporting, power setting logs, power cycle logs, and panel logs.

3.6.1. SunSpec Requirements for Test Procedure

The **required equipment and software** to perform tests in accordance with the SunSpec Cybersecurity Certification requirements are [7]:

(i) *IUT (Interface Under Test)* (one or two devices, depending on local software update support, running older software images);

(ii) *endpoints* (devices to exercise communication capabilities, with documentation for modifying security settings);

(iii) *remote log and incident server* (receives and stores log files and incident reports from the DER);

(iv) *remote software update server* (sends software updates to the DER);

(v) *software images* (current, unauthenticated, modified, and old images provided by the manufacturer);

(vi) *documentation* (completed and signed ICS document, product manual, IXIT, and functional specifications)

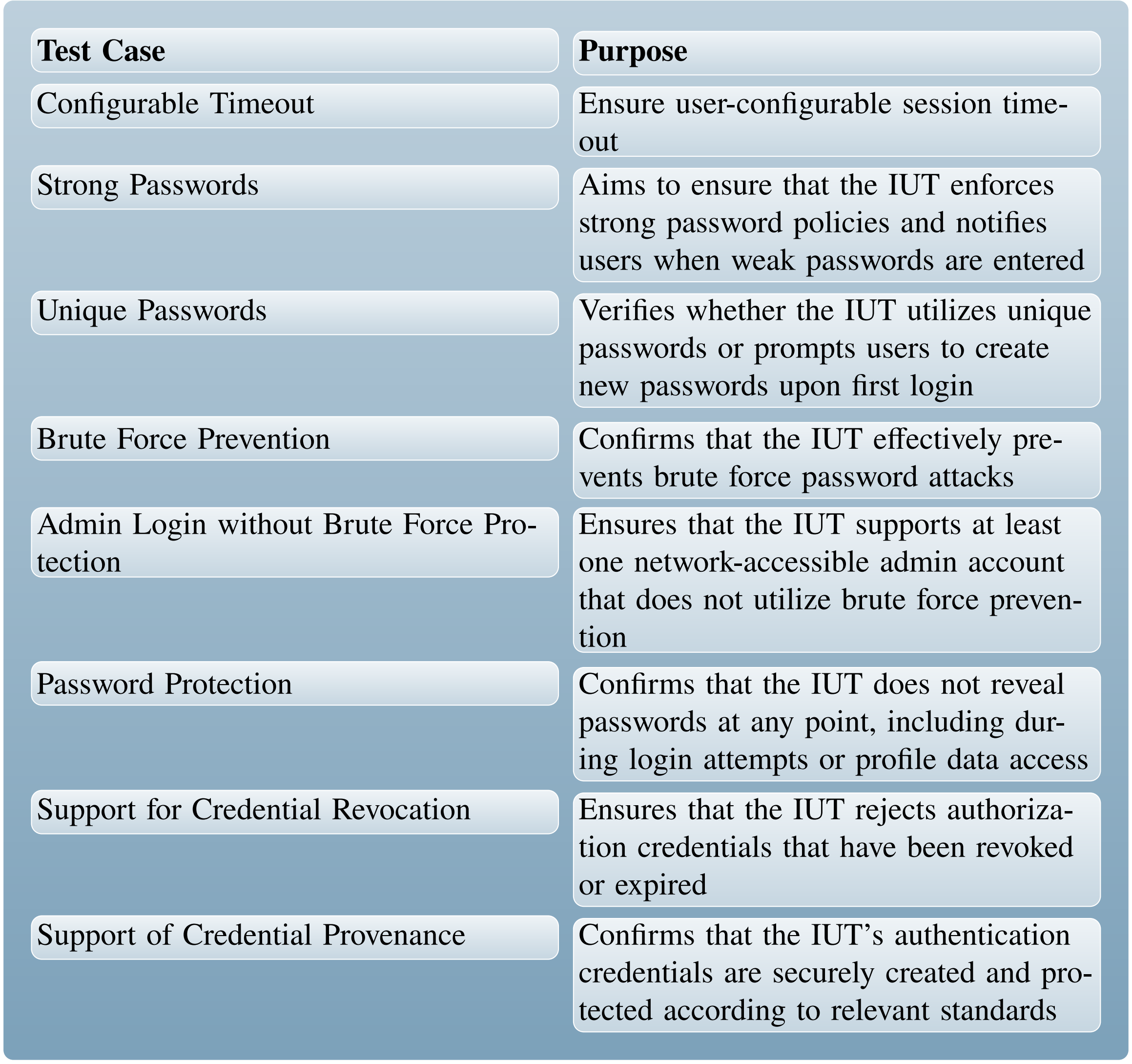
(vii) *network monitoring tools* (traffic monitor, Wi-Fi, Bluetooth, and Ethernet scanners); and

(viii) *secrets* (keys, passwords, tokens for authenticating communications).

The superset test cases that should be validated, along with their purpose, are listed as follows:

Test Case	**Purpose**
Software Version	Verify the IUT can read the version of each component
Secure Updates	Ensure the IUT verifies authenticity and integrity before installing updates
Automatic Remote Updates	Verify support for automatic remote updates
Software Downgrade Prevention	Confirm the IUT rejects updates to older software versions
Secure Update Operations	Optional test to ensure manufacturer maintains secure operations for update processes
Support of Secure Communications	Ensure that all communication capabilities accessible by the public are adequately secured
Communication Downgrade Prevention	Ensure prevention of unsecure protocol usage or downgrade
Minimal Interfaces	Confirm absence of unused interfaces or ports
Support of Secure Boot	Ensure implementation of secure boot
Support of Root of Trust Protection	Verify prevention of root of trust data modification
Support for Root of Trust Extension	Ensure secure extension mechanism for root of trust data
Unique Credentials	Confirm requirement of separate credentials for each user account
Authentication	Ensure authentication of all logical connections, including physical panels
Session Timeout	Confirm timeout of authenticated sessions after inactivity

Table 3-7. Superset test cases that should be validated along with their purpose (part 1).



Test Case	Purpose
Configurable Timeout	Ensure user-configurable session timeout
Strong Passwords	Aims to ensure that the IUT enforces strong password policies and notifies users when weak passwords are entered
Unique Passwords	Verifies whether the IUT utilizes unique passwords or prompts users to create new passwords upon first login
Brute Force Prevention	Confirms that the IUT effectively prevents brute force password attacks
Admin Login without Brute Force Protection	Ensures that the IUT supports at least one network-accessible admin account that does not utilize brute force prevention
Password Protection	Confirms that the IUT does not reveal passwords at any point, including during login attempts or profile data access
Support for Credential Revocation	Ensures that the IUT rejects authorization credentials that have been revoked or expired
Support of Credential Provenance	Confirms that the IUT's authentication credentials are securely created and protected according to relevant standards

Table 3-8. Superset test cases that should be validated along with their purpose (part 2).

3.6.2. SunSpec Requirements SAE J3072 Implementation using the IEEE 2030.5 protocol

This section focuses on the requirements for the implementation of the Society of Automotive Engineers (SAE) J3072 standard using the IEEE 2030.5 protocol. The goal is to support the electric vehicle supply equipment (EVSE) and plug-in electric vehicles (PEVs) manufacturers, and/or operators, and/or system integrators to establish the necessary grid support inverter systems within PEVs connected to electric power systems (EPS) through conductively coupled electric vehicle supply equipment (EVSE). SAE J3072 specifies the necessary technical and performance criteria to ensure safe and effective interaction between the vehicle's inverter system and the power grid in order to enable several functionalities, e.g., vehicle-to-grid (V2G) capabilities [8].

SAE J3072 System Architecture Overview:

- **System Concept:** SAE J3072 defines how the PEVs connect to the EPS via the EVSE using onboard inverter systems. The communication between the PEVs and the EVSEs is managed using the IEEE 2030.5 protocol, which ensures the safe and authorized power discharge from vehicles to the grid.

- **Security Considerations:** The primary security focus is on the communication between PEVs and EVSEs, specifically preventing man-in-the-middle (MITM) attacks. Both the PEV and EVSE must use IEEE 2030.5 compliant certificates and secure HTTPS connections to mitigate these risks. However, due to the point-to-point nature of the physical connection and additional protocols, the likelihood of successful MITM attacks is considered low.

- **Communications Architecture:** The PEV and EVSE communicate over a physical power line communication (PLC) link, utilizing TCP/IP protocols for secure data transfer. Each connection is unique to ensure proper authentication and data integrity.

- **Operations and Compliance:** Upon connection, the PEV identifies and authenticates the EVSE, discovers necessary resources, and exchanges information to receive discharge authorization. This authorization is periodically monitored and managed to ensure the PEV operates within defined limits. If unauthorized activity is detected, the EVSE can revoke discharge permissions and, if necessary, disconnect the PEV.

- **Periodic Operations:** PEVs continuously send operational data to the EVSE, including metrology and status information, ensuring compliance with site-specific limits and discharge authorizations. The communication frequency and data requirements are dynamically managed by the EVSE.

- **Exception Handling:** PEVs operate in a default mode unless explicitly authorized to discharge by the EVSE. Authorization can be withdrawn due to communication failures or other exceptions, prompting the PEV to cease discharging within a specified timeframe. Both PEVs and EVSEs must be capable of handling such scenarios to maintain system integrity.

The main security protocols identified by the SunSpec Alliance in order to implement the SAE J3072 using the IEEE 2030.5 protocol are summarize as follows.

1. **TLS Encryption:** Mutual TLS encryption is mandatory during initial communications to establish a secure connection. Both devices exchange IEEE 2030.5-compliant certificates to authenticate each other.

2. **Device Certificates:** PEV certificates must encode make and model details using Object IDs (OIDs). This information enables the verification of the PEV's authenticity and suitability for connection.

3. **IPv6 Usage:** All communications utilize IPv6, with specific address blocks and stateless address autoconfiguration for secure and unique identification of devices on the network.

4. **Restricted Bridging/Routing:** Initially, the EVSE restricts any bridging or routing of PEV communications to prevent unauthorized network access. Bridging may only be enabled after the successful PEV authorization.

5. **Service Discovery:** Multicast DNS (mDNS) is employed for discovering services on the network, ensuring that devices can locate necessary resources securely without reliance on external DNS servers.

These requirements ensure the secure and authenticated interactions between the EVSE and the PEVs, aiming at securing the data exchange and operational integrity of the electric vehicle charging systems. It is noted that if communication is lost between the PEV and the EVSE, the PEV sends a heartbeat message every second, and the EVSE monitors for these signals. A failure to receive ten consecutive heartbeats prompts the EVSE to stop the PEV from discharging. Therefore, the reception of three consecutive heartbeats restores the connection. Additionally, the EVSE has a gatekeeper function to cut off power if unauthorized or out-of-limit discharging occurs, and can revoke discharge authorization, which the PEV must comply with within three seconds. The SAE J3072 standard also covers coordinated charging/discharging and sleep/wake functions to ensure secure and efficient operations.

The IEEE 2030.5 messages: (i) facilitate the communication between the PEVs and the EVSE, and (ii) ensure secure interactions, i.e., service discovery and resource retrieval. The following cybersecurity requirements need to be considered throughout the communication between the PEVs and the EVSE:

I. **Service Discovery:** The PEVs and EVSEs use mDNS and DNS-SD for the service discovery, and also they establish a secure TLS connection before retrieving the DeviceCapability resources.

II. **Resource Discovery:** The PEVs have access to a wide range of resources, e.g., DeviceCapability, Time, EndDeviceList, and DERList, in order to ensure the secure data exchange.

III. **PEV Gets Site Limits:** The PEVs retrieve site limits from the EVSEs in order to guarantee their compatibility and secure communication.

IV. **PEV Sends Info to EVSE:** The PEVs send information, e.g., Device Information, Power Status, DER Capability, and DER Settings, to the EVSEs in order to guarantee the secure data transmission.

V. **PEV Gets Management Information:** The PEVs retrieve information, e.g., Function Set Assignments, Time, DER Program List, Default DER Control, and DER Control List, in order to guarantee the secure management and operation.

VI. **DERControl Responses:** The EVs send responses to the DERControl commands, in order to indicate the status of the control action. These responses are immediately sent upon receiving the control command.

VII. **Mirror Usage Point Setup:** The EVs post mirror usage point data, including meter readings such as active power, reactive power, voltage, and frequency. These readings are posted periodically and their update rate is determined by the meter usage point configuration.

VIII. **Subscriptions and Notifications:** The EVs subscribe to receive notifications about changes in control commands or system configurations. The charging infrastructure sends notifications to EVs when such changes occur.

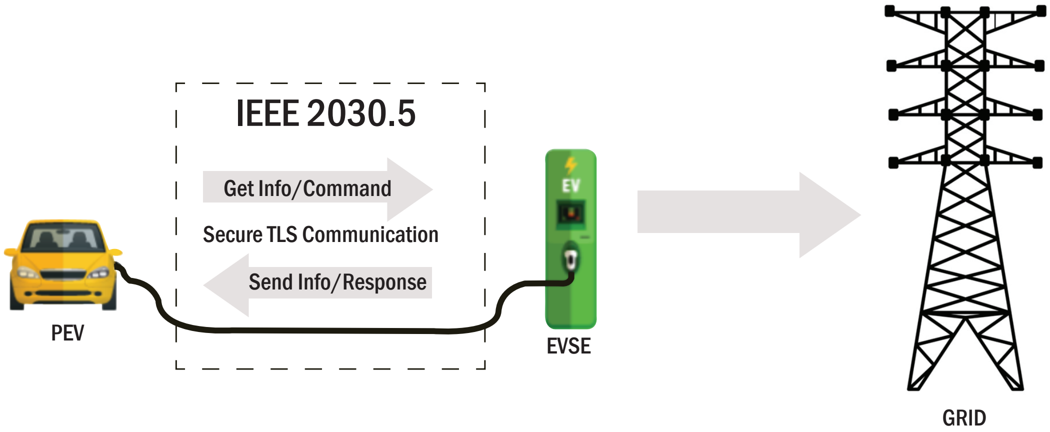


Figure 3-8. PEV and EVSE Interaction following the IEEE 2030.5 protocol.

IX. **Periodic Gets of Information:** The EVs periodically query the charging infrastructure for updates on control commands, meter readings, and system configurations. This allows the EVs to stay synchronized with the charging infrastructure and respond to the changes in a timely and synchronized manner.

X. **Sends Periodic Information:** The periodic information sent by the PEVs includes updates on the DERStatus, PowerStatus, DERAvailability, Meter Readings (i.e., Active Power, Reactive Power, Voltage, and Frequency), which serve as the heartbeat messages for the detection of the loss of communication. Additionally, the PEVs interact with the new DERControl, and they adjust the Active Power limits for the site, and also, coordinate the charging and discharging processes through the DERControl responses.

3.6.3. SunSpec Blockchain Cybersecurity Requirements

The SunSpec Blockchain Work Group proposes a blockchain-based key registry for DER devices to enhance cybersecurity by providing accessible and integrity-protected information about cryptographic keys. This set of cybersecurity standards addresses the current shortcomings in security practices for DERs and ensures their robust protection against cyber threats [9].

A permissioned blockchain architecture is proposed using Byzantine Fault Tolerant (BFT) consensus, with governance structures designed to mitigate security risks, including nation-state threats and coercion. The main components of this architecture include a high-level data model and an API for managing and querying key security information. The main actors involved in the DER service security based on this standard are summarized in Table 3-9, while different use case scenarios where this standard can find applications are presented in Table 3-10.

The proposed standard organizes and secures the key management practices across the energy grid. The primary use case involves the secure management of private/public key pairs for Distributed Energy Resources (DER) devices, facilitated by blockchain technology. The main interactions that take place, include:

- **Authorized Assessor Audit:**

Table 3-9. Main Actors Involved in DER Device Security with Different Colors.

Actor	Description
Manufacturer	Responsible for device manufacturing and key registration on the blockchain.
Authorized Assessor	Independent evaluator of key creation and provisioning processes, auditing device security.
Key Generator	Entity creating and provisioning cryptographic keys into DER devices.
Certificate Authority	Issues digital certificates based on blockchain information to validate DER device identities.
Governing Body	Oversees the blockchain governance, establishing rules and security protocols.
DER Client	Equipment in the DER space using registered keys for secure communications.
DER Server	Web server endpoint managing communications with DER Clients based on key security levels.

Table 3-10. Main Use Case Scenarios.

Use Case Description	Key Features
Manufacturer registers private/public key pairs on blockchain for DER devices.	Secure key creation and provisioning processes.
Authorized Assessor audits and stores evaluation reports on blockchain.	Independent verification of device security measures.
Certificate Authority validates device identities using blockchain information for TLS sessions.	Issuance of digital certificates based on verified device keys.
DER Server makes trust decisions based on blockchain data regarding device security properties.	Secure communication with DER Clients based on certified key security levels.

  - An authorized assessor conducts security audits on key generation, key storage within DER Clients, and key exposure in the manufacturing supply chain.
  - Audit results are stored on the blockchain for transparency and integrity.

- **Key Generation and Provisioning:**
  - The Key Generator creates and provisions private/public key pairs into DER Clients, ensuring adherence to audited processes.
  - Keys can be provisioned during manufacturing or installation, with mechanisms to

securely store and control access to the private key.

- **Manufacturer Responsibilities:**
  - Manufacturers produce DER Clients, ensuring compliance with audited processes for key handling and provisioning.
  - Manufacturers register each device's key on the blockchain, linking it to audited processes and device information.
- **Certificate Authority (CA) Issuance:**
  - CAs issue certificates based on blockchain-verified information, ensuring secure mapping between public keys and device attributes.
  - Certificates are essential for secure TLS sessions between DER Clients and DER Servers, facilitating mutual authentication.
- **DER Server Validation:**
  - DER Servers validate DER Client certificates during TLS handshakes using blockchain data, ensuring the trustworthiness of private key management meets minimum security requirements.

The proposed cybersecurity standard also integrates traditional certificate authority (CA) mechanisms with Blockchain for enhanced security and lifecycle management of DER Clients. To realize the latter, the following main points need to be ensured:

Certificate Creation and Validation:

- A CA issues X.509 certificates containing DER Client public keys and policy parameters.
- Certificates are used for authentication during communication with DER Servers.

Blockchain Integration:

- DER Servers query the Blockchain using extracted key identifiers from certificates.
- Blockchain provides additional cybersecurity information beyond traditional mechanisms like OCSP and CRL.

Key Lifecycle Tracking:

- Lifecycle stages include manufacturing, distribution, installation, and decommissioning.
- Blockchain records ownership transfers, end-of-life events, and key revocations.

Supply Chain Security:

- Involves multiple actors (manufacturers, distributors, installers) ensuring secure key provisioning and ownership transfer.
- Different scenarios (component integration, service provision) affect Blockchain recording requirements.

3.7. ISO 15118-20 Road Vehicles – Vehicle to grid communication Interface – Part 20: Network and application protocol requirements

The ISO 15118-20 standard, which is a part of the ISO 15118 series, outlines communication between electric vehicles (EVs) and electric vehicle supply equipment (EVSE), including both battery electric vehicle (BEV) and plug-in hybrid electric vehicles (PHEVs). Its primary focus is application layer messages supporting electricity power transfer, including bidirectional power transfer (vehicle-to-grid V2G). The standard specifies communication requirements for both conductive and wireless charging, automatic connection devices, and information about charging and control status. The document covers messages, data models, XML/EXI formats, and protocols (V2GTP, TLS, TCP, IPv6) across the 3rd to 7th OSI layers.

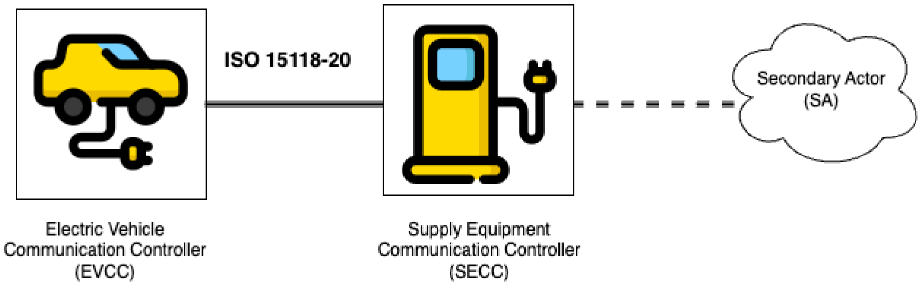

ISO 15118-20
Secondary Actor (SA)
Electric Vehicle Communication Controller (EVCC)
Supply Equipment Communication Controller (SECC)

Figure 3-9. Communication among EVCC, SECC, and SA.

3.7.1. ISO 15118-20: Security Concept

Section 7.3 of the standard defines various security concepts emphasizing the distinct requirements for the Private Supply Equipment Communication Controller (Private SECC) and Supply Equipment Communication Controller (SECC). Transport Layer Security (TLS) is mandated for all communication, ensuring secure data transmission between Electric Vehicle Communication Controllers (EVCCs) and SECCs. The protocol supports both ISO 15118-2 and ISO 15118-20 connection setup processes. While TLS provides fundamental protection, application layer security is enhanced through XML-based signatures for specific messages. TCP/IP communications between peers are safeguarded with mutually authenticated TLS channels. According to the standard, EVCCs may send power profiles to SECCs, which then securely transmit them to Secondary Actors (SAs). Security measures also encompass the initial and ongoing management of contract certificates and keys, and the storage of certificate and message data must comply with relevant privacy regulations at various levels. The security section includes several subsections addressing specific cybersecurity requirements.

Subsection 7.3.2 Certificate and key management

The standard allows various certificates (SECC, Contract, V2G Root CA, Sub-CA, OEM Root CA, and Vehicle Certificates) and supports OEM Provisioning Certificates for managing Contract Certificates. It requires X.509v3 certificates, SHA-512 hashing, ECC with ECDSA, and Ed448 signatures. While multiple cryptographic algorithms are supported, ECC with ECDSA is preferred. The standard ensures proper r- and s-value length, mandates a 521-bit ECC key length,

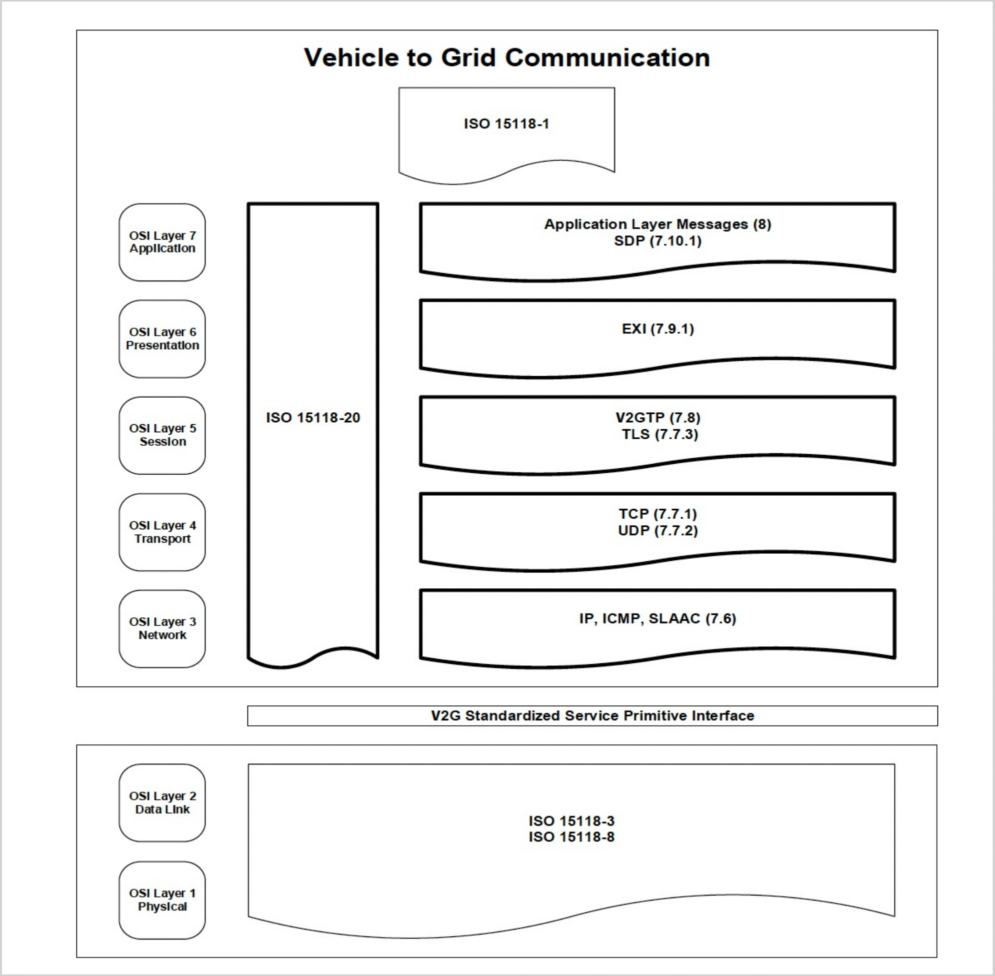


Figure 3-10. Document overview

limits certificate chain length to 3 (4 for cross-certificate chains), and requires certificate validity, validation rules, and result caching for EVCC and SECC. Curve usage is based on configuration.

This subsection also defines certificate structure and requirements, establishing minimum guidelines and compliance with Annex B profiles. It specifies that SECC, OCSP Signer, and CPS Leaf Certificates must use the V2G Root CA for trust, allows Contract Certificates to use either eMSP or V2G Root CA, and mandates that PE Certificates use a PE Private Root CA, prohibiting V2G or eMSP Root CA signing. OCSP Signer Certificates may use either eMSP or V2G Root CA, while Vehicle and OEM Provisioning Certificates can use either OEM or V2G Root CA. PE Certificates allow cross-signing within their chains. SECCs must have an SECC, V2G Root CA, or OEM Root CA Certificate, and EVCCs require a Vehicle Certificate and at least one V2G Root Certificate for TLS sessions. For Plug and Charge (PnC), EVCCs must include or store at least one Contract Certificate, which is optional but must be supported if implemented. Additionally, while Contract Certificate installation via EVSE is optional, it must comply with mandatory requirements if supported, including the need for an OEM Provisioning Certificate and restrictions on CertificateInstallationReq messages if this certificate is absent.

In a private environment, the minimum required certificates are the PE Private Root CA and PE Certificates for establishing TLS sessions in Private SECC. SECC, operating in a public environment, cannot use PE Private Root CA or PE Certificates, and SECC certificates cannot be used in Private SECC.

The standard emphasizes the importance of certificate governance but excludes it from this standard. It defines Certificate Policy (CP) and Certification Practice Statement (CPS) for private key security and identity, requires a robust governance structure for V2G, eMSP, and OEM Root CA certificates, exempts PE Private Root CA certificates from strict governance unless they support PnC, and leaves the implementation of governance structures to industry participants.

7.3.3 Number of root certificates and root validity

The document outlines the storage requirements for Root CA Certificates for SECCs and EVCCs but does not mandate their installation, leaving this decision to CSOs and OEMs. It requires SECCs to store two V2G Root CA Certificates and two OEM Root CA Certificates (both current and future). Private SECCs must store at least one OEM or V2G Root CA Certificate. While the support for local or regional V2G and OEM Root CA Certificates is advised, it is not mandatory. The standard does not define a maximum number of Root CA Certificates, leaving this to the discretion of OEMs and CSOs. It is recommended to consider certificates for new OEMs, and EVCCs are encouraged to store at least one PE Private Root CA Certificate, even though Private Environment support for EVs is not mandatory. Additionally, Root CA Certificates cannot issue leaf certificates outside Private Environments; leaf certificates must be issued by a Sub-CA.

7.3.5 Firewall

The standard defines SECCs and SDP servers as trusted networks controlled by EVSE operators, while EVCCs are defined as untrusted networks. It mandates the use of at least one firewall between the EVCC (untrusted) and SECC (trusted) networks. This firewall acts as a critical barrier, safeguarding the trusted network from potential threats originating from the untrusted network. Additionally, the standard includes a comprehensive table of mandatory firewall rules specifically designed for wireless communication.

Trusted Networks	Untrusted Networks
Supply Equipment Communication Controllers (SECCs)	Electric Vehicles Communication Controllers (EVCCs)
SDP servers	

Table 3-11. Trusted vs. Untrusted networks

7.3.6 Protection of the cryptographic keys

The ISO 15118-20 standard advocates for cryptographic key protection through a range of methods, from basic microcontroller safeguards to advanced secure boot facilities and Hardware Security Modules (HSMs). It specifically recommends the use of HSMs due to their resistance to physical attacks and their ability to perform secure key operations. Additionally, the standard suggests employing a Trusted Platform Module (TPM) 2.0 for its robust security features. However, it's important to note that these recommendations are advisory rather than mandatory.

The table below provides recommendations for protecting cryptographic keys.

V2G Entity	Recommendation
EVCC	Recommends integrating HSM in EVCCs as either a separate physical unit or embedded microcontroller, ensuring secure key operations such as encryption, decryption, and signature verification. TPMs are also acceptable.
Public SECC	Protection methods are the same as for EVCCs.
Private SECC	Protection methods for EVCCs should be considered. The standard encourages adherence to public environment security standards, with mandatory compliance specifically required for Contract Certificates in Plug and Charge (PnC) support.

Table 3-12. Protection of cryptographic keys

7.3.7 Random number generation (RNG)

The standard requires cryptographically secure random number generation for nonce, AES-GCM initialization vectors, PnC challenges, and TLS session negotiation. It mandates state-of-the-art RNG for V2G entities and defines two types:

- **Deterministic Random Bit Generator (DRBG)**: Fast, seed-based, used in cryptographic applications.

- **Non-Deterministic Random Bit Generator (NRBG)**: Slower, entropy-based, used to seed DRBG.

The document also ensures entropy for DRBG re-seeding, mandates single-use of random numbers, and specifies best practices, including:

- Use only by the intended process

- Erasure of seeds after use

- Regular DRBG reseeding (every 24 hours or at power-up)

- Minimum entropy requirement of 0.90 bits per bit generated, equating to 116 bits of entropy in a 128-bit random number

3.7.2. ISO 15118-20: Other Relevant Sections

Subsections outside the security concept section also address important security requirements. Thus, Section 7.4 outlines fundamental processes for V2G communication beyond the data link layer, without detailed implementation specifics. It includes key states for V2G communication between EVCC and SECC:

- IP address assignment
- SECC discovery
- TCP/TLS connection establishment
- V2G communication session
- TCP/TLS connection termination

Section 7.5 addresses the requirements for **the data link layer**. It mandates compliance with ISO 15118-3 for power line communications (PLC) and ISO 15118-8 for WLAN communications between V2G entities. It optionally refers to IEEE 802.1X for enhancing WLAN security. This section also details optional security mechanisms for the data link layer, recommending Extensible Authentication Protocol (EAP) for both wireless and wired media, and discusses RFCs for Remote Authentication Dial-In User Service (RADIUS) if used. Secure WLAN connection setups are illustrated, advising the use of RADIUS for encrypted channels and recommending WPA3-Enterprise or WPA2-Enterprise for wireless connections. Specific connection rules and authentication processes between V2G entities are provided, along with requirements for cipher suites, elliptic curves, ECDHE, and signature algorithms for EAP.

Section 7.6 outlines **the network link layer** specifications based on IPv6, referencing IETF RFC 8200. It details protocol parameters, including IPv6 support and requirements, and prohibits the use of IPsec due to the adoption of TLS 1.3 in ISO 15118-20. The section mandates path MTU discovery and the handling of IP fragments, forbids IP fragmentation between EVCCs and SECCs, and specifies header values for packets. It also discusses the optional use of DHCPv6, along with IPv6 node requirements and the Neighbor Discovery Protocol (NDP) for assigning unique IP addresses. Additionally, it requires the implementation of the Internet Control Message Protocol (ICMP) and provides a table of relevant RFCs for ICMP message types.

Furthermore, Section 7.6 outlines the IP addressing requirements for communication between EVCCs and SECCs over IP networks. It covers the retrieval of valid IP addresses, including both link-local and global addresses, mandates that EVCCs support Stateless Auto Address Configuration (SLAAC), and references various IETF RFCs for detailed rules. It also specifies criteria for address selection when multiple IPv6 addresses are supported.

Section 7.7 covers **transport layer** requirements for V2G entities. It mandates the implementation of Transmission Control Protocol (TCP) according to IETF RFC 793 and recommends additional congestion control and retransmission algorithms, as well as checksum algorithms from RFC 1624 and RFC 2018. For User Diagram Protocol (UDP), it requires implementation in accordance with IETF RFC 768. Additionally, the ISO 15118-20 standard includes a comprehensive subsection dedicated to transport layer security.

7.7.3 Transport layer security (TLS)

Subsection 7.7.3 details the use of Transport Layer Security (TLS) for establishing authenticated and encrypted channels between the EVCC and SECC, ensuring mutual authentication. It specifies that SECCs must provide a certificate chain and Online Certificate Status Protocol (OCSP) responses for EVCC verification, with Private SECCs using PE Certificates. EVCCs are authenticated by SECCs through Vehicle Certificates, with verification carried out via certificate chains and revocation checks using OCSP or Certificate Revocation Lists (CRLs). The section mandates support for TLS 1.3 per IETF RFC 8446, but allows for TLS 1.2 to ensure compatibility. Additionally, it requires that random numbers and session keys used in TLS meet the criteria specified in 7.3.7 and 7.3.6.

TLS Usage

The standard mandates that the EVCC acts as a TLS client, initiating sessions with a ‘ClientHello’ message and withholding application data until the handshake is complete. The ‘ClientHello’ must include a nonce with at least 231 bits of entropy and specify supported versions as ’0x0304’. For Certificate Provisioning Mode for Private Environment (CPM4PE) activation, secure methods must be used, and sessions should expire after at least 120 seconds. The EVCC is required to list V2G Root CA and PE Private Root CA Certificates in the ’certificate_authorities’ extension. It must manage the "authorities" element in ‘ClientHello’ messages in accordance with IETF RFC 8446 and include a "status_request" along with a zero-length "responder_id_list" fields in messages to the SECC.

The SECC must always function as a TLS server, refraining from sending application data until the TLS handshake with the EVCC is complete. Private SECCs supporting CPM4PE must ensure a secure user activation method and have CPM expire at least 120 seconds after activation. Public SECCs are required to include their certificate chain in ’ServerHello’ messages, based on either EVCC-provided ots or self-chosen roots. If the EVCC provides roots, the Public SECC must select a certificate chain from the "DistinguishedNames" provided in the ‘ClientHello’ message. Private SECCs not using CPM4PE should also include their PE Certificate chain in ‘ServerHello’ messages. If CPM4PE is used, they must include both their PE Certificate and PE Private Root CA Certificate. Both Public and Private SECCs must select certificate chains based on EVCC-provided "DistinguishedNames" when EVCC roots are specified.

For TLS usage, SECCs must include OCSP responses for each certificate in their chain within ‘ServerHello’ messages, utilizing the "status_request" extension. OCSP responses should include the responder’s certificate chain if it is not signed by the issuing CA. Public SECCs use V2G Root CA Certificates, while Private SECCs use PE Private Root CA Certificates. SECCs are required to omit unsupported OCSP responses and, if not supporting PnC, can disregard the "status_request" extension and operate offline. Public SECCs must provide a valid certificate chain leading to a root indicated by the EVCC during the TLS handshake. SECCs are also required to request the EVCC’s certificate for mutual authentication, provide a list of Root CA Certificates, and ensure the structure of “DistinguishedNames” filed is correctly followed. If no Root Certificates are available, the "authorities" element should be left empty for Public SECCs and Private SECCs not using CPM4PE.

According to ISO 15118-20, EVCCs are advised to discard outdated certificates and must validate the revocation status of certificate chains, contacting OCSP as needed. They must verify the OCSP responder’s certificate and signature, and treat the entire chain as invalid if the status is not “good.” While EVCCs can proceed with PE Certificate validation even if OCSP responses are not provided, they must store a validated PE Private Root CA Certificate in CPM4PE. Out-of-band validation is required for non-trusted chains, and TLS sessions must be aborted if validation fails. Additionally, EVCCs must send their certificate chain in response to a “CertificateRequest.”

Public and Private SECCs are required to validate the EVCC certificate chain during TLS, using OCSP or CRL for revocation checks. Both types of SECCs must consider the Vehicle Certificate chain invalid if the status is not “good.” Private SECCs with PnC support must check the revocation status, while non-PnC SECCs can skip this step. SECCs must perform out-of-band validation for non-trusted chains using Server-Based Certificate Validation Protocol (SCVP), and any validation failure requires aborting the TLS session. Also, Private SECCs in CPM4PE must store the validated Root CA for TLS and ensure that CPM4PE expires after installations.

The clause specifies the requirements for vehicle certificate revocation checks using both OCSP and CRL methods. For **OCSP checks**, responses must be updated weekly and include the responder’s certificate chain up to the root, with the AuthorityInfoAccess extension, except for the OCSP Signer and root certificates. SECCs must ensure that OCSP responses are signed by a trusted Root Certificate and verify both the OCSP responder’s certificate and its signature. For **CRL checks**, CRLs must also be updated weekly and include the issuer’s certificate chain up to, but not including, the root, with CRLDistributionPoints extensions. CRLs received must be signed by a certificate derived from supported Root Certificates, and SECCs must verify both the CRL issuer’s certificate and its signature. Failure to meet these requirements renders the Vehicle Certificate chain invalid.

TLS Credentials and Cipher Suites

The ISO 15118-20 standard outlines specific requirements for transport layer security credentials and cipher suites. Both SECC and EVCC must support and list cipher suites and named groups in the specified order, with the SECC selecting the preferred cipher suite from the ‘ClientHello’ message. Both entities must prioritize named groups, such as ’secp521’ or ’x448,’ and include supported named groups and signature algorithms in their respective TLS messages. The SECC should prefer the most supported signature algorithm from the ‘ClientHello’ message. Furthermore, both SECC and EVCC must support pre-shared key exchange modes and use them for resuming TLS sessions.

TLS Session Setup, Resumption, and Termination

The clause provides general details for setting up a TLS session between the EVCC and SECC:

- Full-handshake TLS, excluding Value Added Services (VAS) communications
- Use of TLS 1.3
- CPM4PE must expire on the EVCC and Private SECC if the respective root certificates are not received after the TLS session is established

For Value Added Service (VAS) communication, each VAS must be offered through dedicated ports, with the SECC configuring firewalls to permit access. Both full-handshake and resumed TLS are allowed for VAS, with resumption based on the TLS context from the V2G session. If TLS resumption is supported, the SECC must issue a separate TLS session ticket for each VAS. If resumption is not supported, the EVCC is required to establish a new TLS session for each VAS.

For VAS communication, TLS session resumption is supported but does not apply to V2G communications, which must use full-handshake TLS. Sessions must be closed and resumed using session tickets according to IETF RFC 8446. Zero-RTT (Zero Round-Trip Time), which allows data to be sent before the TLS handshake is complete, is prohibited to prevent replay attacks. The SECC can send up to eight distinct ‘NewSessionTicket’ messages for VAS, each linked to the same V2G session. Each ticket must contain a nonce with at least 7 bits of entropy and have a lifetime between 20 seconds and 24 hours. The SECC must follow these guidelines for all full-handshake sessions, updating tickets before expiration and ceasing updates after 7 days from the last full handshake. The SECC should not use the “early_data” extension and must securely handle and discard session ticket data. The EVCC must verify the ‘ticket_lifetime,’ reject invalid tickets, and securely store valid ones, using only one ‘PskIdentity’ per ‘NewSessionTicket.’ If no active TLS session exists, the SECC must establish a full handshake session instead.

For TLS session termination, both EVCC and SECC must irretrievably erase all cryptographic data if a TLS session ends due to the termination of a VAS session or if a V2G session is paused. Upon the termination of a V2G session, all associated TLS sessions must also be terminated, and all cryptographic data must be erased.

TLS Compatibility

ISO 15118-20 requires that for TLS backward compatibility, both EVCC and SECC adhere to ISO 15118-2 specifications, supporting the relevant certificate profiles, cipher suites, and extensions. The EVCC should include ISO 15118-2 cipher suites and extensions in the ‘ClientHello’ message, and the SECC must support these. For TLS 1.2 and 1.3 setups, the EVCC must use version 0x0303 in the supported_versions extension; failing to do so will result in the SECC defaulting to TLS 1.2. If the SECC selects TLS 1.2, the EVCC must proceed with a TLS 1.2 handshake. Additionally, if the supported_versions extension is absent or set to 0x0303, the SECC must handle TLS 1.2. Legacy connections should not request the EVCC’s certificate, and the EVCC must abort the session if a downgrade is detected. If the EVCC and SECC do not support compatible TLS versions, the TLS session setup will fail, leading both parties to abort the process.

Subsection 7.8 V2G transfer protocol

According to ISO 15118-20, the V2G Transfer Protocol (V2GTP) sets the standard for communication between EVCC and SECC, and it can also be used by other V2G entities. It utilizes TLS and TCP over IP addresses and port numbers for bidirectional data exchange, specifying particular ports for source and destination communication. The EVCC must connect using the source port V2G_SRC_TCP_DATA, while the SECC provides the destination port V2G_DST_TCP_DATA and adheres to the port specified in the last SECC discovery response. The V2GTP defines a detailed Protocol Data Unit (PDU) structure, which includes mandatory header and payload configurations. The protocol also outlines the processing sequence for headers and mandates that messages with incorrect header data be ignored.

3.8. ANSI Roadmap

The ANSI Roadmap is a comprehensive deep dive into the charging infrastructure of electric vehicles. The Roadmap covers all standards that pertain to EVs and is an effort to create a comprehensive evaluation of standards for the US. "It identifies key safety, performance, and interoperability issues, notes relevant published and in-development standards, and makes recommendations to address gaps in codes and standards"[10]. It has defined ‘gap’ to mean a lack of coverage by standards. And has determined that the gaps found in this research at this time needs no further current work but may need to be addressed in the future and state, “As a result of constantly evolving cybersecurity threats, there is a need to encourage minimum cybersecurity redundancy and resiliency within the EV charging ecosystem. This would include retention of a minimum level of functionality and communication under any circumstances and could include implementation of mechanisms such as phase change materials”[10].

3.8.1. ANSI Roadmap of Standards and Codes for Electric Vehicles at Scale

The ANSI document covers all regulated areas of EVs with chapters dedicated to vehicle systems, charging infrastructure, grid integration, and cybersecurity. The portion of this document that is reviewed here is the cybersecurity section. Below lists the gaps in this area as determined by this document.
The gaps listed in the document are[10]:

- **"Gap S1: Comprehensive review of cybersecurity codes and standards for applicability to the EV charging ecosystem.** Gaps should be identified and prioritized.

- **Gap S2: The lack of an end-to-end secure trust chain and encryption system for the EV charging ecosystem.** This results from the use of different protocols and data transfer mechanisms between EV charging related systems. An entity trust chain is needed across all elements of the EV charging ecosystem incorporating a comprehensive public key infrastructure (PKI).

- **Gap S3: Cybersecurity and Data Privacy.** Due to the nature of cybersecurity, the interactions of systems, and the emerging threats environment, there is an ongoing need for guidelines and standards to address cybersecurity and data privacy concerns specific to EVs and smart grid communications. Architectures should be designed with cybersecurity in mind.

- **Gap S4: Robust "Security-by-Design."** Security-by-Design is needed for equipment and systems throughout the EV charging ecosystem.

- **Gap S5: Digital Cybersecurity as Part of Interconnection Standards.** Cybersecurity threats exist at the power system point of interconnection. The digital interconnection could be compromised which may affect the electrical interconnection. Presently, there appears to be no standards requirements nor other guidance for utilities to address digital cybersecurity challenges.

- **Gap S6: Cybersecurity of Power Management under DER Aggregation Scenarios.** Cybersecurity gaps exist with regard to aggregation of DERs for Grid Services and subsequent power management.

- **Gap S7: Cybersecure Firmware and Software Updates.** Cybersecurity posture, unlike safety, diminishes over time as the threat landscape evolves and new vulnerabilities are uncovered. Therefore, updating/patching of software is absolutely paramount to maintain good cybersecurity for the lifetime of vehicles.

- **Gap S8: EVSE Cyber-physical Vulnerabilities.** EVSE have physical vulnerabilities that can serve as threat vectors and cascade to cybersecurity high consequence events."

The Roadmap discusses some approaches that are useful for closing gaps, such as risk assessments and actively addressing the higher risks in systems. Additionally, devising and implementing a cybersecurity strategy that includes a layered approach that would strengthen the system as a whole. This method "combines technical, organizational, and procedural measures," [10]. Each gap is also given a low, medium, or high level of priority, whether R&D is thought to be needed, recommendations for remediation, and which organizations would be best suited to work toward solutions. This paper is addressing the first gap and is labeled as a high concern by the Roadmap.

3.9. State Requirements

The National Electric Vehicle Infrastructure (NEVI) Formula Program was enacted November 2021 to fund up to 80% of project costs for increasing electric vehicle charging (EV) station accessibility and reliability across the nation. There are three key points of the 2024 update to the NEVI Formula Program Guidance, detailing the requirements and processes for states to receive funding for EV charging infrastructure.

1. Purpose and Background:

   The NEVI Formula Program is part of the Bipartisan Infrastructure Law (BIL) and is designed to fund the deployment of EV charging infrastructure across the United States. The program aims to create a convenient, affordable, reliable, and equitable national network of EV chargers.

2. Program Requirements:

   States must submit an EV Infrastructure Deployment Plan annually, detailing how they intend to use the allocated funds. The guidance outlines minimum standards for EV chargers, including technical specifications, reliability, payment methods, data submission, and workforce qualifications.

3. Funding and Deadlines:

   States need to submit updated plans to the Joint Office of Energy and Transportation by specific deadlines to receive funding for the following fiscal year. The guidance also discusses funding distribution, federal share, and state/local match requirements.

Cybersecurity Requirements
The document mentions specific requirements under the National Electric Vehicle Infrastructure Standards and Requirements, including aspects like network connectivity and interoperability of EV charging infrastructure. However, there is no explicit mention of detailed cybersecurity measures or requirements. The focus is more on technical and operational standards rather than cybersecurity specifics.

The updated requirements include the condition that receiving funds means that the state also adheres to the Title 23 CFR 680. Under this Code, 680.106, 680.108, 680.112, and 680.114 are dealing with cybersecurity aspects. There are 50 Titles under the Code of Federal Regulations. This is the codification for federal agencies in the US. The 50 Titles are the 50 general areas that are regulated by the Federal Government. Title 23 contains the codes for highways and Chapter I is the Federal Highway Administration, under the Department of Transportation (DOT). Subchapter G is the Engineering and Traffic Operations and Part 680 is the NEVI Standards and Requirements.

4. IDENTIFIED GAPS

The NIST Cybersecurity Framework (CSF) was used as a baseline for understanding where gaps may have existed in the previously reviewed standards. The analysis was performed on the standards and evaluated based on the provided matrix in Figure 4-3. Table 4-1 below shows the overall outcomes of the gap analyses for all standards reviewed for reference. This helps to view the gaps between the standards as well as where the standards fall with respect to the NIST CSF.

A summary of the results of the gap analysis is provided along with Table 4-1. In the gap analysis, Table 4-1, below, has the same Category subtitles along with the color-coded cells that visualize the outcomes of each standard's gap analysis results. The matrix (Fig 4-3) guided the color coding and the two-letter code within each cell of Table 4-1.

It is also important to note that the gap analysis was done for product standards against NIST CSF which is aligned to an organizational framework. This has affected the gap analysis and is taken into consideration.

4.1. NIST CSF Profile

The NIST Cybersecurity Framework (CSF) was initiated by DOE and EPRI to advance the capabilities for managing organizational cybersecurity risks. "The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes" [11]. Within the NIST CSF, there is the core, organizational profiles, and tiers which together comprise the CSF structure as seen in Figure 4.1. The core structure outlines the breakdown by Function, Category, and Subcategory. The Categories are a subset of the Functions and Subcategories a subset of the Categories. The Categories are listed in Figure 4-2. These are the same Categories that are used in Table 4-1 in section 4-2 for the gap analysis.

The gap analysis done by the team utilized the NIST CSF Categories and Subcategories to evaluate whether or not each standard had corresponding features that mapped to the NIST CSF. The process used this framework consisting of the five functions approach: Identify, Protect, Detect, Respond, and Recover and worked through each subcategory of these Functions to identify where the standards Addressed, Insufficiently Addressed, or did Not Address the NIST CSF subcategory. Following this section are the results of the analysis for each previously reviewed standard using this NIST CSF as a comparison.

The following section (4.2) identifies gaps by standard as mapped to the NIST CSF version 2.0.

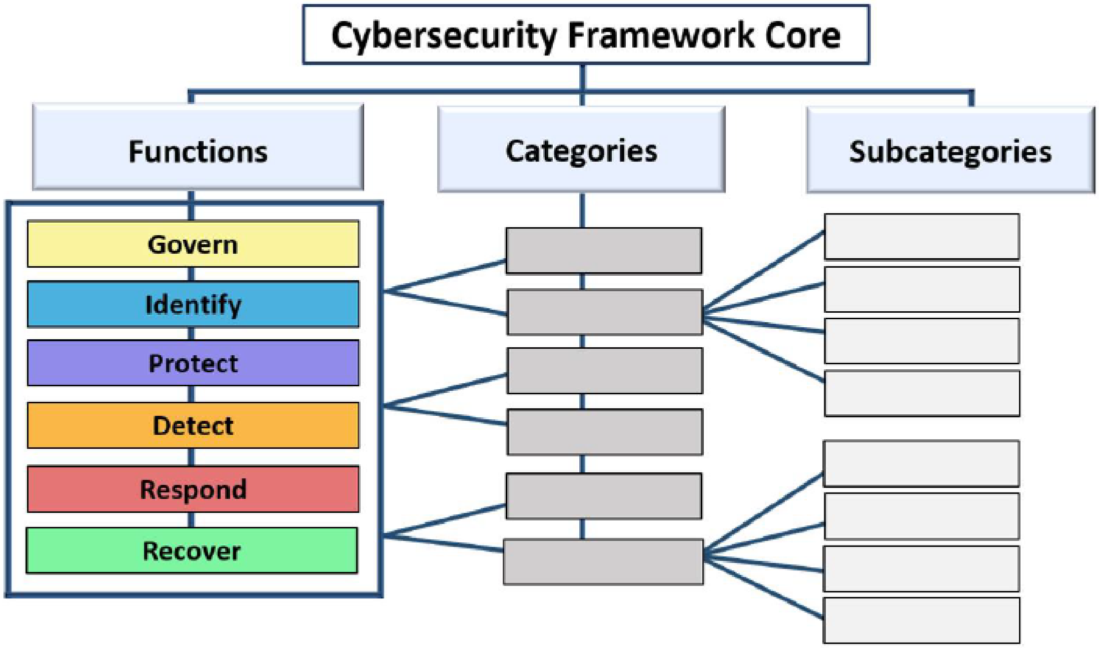
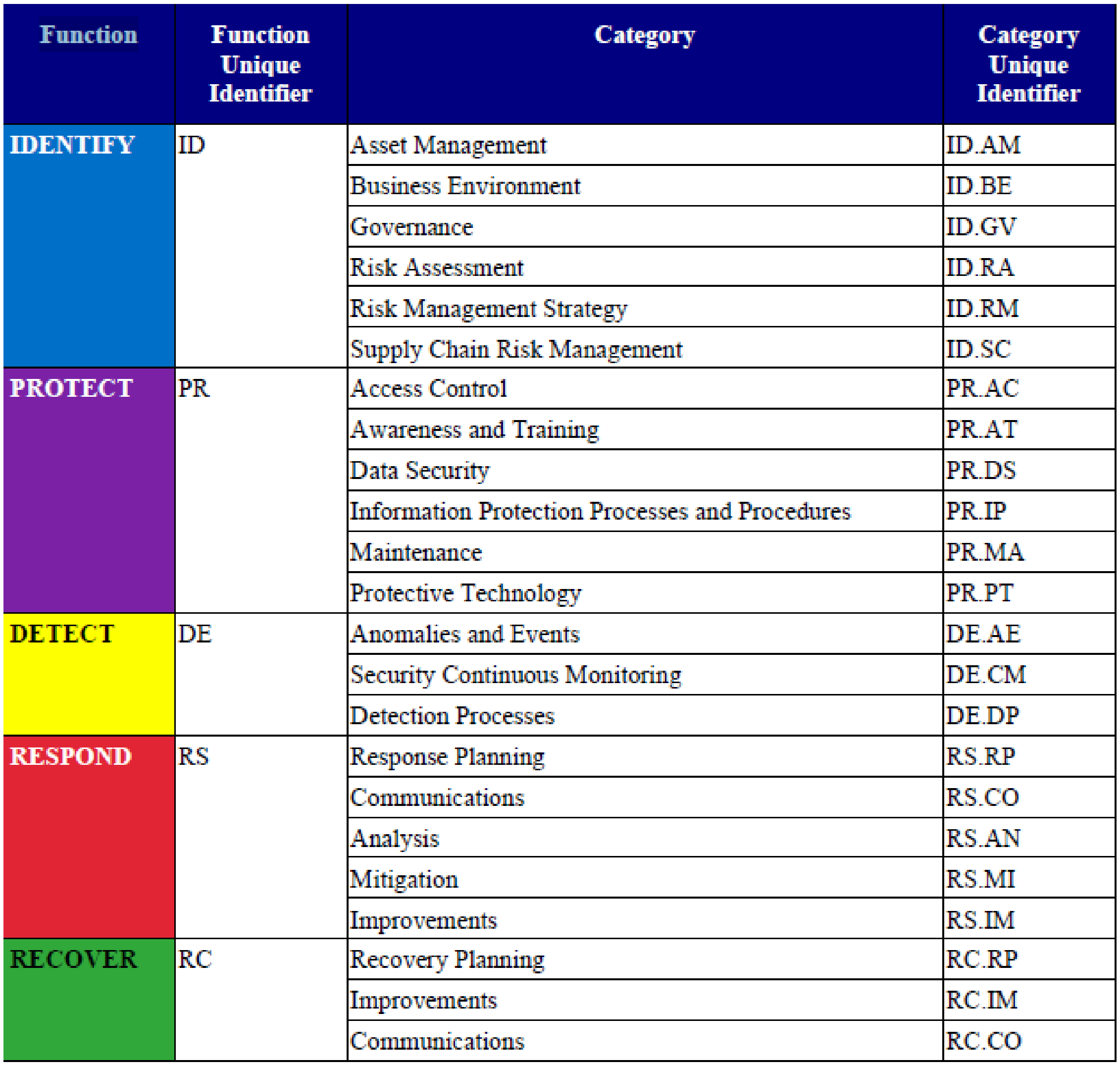


Figure 4-1. NIST CSF Core Structure.

4.2. Identified Gaps

- The **UL 2941** standard outlines the minimum cybersecurity requirements that inverter-based resources (IBR) equipment shall support. The standard includes requirements in the following categories: Access Control, Cryptography, Sensitive Data Management, Security Management, Risk Management, Documentation, Monitoring, Logging, Product Management, Time Synchronization, and Physical Anti Tamper. The standard is mainly focused on cybersecurity requirements in the areas listed above and does not contain the methods of validation of these requirements, requirements regarding functional testing of a product, or requirements regarding the hardware components contained in a product.
  The gap analysis for UL 2941 shows that UL 2941 does not address, or insufficiently addresses most of NIST CSF. Only Identity Management, Authentication, and Access Control (PR.AA) is fully addressed in UL 2941 because the standard more focuses on requirements for inverter-based resources equipment rather than organizational practices. Specifically, the standard insufficiently address the categories in Govern, Identity, and Detect, and does not address the categories in Response and Recover in NIST CSF. In Govern, the standard has a section for Risk Management, which partly addresses risk management category but UL 2941 does not address the other categories in Govern. One solution to address this gap is the extension of the standard or complementing it with the existing or new standards. Only some parts of asset management and risk management categories of Identify in NIST CSF are addressed in Documentation section and Risk Management section of UL 2941, respectively. Improvement category is not addressed in UL 2941. The gaps in subcategories in Asset Management can be filled by addressing them in extension of Documentation section of UL 2941. This same resolution can be used for the gaps in Risk Management category in Identify. The entire Improvement category in Identify is not addressed in UL 2941 and



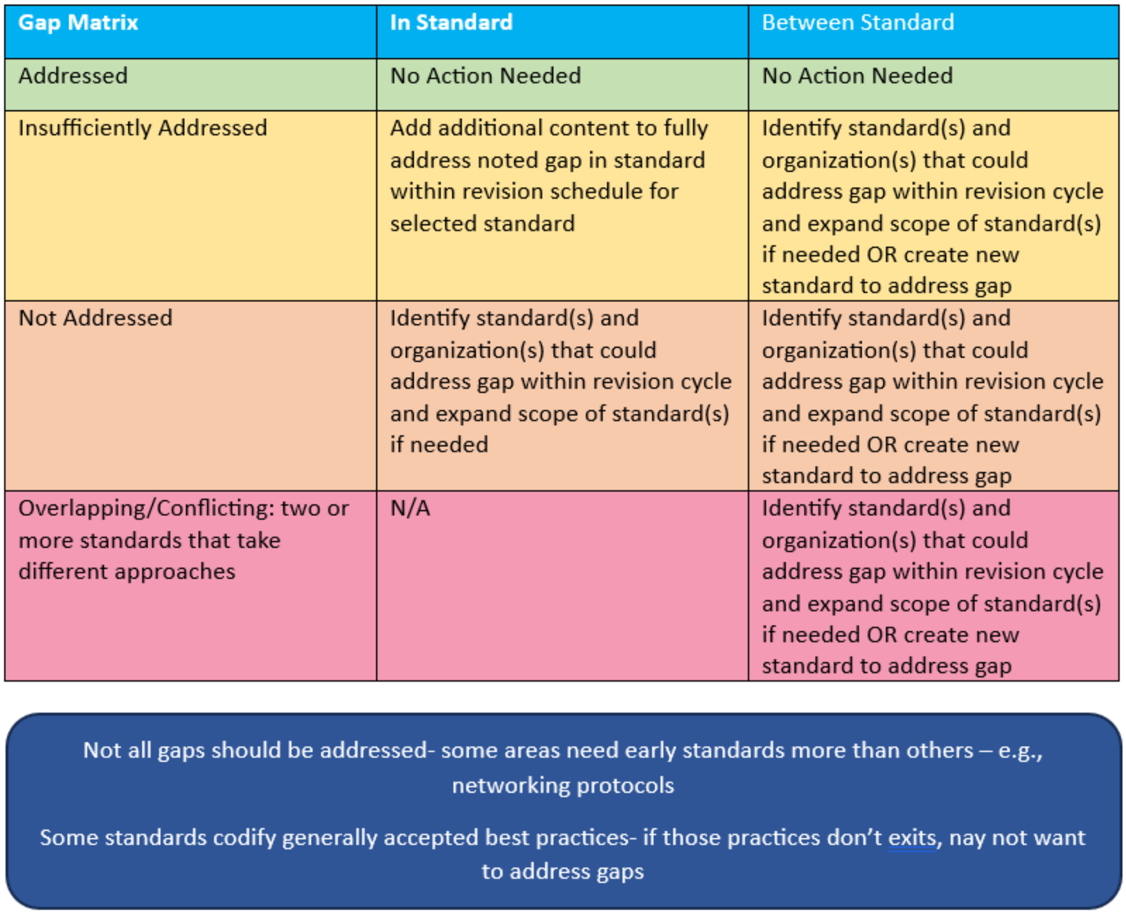
Function	Function Unique Identifier	Category	Category Unique Identifier
IDENTIFY	ID	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PROTECT	PR	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes and Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
DETECT	DE	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
RESPOND	RS	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
RECOVER	RC	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

oi

Figure 4-2. NIST CSF Core Structure.

the category is not within the scope of UL 2941, thus this gap should be filled by other standards. Awareness and Training (PR.AT) and Technology Infrastructure Resilience (PR.IR) categories in Protect are not addressed in UL 2941 and these are not within the scope of the standard either. Thus, these gaps should be filled by other standards. Gap analysis shows that Continuous Monitoring (DE.CM) category in Detect is partially covered in UL 2941 and these gaps can be filled by the extension of the standard. Response and Recover in NIST CSF are not addressed in UL 2941 because they are not within the scope of the standard. Thus, Response and Recover functions for cybersecurity of inverter-based resources should be addressed in other standards.

- The **UL 2900** standard covers risk management requirements for network-connectable products to ensure vendors of such products follow security best practices for software and security risk controls during integration. As such, the standard offers substantive guidance on risk management and oversight, specifically for governance. In this category, lined up against the NIST CSF, UL 2900 indicates specific tasks for product vendors to delineate the function and security protocols of their products, with significant requests for documentation of design



Gap Matrix	In Standard	Between Standard
Addressed	No Action Needed	No Action Needed
Insufficiently Addressed	Add additional content to fully address noted gap in standard within revision schedule for selected standard	Identify standard(s) and organization(s) that could address gap within revision cycle and expand scope of standard(s) if needed OR create new standard to address gap
Not Addressed	Identify standard(s) and organization(s) that could address gap within revision cycle and expand scope of standard(s) if needed	Identify standard(s) and organization(s) that could address gap within revision cycle and expand scope of standard(s) if needed OR create new standard to address gap
Overlapping/Conflicting: two or more standards that take different approaches	N/A	Identify standard(s) and organization(s) that could address gap within revision cycle and expand scope of standard(s) if needed OR create new standard to address gap

Not all gaps should be addressed- some areas need early standards more than others – e.g., networking protocols

Some standards codify generally accepted best practices- if those practices don't exits, nay not want to address gaps

Figure 4-3. Gap Matrix by Color.

and use. There are also thorough requirements for information to be covered in a product evaluation, including all possible external interfaces for the product and how it manages cybersecurity objectives throughout the lifecycle. The standard also requires vendors to execute a Software Composition Analysis, which can be used to construct a software bill of materials. While there are thorough reporting requirements for software configuration and data protection, the biggest gaps in coverage of UL 2900 appear in the context of cybersecurity incident management, response, and analysis, and further—recovery. The gap analysis determined that UL 2900 covers protocols for the software products to ensure the protection of sensitive data and communications, which is crucial in the context of EVSE. While this awareness of protective measures will enhance a software product's cybersecurity, without sufficient requirements governing incident management, UL 2900 leaves vulnerabilities with latency and safety from cyber risk in the aftermath of a cybersecurity event. One method for addressing this gap is the overlay of requirements from the NIST CSF categories of detection and response to cybersecurity incidents for characterizing the risk, collecting data, and providing sufficient records integrity for the appropriate safety response to be conducted. Another method for addressing gaps in incident response is to overlay requirements for a product vendor with those for end-use supervisors to understand where responsibilities divide in the context of incident response. Under UL 2900 alone, it is not clear if or where the product vendor responsibilities for cybersecurity safety end and where a product user's responsibilities begin, and this may be the natural limits of the standard, or may be a place for future development and growth of incident response requirement specificity.

- The **IEEE 2030.5** standard defines the application layer with TCP/IP for the management of energy resources. The standard includes the ability of managing demand response, load, pricing, as well as managing the generation of distributed assets such as electric vehicles. The protocol is implemented through a REST architecture, secured through the protocol specific public key infrastructure. The standard is technically focused on the implementation of the protocol, for which a lot of the NIST CSF is out of scope for the document.
  The gap analysis reveals that IEEE 2030.5 does not, or only partially addresses the CSF. This is, however, expected as the CSF is more scoped to higher level organizational practices rather than technical implementation. For example, the CSF section continuous monitoring is only partially addressed due to there being potential areas for monitoring logging and the requirement to continually assess your practices, however it does not directly say to conduct any monitoring practices. The same is true for the respond section, where the focus is on analysis and responding to cybersecurity incidents, where the protocol focuses on implementation of security mechanisms.
  The gap analysis in 2030.5 displays gaps in aspects of the CSF relating to organizational governance, and response. 2030.5 is a highly technical standard, focusing on the requirements for implementation of the protocol with the devices. This leads to a lacking area of addressing the response categories of the CSF as the scope of the document does not include responding to cybersecurity scenarios. Additionally, the document lacks addressing key areas such as detection of anomalous behavior or monitoring for external behavior. While the scope of the document remains to be on protocol implementation, the connection between the protocol and detection and monitoring is a gap that may be addressed through extension of the scope or through additional supplemental guidance not within the document. Furthermore, while the protocol does not dictate organizational guidance, there may be a connection between roles and responsibilities within an organization interacting with the protocol for which it may benefit to have clear guidance on.

- **IEEE 1547-2018** defines interconnection and interoperability requirements for Distributed Energy Resources (DER) connected to the Electric Power System (EPS). IEEE 1547.3 has a scope for providing guidelines for cybersecurity of DERs interconnecting with EPS. The scope is limited to local DER interface between individual DER assets and network equipment. Internal or inter-DER communication is out-of-scope for IEEE 1547.3 and so is external communications with entities such as DER Management Systems (DERMS), aggregators, and utility network operators. Effective cybersecurity requires to be end-to-end in order to protect and manage the secure transmission and distribution of power. IEEE 1547.3 describes DER stakeholders and maps roles and responsibilities to NIST CSF categories of Identify, Detect, Protect, Respond, and Recover but insufficiently maps several of these categories. Gaps also include the 'Govern' category since NIST CSF was update after IEEE 1547.3 was released. Generally, IEEE 1547.3 covers risk assessment and management, communication and network security, access control, data security, and other security management controls. It also describes testing and commissioning for cybersecurity and conformance that highlights recommendations for DER lifecycle.

Due to the technical scope of 1547.3 being focused more on the interconnection and devices, there exist gaps in the mappings to the CSF. There exist gaps in addressing the governance aspects of the CSF, as it is a newer addition to the CSF. 1547.3, when it was under edits, did a similar mapping exercise to the CSF in its previous version. In the current version of the CSF, there exist many areas of which there are gaps in the standard. Particularly, where there are organizational aspects of the standard. The standard does address aspects of risk assessment and management of the device itself, however there is a lacking area in connecting the risk assessment and management to the larger organizational structure. While it is not strictly in scope of the document to provide recommendations for organizations to adhere to those practices, there may need to be supplemental information provided by other resources to understand how the device level risks map to the organizational risks. The standard addresses both security for data at rest and for data in transit but does not directly provide recommendations for securing data in use. The standard, while addressing key areas such as logging and maintaining both hardware assets and software assets, lacks in describing physical threats such as environmental concerns and other resilience factors. This being said, the standard does address physical access to ports on the device itself. The standard in its next revision may seek to incorporate additional considerations into resiliency factors for the device, thus bridging the gap.

- The **ISA/IEC 62443** standards are scoped for industrial communications, automation, and control systems, and networks. ISA/IEC 62443 also stated as IEC 62443-3-3 (3-3) covers networks and system security, 62443-4-1 (4-1) covers the security of automation and control systems at the industrial level for the product development lifecycle. IEC 62443-4-2 (4-2) covers industrial control systems with respect to the seven foundational requirements that are enumerated in IEC 62443-1-1. Under IEC 62443-3-3, 4-2 may be seen as a subset.

  The gap analysis for IEC 62443 was done for substandards (3-3), (4-2), and (4-1). The standards were previously mapped to the NIST CSF version 1 for 3-3. The mapping for 3-3 was first updated to align with the categories and subcategories for NIST CSF version 2. Then a second gap analysis was done for 4-1. Finally, due to 4-2 being a subset of 3-3, 4-2 was added to the 3-3 mapping under the comments section. From these documents, a more simplified version was created to show all three of the 62443 standards analyzed. Using this simplified version, the gaps were then color coded by category. The colors are taken from the matrix (Fig 4-3) above.

  The main gaps for IEC 62443 when mapped to the NIST CSF included Recover where neither of the subcategories is covered. The Govern Function has six categories with four that are not addressed, one is insufficiently addressed and one, Cybersecurity Supply Chain Risk Management is addressed. The Detect Function has two categories, Continuous Monitoring, and Adverse Event Analysis, both of which are insufficiently addressed. The Protect Function has five categories and IEC 62443 does address three of those with the other two being insufficiently addressed. Overall, it seems that many of the standards are lacking in the areas of Risk Management and the Govern category. This can be attributed to the fact that the NIST CSF was used for the gap analysis. Product standards do not generally take into account these categories related to cybersecurity or otherwise. Additionally, the scope of this project did not include other parts of the IEC 62443 standard such as 2-1 and 3-2. Part 3-2 does address risk management, and 2-1 addresses building a security program and governance.

Incident detection and response was covered in the context of security requirements and levels within IEC 62443-3-3, 2-1 primarily covered the requirements for establishing a cybersecurity management system for IACS asset owners, and 2-4 covered service providers, with a focus on including incident response capabilities. Another gap existed when covering role-based access control, a key component of IEC 62351-8, in which monitoring and responding to unauthorized asset attempts is emphasized. Similarly on the topic of organizational context as it pertains to understanding circumstances surrounding an organization's cybersecurity risk management decisions, the reviewed IEC standards were lacking. IEC 62443-2-1 contained a section covering requirements for establishing a management system that included organizational context, stakeholder expectations and regulatory requirements for IACS asset owners, and 2-4 covered organizational context and dependencies from a service provider perspective.

- The **SunSpec Cybersecurity Certification** program mainly covers the secure communication among the different DER devices, authentication, software updates, and continuous monitoring of the DER devices. Specifically, SunSpec requires the use of protocols like TLS and IPSec in order to protect the data in transit and it mandates secure methods in order to manage the authentication credentials and ensure that only authorized access is possible. Moreover, SunSpec address the need for regular software updates and provides guidelines in order to prevent the unauthorized software installations. Additionally, SunSpec includes aspects of continuous monitoring and secure communication among the DER devices. On the other hand, topics related to organizational relevant cybersecurity requirements are not covered by SunSpec. Specifically, SunSpec does not cover organizational security measures, cybersecurity training of personnel, data security specifically in terms of data-in-transit and data-in-use, platform security and infrastructure, and the incident management. Specifically, SunSpec does not cover identity management and access control policies beyond the ones described at the DERs device level as well as broader organizational security practices. SunSpec does not provide requirements for training programs for personnel and for data backup for recovery from data loss or corruption. Additionally, SunSpec does not discuss configuration management practices, technology infrastructure resilience, hardware maintenance and lifecycle management of the hardware. The device level cybersecurity standards provided by SunSpec cover all the critical aspects related to the communication, authentication, authorization, software updates, and monitoring of the devices which is one of the main goals of this project. Organizational related cybersecurity standards can be addressed, if needed, by other standards listed in this survey analysis. Thus, from the performed analysis it is concluded that SunSpec covers all the most critical aspects of the device-level security which becomes critical for securing the electric vehicles' infrastructure both of the front-end and at the back-end.

  Addressing Gaps in SunSpec Standards: Based on the performed analysis of the existing SunSpec cybersecurity standards and the discussion regarding the identified gaps, we conclude to the outcome that it is important to extend the focus of the cybersecurity standards beyond the device level security and incorporate organizational levels cybersecurity measures, as identified by the NIST CSF. Based on the above discussion, it is evident that the SunSpec cybersecurity standards mainly emphasize on securing the communication among the distributed energy resource devices, the authentication processes, and the software updates. However, we identified that the SunSpec cybersecurity standards lack coverage in areas such as organizational security policies, personnel training, and incident management protocols. One solution to address this gap is to introduce an additional framework that supplements the SunSpec cybersecurity standards by establishing clear guidelines for organizational practices and include policies for cybersecurity awareness training, data management, and recovery procedures in order to ensure that the organizations not only secure the DER devices but also they built a robust security culture across all personnel and systems. Another way to address the organizational policies is the extension of the SunSpec cybersecurity standards in order to include broader security management practices, for example identity and access control management at an organizational level.

Based on the performed gap analysis, we concluded that the SunSpec cybersecurity standards cover authentication between the devices, however, the standards do not specify how the organizations should manage the overall lifecycle of their identities, for example the employee credentials and the multi-factor authentication. One solution to address this gap is the extension of the SunSpec cybersecurity standards or complementing them with existing or new standards in order for the organizations to implement a centralized identity management system which will ensure the secure access across all the devices and personnel regardless of their role. This solution will mitigate the risks that are associated with the unauthorized access, as well as the insider threats and the danger of identity misuse. Based on the performed gap analysis, we also concluded that the SunSpec cybersecurity standards do not include the concept of platform security especially when this is related to the data-in-use or the data-in-transit. Therefore, a way to strengthen the data security is to integrate additional protocols into the existing SunSpec cybersecurity standards and provide explicit guidance in terms of how the data will be secured at all the stages of their lifecycle. This solution can include data segmentation techniques that minimize the exposure of sensitive information complementary to existing encryption methods. Also, another solution could be the adoption of standards that cover incident management and data backup procedures to complement the SunSpec cybersecurity standards in order to ensure that the organizations can swiftly respond to data breaches or system failures and ultimately minimize their downtime but also prevent data corruption or loss. Towards addressing the hardware lifecycle management which is absent in the SunSpec cybersecurity standards, a solution could be the periodic hardware audits and the establishment of maintenance protocols. Specifically, the organizations can adopt a continuous monitoring approach for the hardware and document specific procedures in order to manage the replacement, upgrade, or the commissioning of the devices. By incorporating such an approach within the existing SunSpec cybersecurity standards, the hardware vulnerabilities can quickly be identified and resolved, thus the risk of exploitation due to outdated or compromised equipment will be reduced. Additionally, by adopting the lifecycle management protocols, the resilience of the overall system will be improved in addition to securing the DER devices.

- The **ISO 15118-20** standard, part of the ISO 15118 series, defines how electric vehicles

(EVs) and electric vehicle supply equipment (EVSE) communicate. This includes both battery electric vehicles (BEVs) and plug-in hybrid electric vehicles (PHEVs). The standard primarily addresses messages at the application layer that facilitate power transfer, including bidirectional power transfer (vehicle-to-grid, V2G). It outlines communication needs for both wired and wireless charging, automatic connection devices, and information about charging and control status. Additionally, the standard details messages, data models, XML/EXI formats, and protocols (V2GTP, TLS, TCP, IPv6) spanning the 3rd to 7th layers of the OSI model.

The analysis of the ISO 15118-20 standard reveals that, due to its highly technical nature, it does not address many organizational aspects of the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). The standard offers substantial but incomplete coverage of the 'Protect' function, including Identity Management, Authentication, Access Control (PR.AA), Data Security (PR.DS), and Technology Infrastructure Resilience (PR.IR). To address the remaining gaps in this function, other reviewed standards can be utilized. For instance, UL 2941 and IEEE 1547.3 offer sufficient coverage of controls in the PR.AA subcategory. To address deficiencies in Data Security controls, IEC 62443 and UL 2900 are appropriate as they meet the required standards. For enhanced coverage of Technology Infrastructure Resilience, IEC 62443 should be considered as the primary protocol, complemented by SunSpec, IEEE 1547.3, and IEEE 2030.5 protocols. Additionally, Awareness Training (PR.AT) and Platform Security (PR.PS) controls, which are not addressed by ISO 15118-20, can be covered by IEEE 1547.3 (for PR.AT) and IEC 62443 and UL 2900 (for PR.PS).

The ISO 15118-20 standard partially addresses some controls within the 'Identify' function, such as Asset Management (ID.AM) and Risk Assessment (ID.RA). To achieve more comprehensive coverage for these subcategories, organizations can utilize provisions from UL 2900 and IEC 62443, which offer extensive coverage. The Improvement subcategory (ID.IM) is not covered by ISO 15118-20, and none of the reviewed standards fully address this subcategory. However, partial coverage can be found in the SunSpec, IEC 62443, and IEEE 1547.3 standards to help bridge this gap.

ISO 15118-20 provides partial coverage of Continuous Monitoring (DE.CM) controls within the 'Detect' function. To address the gaps in this area comprehensively, provisions from the reviewed SunSpec, IEC, UL 2941, and IEEE standards can be combined, as they also offer partial coverage of this subcategory. However, Adverse Event Analysis (DE.AE) controls are not covered by ISO 15118-20 and are only partially addressed by IEC 62443, UL 2900, and IEEE 1547.3. To fully cover the gaps in Adverse Event Analysis controls, it is beneficial to utilize not only these reviewed standards but also additional industry standards.

The ISO 15118-20 standard does not cover the 'Govern,' 'Respond,' and 'Recover' functions of the NIST CSF. To address these gaps, several reviewed protocols can be utilized. For instance, UL 2900 provides coverage for the Risk Management Strategy (GV.RM) subcategory, SunSpec addresses controls related to Policy (GV.PO), UL 2900 and IEEE 1547.3 cover provisions for Oversight (GV.OV), and the IEC 62443 protocol addresses Cybersecurity Supply Chain Risk Management (GV.C) within the 'Govern' function of the NIST CSF. For the 'Respond' and 'Recover' functions, IEC 62443 and IEEE 1547.3 can be utilized, as they cover more controls compared to the other reviewed standards, although they still provide only partial coverage. Since the reviewed standards do not address many of the organizational requirements of the CSF, it is essential to supplement these standards with additional guidelines and practices that align with the unaddressed NIST CSF functions. This includes integrating organizational aspects and enhancing protocols for governance, response, and recovery to create a more comprehensive cybersecurity framework.

	SunSpec	**IEC 62443 (3-3, 4-1, 4-2)**	**UL 2900**	**UL 2941**	**IEEE 1547.3**	**IEEE 2030.5**	**ISO 15118**
Organizational Context (GV.OC)	IA	NA	IA	NA	IA	IA	NA
Risk Management Strategy (GV.RM)	IA	NA	A	IA	IA	NA	NA
Roles, Responsibilities, and Authorities (GV.RR)	IA	NA	IA	NA	IA	NA	NA
Policy (GV.PO)	A	NA	NA	NA	IA	IA	NA
Oversight (GV.OV)	IA	IA	A	NA	A	IA	NA
Cybersecurity Supply Chain Risk Management (GV.SC)	NA	A	NA	IA	IA	NA	NA
Asset Management (ID.AM)	IA	IA	A	IA	IA	IA	IA
Risk Assessment (ID.RA)	NA	A	A	IA	IA	IA	IA
Improvement (ID.IM)	IA	IA	NA	NA	IA	NA	NA
Identity Management, Authentication, and Access Control (PR.AA)	IA	IA	IA	A	A	IA	IA
Awareness and Training (PR.AT)	NA	IA	NA	NA	A	NA	NA
Data Security (PR.DS)	IA	A	A	IA	IA	IA	IA
Platform Security (PR.PS)	IA	A	A	IA	IA	IA	NA
Technology Infrastructure Resilience (PR.IR)	IA	A	NA	NA	IA	IA	IA
Continuous Monitoring (DE.CM)	IA	IA	NA	IA	IA	IA	IA
Adverse Event Analysis (DE.AE)	NA	IA	IA	NA	IA	NA	NA
Incident Management (RS.MA)	NA	A	NA	NA	IA	NA	NA

	SunSpec	IEC 62443	UL 2900	UL 2941	IEEE 1547.3	IEEE 2030.5	ISO 15118
Incident Analysis (RS.AN)	IA	NA	NA	NA	IA	NA	NA
Incident Response Reporting and Communication (RS.CO)	NA	A	NA	NA	A	NA	NA
Incident Mitigation (RS.MI)	NA	IA	NA	NA	A	NA	NA
Incident Recovery Plan Execution (RC.RP)	NA	NA	NA	NA	IA	IA	NA
Incident Recovery Communication (RC.CO)	NA	NA	NA	NA	A	NA	NA

Table 4-1. Table of Gaps

The colors come from the matrix, which are listed below for reference.

Addressed (A)
Insufficiently Addressed (IA)
Not Addressed (NA)

An Overview of the Table of Gaps

The ISA/IEC 62443 standards address the most subcategories, with seven subsections being fully addressed. UL 2900 and IEEE 1547.3 both address six subcategories. The only overlapping subcategory addressed by UL 2900 and IEEE 1547.3 is the Oversight (GV.OV) which is "Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy" [11]. Standards that only fully address one subcategory are SunSpec and UL 2941. IEEE 2030.5 and ISO 15118 do not fully address any subcategories of the CSF. This is not to dismiss that many of the functions have multiple subcategories that are somewhat addressed, defined here as IA (insufficiently addressed) in the table.

The analysis highlighted gaps, particularly in the Detect and Recover functions and the Govern, Identify, and Respond also have minimal coverage. Some categories are addressed by more than one standard. The Protect function has all subcategories addressed with coverage from four different standards. While each cybersecurity standard does provide strong coverage in certain areas specific to its respective intent, the standards all have significant gaps when compared to the NIST CSF. Good coverage exists for areas like software configuration and data protection, and significant gaps exist in cybersecurity incident management, response, and recovery. Most of the standards lack clear requirements for handling incidents after a cybersecurity event, leaving vulnerabilities in post-incident safety and latency.

This page intentionally left blank.

5. CONCLUSION

In an effort to provide guidance toward the harmonization of EVSE cybersecurity standards, this report discussed those cybersecurity standards that would be best suited as a foundation for a voluntary certification program. The standards landscape currently has no dedicated EVSE cybersecurity standards, and in review of other related cybersecurity standards, such as those for DER or industrial automation and control systems (IACS); and as seen in the gap analysis, there is a need to develop standards for the cybersecurity of the EVSE infrastructure. While these standards provide substantial technical coverage for the Protect function, addressing areas such as identity management, authentication, and platform security, it lacks provisions for Governance, Incident Response, and Recovery, and for subcategories like Risk Management, and cybersecurity incident management. To bridge these gaps, organizations should supplement standards with guidelines from frameworks like the NIST Cybersecurity Framework (CSF), ensuring full coverage of organizational aspects related to Governance, Response, and Recovery. Integrating NIST CSF Functions would help vendors better manage risks, collect data, and ensure record integrity during incidents. Additionally, clarifying the division of responsibility between vendors and product users for incident response could improve cybersecurity safety. By integrating hardware lifecycle management, incident response, and recovery protocols, organizations can enhance their cybersecurity posture and improve system resilience.

Cybersecurity certification programs for EVSE are fragmented, with no single certification covering all aspects of the device. These devices face vulnerabilities due to their complex software, firmware, and hardware integration, as well as their connections to other systems like electric vehicles, cloud data, and the electric grid. While no certifications specifically address EVSE cybersecurity, some existing standards, such as ISA/IEC 62443 align with many of the security needs of the devices. This standard specifically, will be tested for certification purposes on EVSE and ongoing efforts aim to create or revise EVSE standards throughout this process. Future work will be conducted to provide guidance, align testing, and close gaps in the standards where possible, ultimately establishing a roadmap to a unified cybersecurity program.

This page intentionally left blank.

REFERENCES

[1] JIM MOTAVALLI. As Cyberattacks Ramp Up, Electric Vehicles Are Vulnerable, 2024.

[2] Abby Brown, 1 Jeff Cappellucci,1 Alexia Heinrich, 2 and Emma Cost. Electric Vehicle Charging Infrastructure Trends from the Alternative Fueling Station Locator: Third Quarter 2023, 2024.

[3] US Deptartment of Energy, Office of Energy Efficiency Renewable Energy. FOTW 1334, March 18, 2024: By 2030, the US Will Need 28 million EV Charging Ports to Support 33 million EVs, 2024.

[4] Institute of Electrical and Electronics Engineers. IEEE Std 1547.3-2023 - IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems, 2023.

[5] ISA Global Cybersecurity Alliance. Security of industrial automation and control systems an overview of isa/iec 62443 standards, 2024.

[6] SunSpec. Cybersecurity Certification. https://sunspec.org/wp-content/uploads/2024/03/SunSpec-Cybersecurity-Certification-Requirements-Release-2024-v2-clean.pdf.

[7] SunSpec. Cybersecurity Certification Release 2024 Test Procedure. https://sunspec.org/wp-content/uploads/2024/03/SunSpec-Cybersecurity-Certification-Test-Procedure-Release-2024-240319-clean.pdf.

[8] SunSpec. IEEE 2030.5 V2G-AC Profile Implementation Guide for SAE J3072. https://sunspec.org/wp-content/uploads/2022/06/SunSpec-IEEE-2030.5-V2G-AC-Profile-TEST-1.0.pdf.

[9] SunSpec. Blockchain to Record Private Key Properties in DER Equipment. https://sunspec.org/wp-content/uploads/2021/03/SunSpecAlliance_BlockchainWG_Specification_BlockchainTo RecordPrivateKeyProperties_29032021.pdf.

[10] American National Standards Institute. Roadmap of Standards and Codes for Electric Vehicles at Scale, 2023.

[11] NIST, National Institute of Standards and Technology, Gaithersburg, MD). The NIST Cybersecurity Framework (CSF) 2.0, 2024.

[12] Industrial communication networks–network and system security–part 3-3: System security requirements and security levels. https://webstore.iec.ch/preview/info$_{i}ec62443 - 3 - 3$

[13] Industrial communication networks–network and system security–part 4-1: Security for industrial automation and control systems. https://webstore.iec.ch/preview/info$_iec62443-3-3$

[14] Industrial communication networks–network and system security–part 4-2: Technical security requirements for iacs components. https://webstore.iec.ch/preview/info$_iec62443-3-3$

[15] SunSpec. Modbus Interface. https://sunspec.org/wp-content/uploads/2019/09/SunSpec-Modbus-FactSheet-RevA-2019-07-web.pdf.

[16] SunSpec. Technology Overview. https://sunspec.org/wp-content/uploads/2022/05/SunSpec-Technology-Overview-20220301.pdf.

[17] SunSpec. Device Information Model Specification. https://sunspec.org/wp-content/uploads/2022/05/SunSpec-Device-Information-Model-Specificiation-V1-1-final.pdf.

[18] SunSpec. DER Information Model Specification. https://sunspec.org/wp-content/uploads/2021/04/SunSpec-DER-Information-Model-Specification-V1-0.pdf.

[19] SunSpec. Energy Storage Models. https://sunspec.org/wp-content/uploads/2019/08/SunSpec-Alliance-Specification-Energy-Storage-ModelsD4rev0.pdf.

[20] Jay Johnson, Timothy Berg, Benjamin Anderson, and Brian Wright. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. *Energies*, 15(11), 5 2022.

[21] International Organization for Standardization. ISO 15118-20:2022 - Road Vehicles — Vehicle-to-Grid Communication Interface — Part 20: Network and Application Protocol Requirements, 2022.

APPENDIX A. Standards Not Selected

The following list of standards are those determined to be out of scope for this paper.
ISO 15118 contains seven parts:ISO 15118-1 General Information and use-case definition. Provides general information and defines various use cases related to the communication interface between EVs and the electric power grid.
ISO 15118-2 Network and application protocol requirements. This part provides technical specifications for the network and application layer protocols used in the communication interface between EVs and charging infrastructure.
ISO 15118-3 Physical and data link layer requirements. This part focuses on the lower layer of communication model, addressing the physical layer and data link layer requirements for the communication interface between EVs and charging infrastructure.
ISO 15118-4 Network and application protocol conformance test (link). - This part specifies conformance tests which specify the testing of capabilities and behaviors of a System Under Test (SUT) according to ISO 15118-2.
ISO 15118-5 Physical and data link layer conformance test (link). - This part focuses on conformance testing for the physical and data link layers of the ISO 15118-3.
ISO 15118-8 Physical layer and data link layer requirements for wireless communication (link). - This document specifies the requirements of the physical and data link layer of a wireless High Level Communication (HLC) between EV and EVSE. The wireless technology is used as an alternative to the wired communication technology defined in ISO 15118-3.
ISO 15118-20 2nd generation network layer and application layer requirements (link). - This part outlines communication standards between EVs and EVSE. This standard focuses on facilitating bidirectional power transfer and defines communication messages and sequences. It specifies requirements for wireless communication in both conductive and wireless charging scenarios. The document also details the communication process between the electric vehicle communication controller (EVCC) and the supply equipment communication controller (SECC).

ETSI EN 303 645 - Cyber Security for Consumer Internet of Things (link). This standard provides high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure and their interactions with associated services.

SAE J 1772-2017 - SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler Covers the general physical, electrical, functional and performance requirements to facilitate conductive charging of EV/PHEV vehicles in North America. This document defines a common EV/PHEV and supply equipment vehicle conductive charging method including operational requirements and the functional and dimensional requirements for the vehicle inlet and mating connector.

SAE J 1773-2014 (SAE J1773-2014) SAE Electric Vehicle Inductively Coupled Charging

(Stabilized: Jun 2014).

SAE J 2894-1-2019 Power Quality Requirements for Plug-In Electric Vehicle Chargers.

Electric Vehicle Supply Equipment - EVSE CSA C22.2 No. 280-2016 C22.2 NO. 280-16 - Electric vehicle supply equipment (Tri-national standard, with UL 2594 and NMX-J-677-ANCE-2016) specifies the requirements for cord sets and power-supply cords employing molded-on or assembled-on fittings, rated 600 V maximum, and intended for use in non-hazardous locations in accordance with the Canadian Electrical Code.

NECA 413-2012 Standard for Installing and Maintaining Electric Vehicle Supply Equipment (EVSE) – (link) - standard describes the procedures for installing and maintaining AC Level 1, AC Level 2 152 and fast charging DC (initially known in the industry as AC Level 3 and currently known in the 153 industry as DC Level 2) Electric Vehicle Supply Equipment (EVSE).

ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering: International standard focuses on cybersecurity risk management regarding the engineering of electrical and electronic systems within road vehicles, which includes EVs. Covers aspects such as threat identification, risk assessment, and the implementation of protective measures throughout the lifecycle of the vehicle.

SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems: Not exclusively for EVs, provides guidance on implementing cybersecurity process for the development of vehicle systems, including those in EVs, emphasizing the importance of designing vehicles to be resilient to cyber threats from the outset.

Vehicles to Grid Communication Interface: This standard specifies the communications between EVs and the power grid, including charging stations. Its primarily focused on enabling efficient charging processes, also includes provisions for cybersecurity to protect the data exchange and ensure the integrity and confidentiality of user and vehicle information.

UNECE WP.29 Regulation No. 155 – Cybersecurity and Cybersecurity Management System: UN Economic Commission for requires automotive manufacturers to establish cybersecurity measures to prevent cyber threats. This includes creating a management system, risk assessments, and continuous monitoring against potential vulnerabilities and threats.

APPENDIX B. EVSE Ecosystem Lifecycle

The EVSE ecosystem is shown below in Figure B-1, and has four main interfaces labeled as 1, 2, 3, and 4. Each interface has associated vulnerabilities that can be mitigated through controls. One way that this can be accomplished is through the application of standards and requirements. The exercise done by the team begins at a high level to show which standards are best suited for each interface at each stage of a device's lifecycle. The ecosystem was evaluated at each stage of the device's lifecycle, which includes the Design, Build, Operations, Decommissioning, and then a final pass was done for Supply Chain consideration. See Figures B-2 and B-3.

Standards Coverage for EVSE Ecosystem Lifecycle

The coverage for the EVSE ecosystem lifecycles is minimum at best. The IEEE 2030.5 did not address any of the interfaces at any point in the lifecycle of the EVSE. This standard is a communication standard for smart grid and distributed energy systems (DER) information exchange for devices which include plug-in EVs and smart meters. This standard was included in the scope of this research because the EVSE does require such protocols and should be addressed.

IEEE 1547 is a technology neutral standard that applies to the interconnection of DERs with electric power systems. The substandard IEEE 1547.3 is a guide for information communications and monitoring of DER systems and has guidance for the cybersecurity aspects of the equipment. The standard does address Authentication (2) and Maintenance Interfaces (4) in the Build and Operations stages of the lifecycle. It insufficiently addresses these same two interfaces in the Design phase of the lifecycle.

UL 2900 addresses the cybersecurity of Couplers (1) for the Design, Build, and Operations phases. The standards do not address any other Interfaces or the Decommissioning phase.

UL 2941 Addresses the first two, Design and Build, and the fourth phase, Decommissioning, of the ecosystem for the Authentication Interface. The third phase, Operations is insufficiently addressed.

ISA/IEC 62443-3-3, 62443-4-1, and 62443-4-2 has the most coverage of all of the standards selected for review. The ISA/IEC 62443 set of standards includes other standards that do provide coverage for some of the phases of the lifecycles. Of the standards in this group that were assessed, the Design, Build, and Operations phases were addressed for Couplers (1), Authentication (2), and Maintenance Interfaces (4). For each of the previous phases, Internet Access (3) was insufficiently addressed. The Decommissioning phase of the ecosystem's lifecycle is not addressed.

ISO 15118-20 addresses the Coupler interface for the first three phases, Design, Build, and Operations. The same three phases are insufficiently addressed for the Authentication interface. The Coupler interface is insufficiently addressed for the Decommissioning as well. Internet Access and Maintenance interfaces are not addressed as a whole for this standard.

Standards Coverage for EVSE Supply Chain

IEEE 2030.5 does not address the supply at all. This standard is not a supply chain standard and therefor does not take the supply chain into consideration.

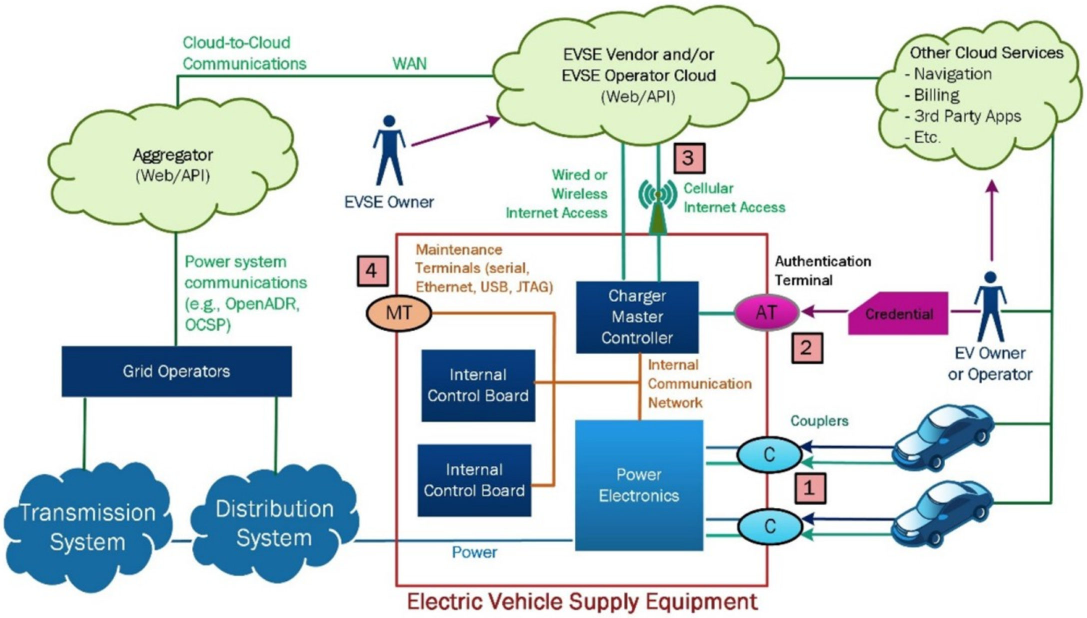


Figure B-1. EVSE Ecosystem

[20]

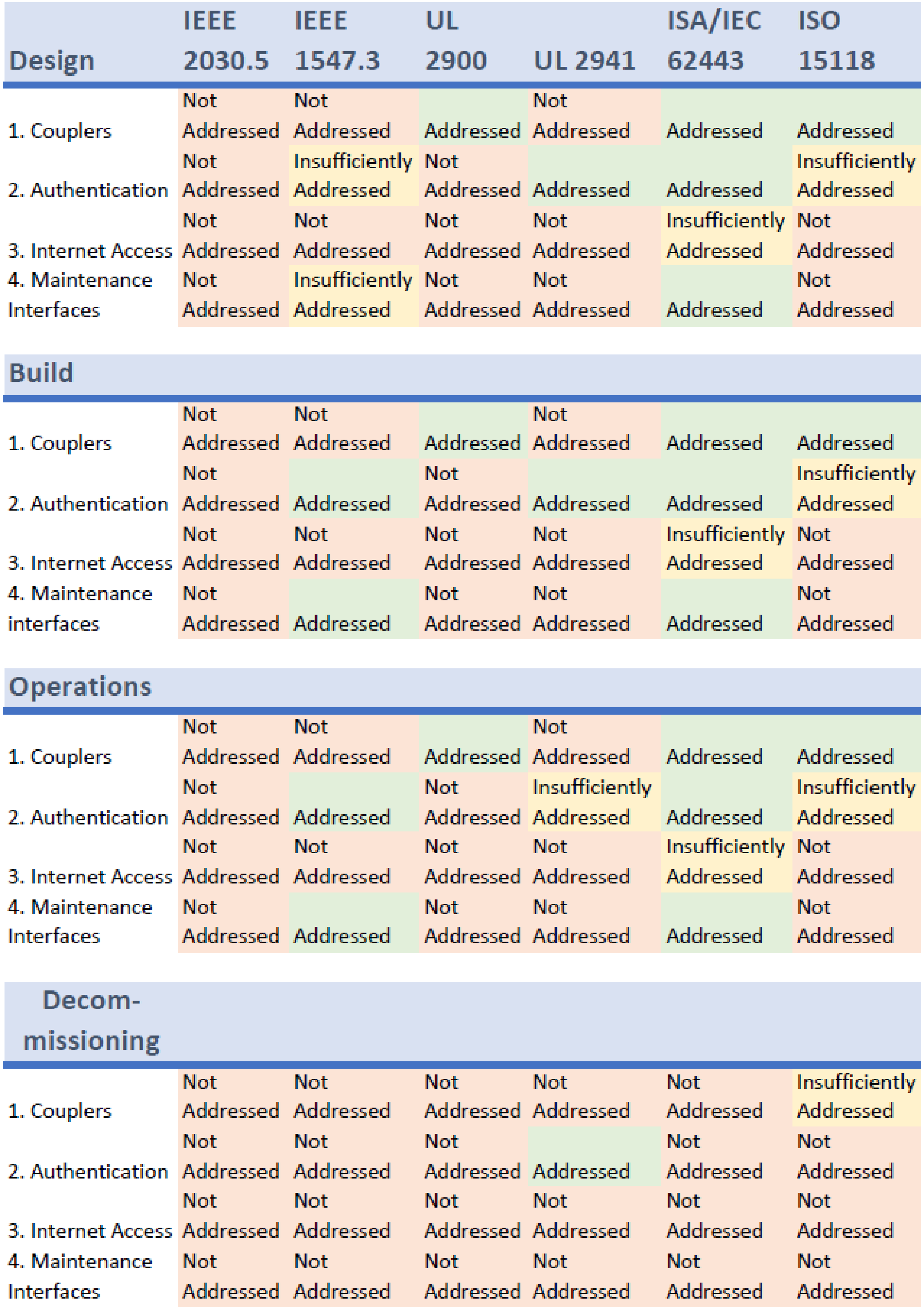
IEEE 1547.3 addresses the Authentication and Maintenance Interfaces with respect to Supply Chain considerations.

UL 2900 does not address anything related to the supply chain.

UL 2941 insufficiently addresses the authentication interface for the Supply Chain.

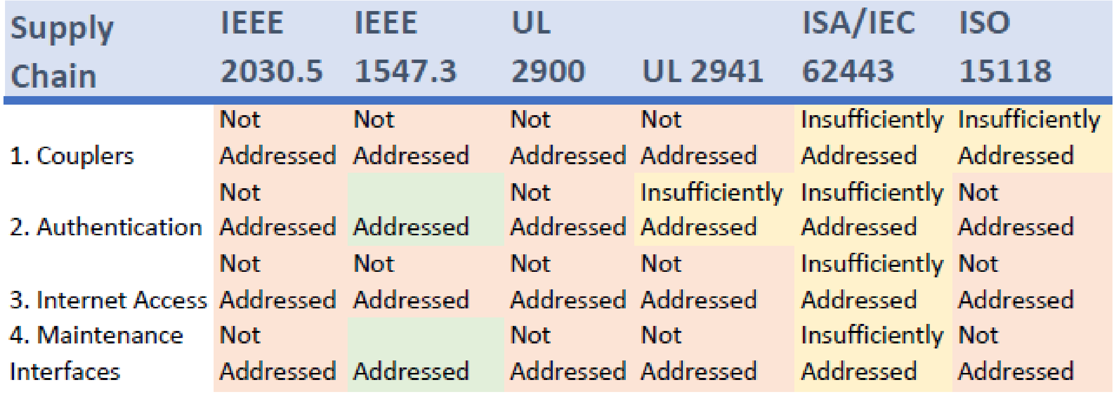
ISA/IEC 62443 (3-3, 4-1, 4-2) has some coverage for Supply Chain concerns, and is marked as insufficiently addressed for all four or the interface areas.

ISO 15118-20 Insufficiently addresses the Couplers for Supple Chain and does not address the other three interfaces.



Design	IEEE 2030.5	IEEE 1547.3	UL 2900	UL 2941	ISA/IEC 62443	ISO 15118
1. Couplers	Not Addressed	Not Addressed	Addressed	Not Addressed	Addressed	Addressed
2. Authentication	Not Addressed	Insufficiently Addressed	Not Addressed	Addressed	Addressed	Insufficiently Addressed
3. Internet Access	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Insufficiently Addressed	Not Addressed
4. Maintenance Interfaces	Not Addressed	Insufficiently Addressed	Not Addressed	Not Addressed	Addressed	Not Addressed
Build						
1. Couplers	Not Addressed	Not Addressed	Addressed	Not Addressed	Addressed	Addressed
2. Authentication	Not Addressed	Addressed	Not Addressed	Addressed	Addressed	Insufficiently Addressed
3. Internet Access	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Insufficiently Addressed	Not Addressed
4. Maintenance interfaces	Not Addressed	Addressed	Not Addressed	Not Addressed	Addressed	Not Addressed
Operations						
1. Couplers	Not Addressed	Not Addressed	Addressed	Not Addressed	Addressed	Addressed
2. Authentication	Not Addressed	Addressed	Not Addressed	Insufficiently Addressed	Addressed	Insufficiently Addressed
3. Internet Access	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Insufficiently Addressed	Not Addressed
4. Maintenance Interfaces	Not Addressed	Addressed	Not Addressed	Not Addressed	Addressed	Not Addressed
Decommissioning						
1. Couplers	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Insufficiently Addressed
2. Authentication	Not Addressed	Not Addressed	Not Addressed	Addressed	Not Addressed	Not Addressed
3. Internet Access	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Addressed
4. Maintenance Interfaces	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Addressed

Figure B-2. Summary of Coverage.



Supply Chain	IEEE 2030.5	IEEE 1547.3	UL 2900	UL 2941	ISA/IEC 62443	ISO 15118
1. Couplers	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Insufficiently Addressed	Insufficiently Addressed
2. Authentication	Not Addressed	Addressed	Not Addressed	Insufficiently Addressed	Insufficiently Addressed	Not Addressed
3. Internet Access	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Insufficiently Addressed	Not Addressed
4. Maintenance Interfaces	Not Addressed	Addressed	Not Addressed	Not Addressed	Insufficiently Addressed	Not Addressed

Figure B-3. Summary of Coverage.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Technical Library	1911	sanddocs@sandia.gov

Hardcopy—Internal

Number of Copies	Name	Org.	Mailstop

Hardcopy—External

Number of Copies	Name(s)	Company Name and Company Mailing Address

Sandia National Laboratories