



SURFACE VEHICLE INFORMATION REPORT

J2931™/7**FEB2018**Issued 2017-10
Revised 2018-02

Superseding J2931/7 OCT2017

(R) Security for Plug-In Electric Vehicle Communications

RATIONALE

The Figures and Tables were not titled in the initial release and after reviewing the Table of Contents, that listed them (without titles), it was appropriate to reopen this TIR, so the titles could be added to clearly identify these in the introductory pages. Considerable effort was taken to produce this document and it didn't seem to be complete without Figure and Table titles.

TABLE OF CONTENTS

1.	SCOPE.....	6
1.1	Purpose	6
2.	APPLICABLE DOCUMENTS.....	6
2.1	SAE Publications.....	6
2.2	ISO-IEC Publications	7
2.3	NIST Publications.....	7
2.4	Other Publications.....	7
3.	DEFINITIONS	8
4.	LOGICAL ARCHITECTURE AND INTERFACES OF THE PLUG-IN ELECTRIC VEHICLE	10
4.1	Logical Architecture Overview	10
4.2	Logical Interface Scenario	11
5.	REQUIREMENTS	16
5.1	General Considerations and Assumptions.....	16
5.2	Basic Requirements	17
5.3	Vehicle Owner Specific Requirements.....	20
5.3.1	Authentication	20
5.3.2	Authorization	20
5.3.3	Non-Repudiation	20
5.3.4	Accountability	20
5.3.5	Data Integrity	20
5.3.6	Confidentiality.....	20
5.3.7	Privacy.....	20
5.3.8	Availability	20
5.3.9	Smart Applications	21
5.3.10	Wireless Communications.....	21
5.4	Vehicle Operator Specific Requirements	21
5.4.1	Authentication	21

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2018 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J2931_7_201802

SAE values your input. To provide feedback on this
Technical Report, please visit
http://standards.sae.org/J2931/7_201802

Documents
Document Sharing Hub

5.4.2	Authorization	21
5.4.3	Non-Repudiation	21
5.4.4	Accountability	21
5.4.5	Data Integrity	21
5.4.6	Confidentiality	21
5.4.7	Privacy	21
5.4.8	Availability	22
5.5	Vehicle Maintenance Personnel Specific Requirements	22
5.5.1	Authentication	22
5.5.2	Authorization	22
5.5.3	Non-Repudiation	22
5.5.4	Accountability	22
5.5.5	Data Integrity	22
5.5.6	Confidentiality	22
5.5.7	Privacy	22
5.5.8	Availability	23
5.6	Vehicle Passenger Specific Requirements	23
5.6.1	Authentication	23
5.6.2	Authorization	23
5.6.3	Non-Repudiation	23
5.6.4	Accountability	23
5.6.5	Data Integrity	23
5.6.6	Confidentiality	23
5.6.7	Privacy	23
5.6.8	Availability	23
5.6.9	Locks and Controls	23
5.6.10	Smart Applications	23
5.7	Utility Specific Requirements	24
5.7.1	Authentication	24
5.7.2	Authorization	24
5.7.3	Non-Repudiation	24
5.7.4	Accountability	24
5.7.5	Data Integrity	24
5.7.6	Confidentiality	24
5.7.7	Privacy	24
5.7.8	Availability	25
5.8	Energy Services Interface Specific Requirements	25
5.8.1	Authentication	25
5.8.2	Authorization	25
5.8.3	Non-Repudiation	25
5.8.4	Accountability	25
5.8.5	Data Integrity	25
5.8.6	Confidentiality	25
5.8.7	Privacy	25
5.8.8	Availability	26
5.9	Energy Management System Specific Requirements	26
5.9.1	Authentication	26
5.9.2	Authorization	26
5.9.3	Non-Repudiation	26
5.9.4	Accountability	26
5.9.5	Data Integrity	26
5.9.6	Confidentiality	26
5.9.7	Privacy	26
5.9.8	Availability	26
5.9.9	Firmware Updates	27
5.10	Electric Vehicle Supply Equipment Specific Requirements	27
5.10.1	Authentication	27
5.10.2	Authorization	27
5.10.3	Non-Repudiation	27
5.10.4	Accountability	27
5.10.5	Data Integrity	27

5.10.6	Confidentiality.....	27
5.10.7	Privacy.....	27
5.10.8	Availability	27
5.10.9	Tamper Resistance	28
5.11	End User Measurement Device Specific Requirements.....	28
5.11.1	Authentication	29
5.11.2	Authorization	29
5.11.3	Non-Repudiation	29
5.11.4	Accountability	29
5.11.5	Data Integrity	30
5.11.6	Confidentiality.....	30
5.11.7	Privacy.....	30
5.11.8	Availability	30
5.11.9	Tamper Resistance	30
5.12	Vehicle Manufacturer Specific Requirements	30
5.12.1	Authentication	30
5.12.2	Authorization	30
5.12.3	Non-Repudiation	30
5.12.4	Accountability	30
5.12.5	Data Integrity	30
5.12.6	Confidentiality.....	30
5.12.7	Privacy.....	30
5.12.8	Availability	30
5.12.9	Supply Chain Security.....	30
5.13	Public Key Infrastructure (PKI) Requirements	31
5.13.1	Certificates	31
5.13.2	Private Keys	31
5.13.3	Root Certificate Authority (Root CA)	31
5.13.4	Certificate Revocation	31
5.13.5	Transport Layer Security (TLS) Protocol	31
5.13.6	Cipher Suites.....	31
6.	USE CASES.....	31
6.1	Use Cases Based on Charging Locations	31
6.1.1	User connects PEV at their premise location using either EVSE cord set or Premise Mounted EVSE.....	32
6.1.2	User connects PEV to EVSE at another premise and premise owner pays for energy use.	33
6.1.3	User connects PEV to EVSE at another premise and the user pays for energy use.	34
6.1.4	User connects PEV to EVSE at another premise outside the enrolled utility's service territory.	36
6.1.5	User connects PEV to EVSE at a public location (curbside, multi-family dwelling location).	37
6.2	Use Cases Based on Payments	39
6.2.1	Anonymous Payment.....	39
6.2.2	Non-Anonymous Payment at EVSE	40
6.2.3	Non-Anonymous Payment with Secondary Actor	41
6.3	Use Cases Based on the Interaction between EVSE and the Customer Energy Management System (CEMS).....	41
6.3.1	Facility Management Dashboard	42
6.3.2	Tenant Notification	42
6.3.3	Equipment Maintenance Operation	43
6.3.4	Load Balancing	43
6.3.5	Demand Response	44
6.3.6	Best Price Charging	46
6.3.7	Charge Time Management	46
6.3.8	Access Control	47
6.3.9	Manage Access Privileges.....	48
6.3.10	Fleet Management	49
6.3.11	Advanced Diagnostics.....	49
6.3.12	Vehicle to Building Storage and Regulation	50
6.4	Use Case Based on the Location of the End Use Measurement Device (EUMD)	51
6.4.1	EUMD is placed inside EVSE.	51

6.4.2	EUMD is placed next to EVSE	52
6.4.3	EUMD is placed inside PEV.....	52
6.5	Use Case Based on Wireless Charging.....	53
6.5.1	Wireless Charger Discovery	53
6.5.2	Vehicle Alignment	54
6.6	Other Use Cases.....	55
6.6.1	Hacking of Electric Vehicle Firmware	55
6.6.2	Hacking of Utility Backend Database Storing User Information.....	55
6.6.3	Hacking of Protocol Translation Module	56
6.6.4	Hacking Wireless Communications	57
6.6.5	Hacking the EVSE Network	57
6.6.6	Hacking into the Firmware Responsible for DC Charging Protocol.....	58
7.	NETWORK SECURITY.....	58
7.1	Inadequate Integrity Checking	58
7.2	Inadequate Network Segregation	59
7.3	Inappropriate Protocol Selection.....	60
7.4	Insufficient Redundancy.....	60
7.5	Physical Access to the Device	60
8.	SOFTWARE VULNERABILITIES	61
8.1	Code Quality Vulnerability (CWE-398).....	61
8.2	Authentication Vulnerability (CWE-287).....	61
8.3	Authorization Vulnerability (CWE-284)	61
8.4	Cryptographic Vulnerability (CWE-310)	62
8.5	Input and Output Validation (CWE-20 and CWE-116).....	62
8.6	Logging and Auditing Vulnerability (CWE-778 and CWE-779)	62
8.7	Sensitive Data Protection Vulnerability (CWE-199)	63
8.8	Session Management Vulnerability (CWE-718)	63
8.9	Mobile Code Vulnerability (CWE-490)	63
8.10	Potential Mitigation for the Vulnerabilities Mentioned Above.....	64
9.	EMERGING TECHNOLOGIES	65
10.	NOTES.....	65
10.1	Revision Indicator.....	65
Figure 1	Logical interfaces for an EVSE and PEV	11
Figure 2	Eumd placed next to standard or smart meter.....	28
Figure 3	EUMD placed next to service panel.....	28
Figure 4	EUMD placed next to EVSE	28
Figure 5	EUMD placed inside EVSE.....	29
Figure 6	EUMD placed inside PEV	29
Figure 7	Software vulnerability summary	64
Table 1	Logical interface	11
Table 2	Actors and their authorized actions summary.....	19
Table 3	PEV connected to customer's site	32
Table 4	PEV connected to another site and site owner pays for energy	33
Table 5	PEV connected to another site and PEV owner pays for energy	34
Table 6	PEV connected to another service territory	36
Table 7	PEV connected to public location	37
Table 8	Energy is paid anonymously	39
Table 9	Energy is paid by user.....	40
Table 10	Energy is paid using secondary actor	41
Table 11	Facility management dashboard.....	42
Table 12	Tenant notification.....	42
Table 13	Equipment maintenance operation	43
Table 14	Load balancing.....	43
Table 15	Demand response.....	44
Table 16	Best price charging	46

Table 17	Charge time management	46
Table 18	Access control	47
Table 19	Manage access privileges	48
Table 20	Fleet management	49
Table 21	Advanced diagnostics	49
Table 22	Vehicle to building storage and regulation	50
Table 23	EUMD inside an EVSE	51
Table 24	EUMD next to an EVSE	52
Table 25	EUMD inside PEV	52
Table 26	Wireless charger discovery	53
Table 27	Vehicle alignment	54
Table 28	Hacking of electric vehicle firmware	55
Table 29	Hacking of utility backend database storing user information	55
Table 30	Hacking of protocol translation module	56
Table 31	Hacking wireless communications	57
Table 32	Hacking the EVSE network	57
Table 33	Hacking into the firmware responsible for DC charging	58

1. SCOPE

This SAE Information Report J2931/7 establishes the security requirements for digital communication between Plug-In Electric Vehicles (PEV), the Electric Vehicle Supply Equipment (EVSE) and the utility, ESI, Advanced Metering Infrastructure (AMI) and/or Home Area Network (HAN).

1.1 Purpose

The purpose of SAE J2931/7 is to define the security requirements for the digital communications between the following:

1. Direct wired point to point communication between PEV and EVSE as end devices

This mode is required for DC Fast Charging or DC DER as defined by SAE J2847/2. This mode could also be used for smart charging, DER operation, or other purposes when the EVSE represents the combined PEV-EVSE to a remote entity and the PEV is completely isolated as with ISO 15118. This mode is used with SAE J3072.

2. Direct wireless point to point communication between PEV and EVSE as end devices

This mode would be used for wireless power transfer as defined by SAE J2847/6.

3. Internet communication between PEV and a remote end device by way of the EVSE

This mode would be used for smart charging (SAE J2847/1) and with onboard inverters (SAE J2847/3). This mode could also be used to engage with a customer with a wireless or wired connection to the internet.

4. PEV engages a remote end device using telematics link

This mode uses a vehicle manufacturer telematics link which exchanges information with an end device using the internet.

5. PEV uses direct wired connection to end device or internet other than by charging port

It may be possible to connect the PEV directly to the internet or end device for maintenance or other purposes which could corrupt the PEV software associated with PEV interaction with the EPS. It is possible that the PEV could use a Wi-Fi link rather than the wired connection through the EVSE to engage the HAN.

For this document, the latest version of NISTIR 7628 (Guidelines for Smart Grid Cyber Security) will serve as a reference to define and map the security requirements for the digital communications for Plug-in Electric Vehicles.

2. APPLICABLE DOCUMENTS

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J1772 SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler

SAE J2836/1 Use Cases for Communication Between Plug-in Vehicles and the Utility Grid

SAE J2836/2 Use Cases for Communication between Plug-in Vehicles and Off-Board DC Charger

SAE J2847/3 Communication for Plug-in Vehicles as a Distributed Energy Resource

SAE J2836/6 Use Cases for Wireless Charging Communication for Plug-in Electric Vehicles

SAE J2847/1 Communication for Smart Charging of Plug-in Electric Vehicles using Smart Energy Profile 2.0

SAE J2847/2 Communication Between Plug-In Vehicles and Off-Board DC Chargers

SAE J2931/1 Digital Communications for Plug-in Electric Vehicles

2.2 ISO-IEC Publications

Copies of these documents are available online at <http://webstore.ansi.org/>.

ISO 15118-1 Vehicle to grid communication interface - Part 1: General information and use-case definition

ISO 15118-2 Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements

2.3 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid

NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

SP 800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems

FIPS 140-2 Security Requirements for Cryptographic Modules

2.4 Other Publications

IEC/TS 62351-1 Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues

IEC/TS 62351-8 Power systems management and associated information exchange - Data and communications security - Part 8: Role-Based Access Control

IEC/TR 62351-10 Power systems management and associated information exchange - Data and communications security - Part 10: Security Architecture

IEC/TR 62351-12 Power systems management and associated information exchange - Data and communications security - Part 12: Resilience and Security Recommendations for Power Systems with DER

IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

CIGRE D2.3 Security architecture principles for digital systems in Electric Power Utilities EPU

Analysis on Cryptographic Module Validation Testing for Side-Channel Attacks (*Journal of Security Engineering*) Analysis on Cryptographic Module Validation Testing for Side-Channel Attacks (*Journal of Security Engineering*) - http://www.sersc.org/journals/JSE/vol7_no4_2010/3.pdf, National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001.

National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010.

National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004.

National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001. Appendix E references Modes of Triple-DES.

National Institute of Standards and Technology, Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A Revision 1, November 2015.

National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-3, June 2009 (DSA, RSA2 and ECDSA2).

National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000 with Change Notice 1 (DSA, RSA and ECDSA).

RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002.

Only the versions of the algorithms RSASSA-PKCS1-v1_5 and RSASSA-PSS are contained.

Chapter Four, Cryptography and Key Management, NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 - August 2010.

3. DEFINITIONS

ADVERSARY: A person or group of people who intend to attack or cause harm to an asset or a system to achieve their goals.

BATTERY MANAGEMENT SYSTEM (BMS): A battery management system is a system which manages the battery pack by monitoring various operating parameters such as module voltage, total battery voltage, battery temperature, battery pressure, etc., by forecasting battery state of charge, maximum allowable charging and discharging current, etc., and by controlling the battery's charging

CHARGE WITH INVERTER: A device which converts AC power from the Energy Service Provider into DC power which can be used to charge the EV Storage Battery. The charger (with inverter) may be situated either on-board (within the vehicle) or off-board (within the EVSE).

CLEARING HOUSE: A clearing house is an organization that provides global PEV account services. It should maintain information necessary to facilitate account validation and billing transactions when customers are charging PEVs at a location not served by the utility that the customer is enrolled with.

DISTRIBUTED ENERGY RESOURCES (DER): Small, modular Distributed Generation (DG) and storage technologies that provide electric capacity power or energy where it is needed on the distribution grid. DG, which includes gensets, solar panels, and small wind turbines, only serve as a source of energy. Storage is a unique form of DER because, unlike pure DG, the unit can provide either energy or variable demand. Plug-in vehicles can serve as DER storage systems.

ELECTRIC VEHICLE SUPPLY EQUIPMENT (EVSE): A PEV connects to the grid using an Electric Vehicle Supply Equipment (EVSE). The EVSE is the physical electrical cord and connectors that are specified by applicable SAE standards (e.g., SAE J1772, SAE J2836, SAE J2847, and SAE J2931) that provide transfer of electrical energy from an energy portal to PEV. This can be 120 V or 240 VAC depending upon the connection. Two types of connection include (1) an EVSE cord-set, and (2) a premise mounted version. The premises EVSE would not include the charger for AC Level 2 energy transfer described in SAE J1772. This would expect the charger to be included on the vehicle. If the EVSE includes an off-board charger, DC energy transfer is expected and the vehicle would bypass any on-board charger and use the one in the EVSE. This EVSE that includes the charger for DC Level 1 may also be capable of AC energy transfer at both 120 V (AC Level 1) and 240 V (AC Level 2) levels. The larger off-board charger in DC Level 2 systems is not expected to also deliver AC since Level 2 systems are fast charge stations and 10 to 20 minute charges are desired here.

END USER MEASUREMENT DEVICE (EUMD): This is the device that is responsible for metering of energy being transferred to a PEV, and is required for Utility or service provider programs such as special EV rates or roaming. Utility or service provider The EUMD may be either a physically discrete unit (for example, a sub-meter located in a branch circuit for PEV charging), or a logical function integrated into another physical device (e.g., the EUMD logical function may be built into an EVSE or the EV). The EUMD is typically (but not necessarily) owned, certified, and implemented at the discretion of the local utility or service provider or energy distributor and may be subject to regulatory control.

ENERGY MANAGEMENT SYSTEM (EMS): Also known as Customer Energy Management System (CEMS). An application used for controlling multiple energy-controllable devices (e.g., pool pump, programmable communicating thermostat, light switches, PEV charging, etc.). This application may reside within a HAN Device (e.g., programmable communicating thermostat, in-home display, computer, cable set-top box, other computing device, etc.). This application may also control other devices or systems in the home providing integrated automated services for the consumer

ENERGY PORTAL: An energy portal is any charging point for a PEV. At a minimum, an energy portal is a 120 V, 15 A outlet, but it can also be an Electric Vehicle Supply Equipment (EVSE) outlet connected to the premises circuit supporting AC or DC charging.

ENERGY SERVICE INTERFACE (ESI): An ESI provides a particular logical function in the HAN. It is an interface which enables secure communications between authorized parties (e.g., Utility or service provider, Consumer, non-Utility or service provider Service Providers, EMS, etc.) and all commissioned HAN Devices that are registered to it. The HAN architecture allows for more than one ESI in a premise. Each ESI creates an independent logical power distribution network within the premises, each with its own security. HAN Devices (e.g., EMS, internet gateway, etc.), which are active on multiple physical networks or transmission media, must have a logical separation between those networks.

ENERGY SERVICE PROVIDER: A utility or other private owner and operator of electrical generation, storage, and supply equipment.

HOME AREA NETWORK (HAN): It refers to the network inside a residence that is usually owned, controlled and or managed by the home owner. A residence includes houses, apartments, and other types of premise. Energy-related devices may use this network in the residence and may share the medium with other devices or networks. Examples of such devices include, but are not limited to appliances, displays, thermostats, etc. A PEV or EVSE may also be considered a HAN device, if it is capable of communicating with other devices in the network.

INDEPENDENT SYSTEM OPERATOR (ISO): An entity authorized by the Federal Energy Regulatory Commission (FERC) to control a regional transmission grid.

INFRASTRUCTURE PROVIDER: A provider of electric vehicle charging infrastructure. For example, a charging station facility owner.

INTEROPERABILITY: The condition where components of a system, relative to each other, can work together to perform the intended operation of the total system. Information interoperability is the capability of two or more networks, systems, devices, applications, or components to share and readily use information securely and effectively with little or no inconvenience for the user.

OFF-BOARD/ON-BOARD BOUNDARY: Off-board/On-board boundary is the point where the ETS is divided into two physical parts. One part becomes realized within the off-board Electric Vehicle Supply Equipment (EVSE). The other part becomes realized within an electric vehicle. This boundary will be in different places, depending on the system architecture.

OFF-BOARD CHARGER: A charger (converter) situated within the EVSE, which converts AC power from the Energy Service Provider to DC power to charge the EV storage battery.

PLUG-IN ELECTRIC VEHICLE (PEV): Also known as Plug-in Vehicle, a PEV plugs into an Energy Portal (see actor definition) to charge the vehicle. This includes many different classifications of vehicles, such as BEVs (Battery Electric), PHEVs (Plug-in Hybrid Electric), E-REV (Extended-Range Electric), and so on.

PLUG-IN ELECTRIC VEHICLE OPERATOR: A person who drives and/or operates one or more plug-in electric vehicles. The plug-in electric vehicle operator may not necessarily be the owner of the vehicle or vehicles. For instance, a fleet driver who operates a vehicle, might not own that vehicle.

PLUG-IN ELECTRIC VEHICLE OWNER: A person who owns one or more plug-in electric vehicles. The plug-in electric vehicle owner may not necessarily be the operator of the vehicle or vehicles. For instance, a fleet owner might not operate or drive any of those vehicles.

POWER LINE COMMUNICATION: Power line communication (PLC), also called power line carrier, mains communication, power line telecom (PLT), or power line networking (PLN), describes several different systems for using electric power lines to carry information over the power line.

RISK: Risk is defined as the potential for loss, damage or destruction of an asset, system, or functionality as a result of a threat exploiting vulnerability.

REGISTERED TRAINING ORGANIZATION (RTO): An organization accredited by the Australian Skills Quality Authority (ASQA) which is the national regulator for Australia's vocational education and training sector. ASQA regulates courses and training providers to ensure nationally approved quality standards are met.

SEP 2.0: The Smart Energy Profile 2.0 is primarily a layer seven protocol, built on top of an Internet Protocol stack which defines the specification to monitor, control, inform and automate the delivery and use of the energy. This is an enhancement of SEP 1.0 version specifications adding services for plug-in electric vehicle, charging, installation, configuration and firmware download, prepay services, user information and messaging, load control, demand response and common information and application profile interfaces for wired and wireless networks.

SMART CHARGING: Smart charging describes a system in which PEVs communicate with the power grid to optimize the vehicle charging or discharging rates with the vehicle operator's preferences, the EVSE capabilities, the grid ancillary services request, the tariff rates, and any spot-market or demand response rates.

THREAT: A threat can be anything that can exploit a vulnerability that is present in an asset, or system, either intentionally or accidentally to gain access to, compromise the operation of, damage, or destroy an asset.

TRANSMISSION SYSTEM OPERATOR (TSO): An entity entrusted with transporting energy in the form of natural gas or electrical power on a national or regional level, using fixed infrastructure.

UTILITY: A utility provides electrical energy and typically refers to a collection of systems that include the Customer Information System (CIS), the Advanced Metering Infrastructure (AMI), Rates and Revenue. The utility makes energy available to PEVs through the ESI pricing tables or discrete events. The utility also supplies information such as tariff rate, interval for metered kWh consumption, and validation of PEV program for PEV ID, etc. Utilities also have requirements for interconnecting with their grids and can request ancillary services for PEVs such as charging rate reductions, frequency support and Volt-VAr support.

VULNERABILITY: Vulnerabilities can be defined as the weaknesses or gaps in a system that can be exploited by threats to gain unauthorized access to an asset.

WEB PORTAL: A general term for a web site which gets the information from different sources and puts them in a unified way.

4. LOGICAL ARCHITECTURE AND INTERFACES OF THE PLUG-IN ELECTRIC VEHICLE

4.1 Logical Architecture Overview

The logical architecture is composed of a set of discrete logical functions that make up the charging process. For each logical function, there are a set of actors that take part in executing that function. The interactions between actors for each function have their own set of security requirements.

4.2 Logical Interface Scenario

Table 1 - Logical interface

Logical Interface Scenario	Actors
Plug-in process	PEV, Vehicle owner, Vehicle operator, EVSE, Energy service provider, Infrastructure provider
Communication Setup	PEV, Vehicle operator, EVSE, ESI, EMS
Identification and Authentication	PEV, Vehicle operator, Vehicle owner, ESI, Utility servers
Utility Programs/Demand Response	PEV, Utility servers, ESI, EMS
Payment Settlement	Vehicle owner, Utility, EUMD, Utility/3 rd party web portal, Utility/3 rd party HMI interface(at the place of charging), Clearing House
Charging	PEV, EVSE, EUMD, ESI, BMS
Plug-out process	PEV, ESI, EVSE, EMS

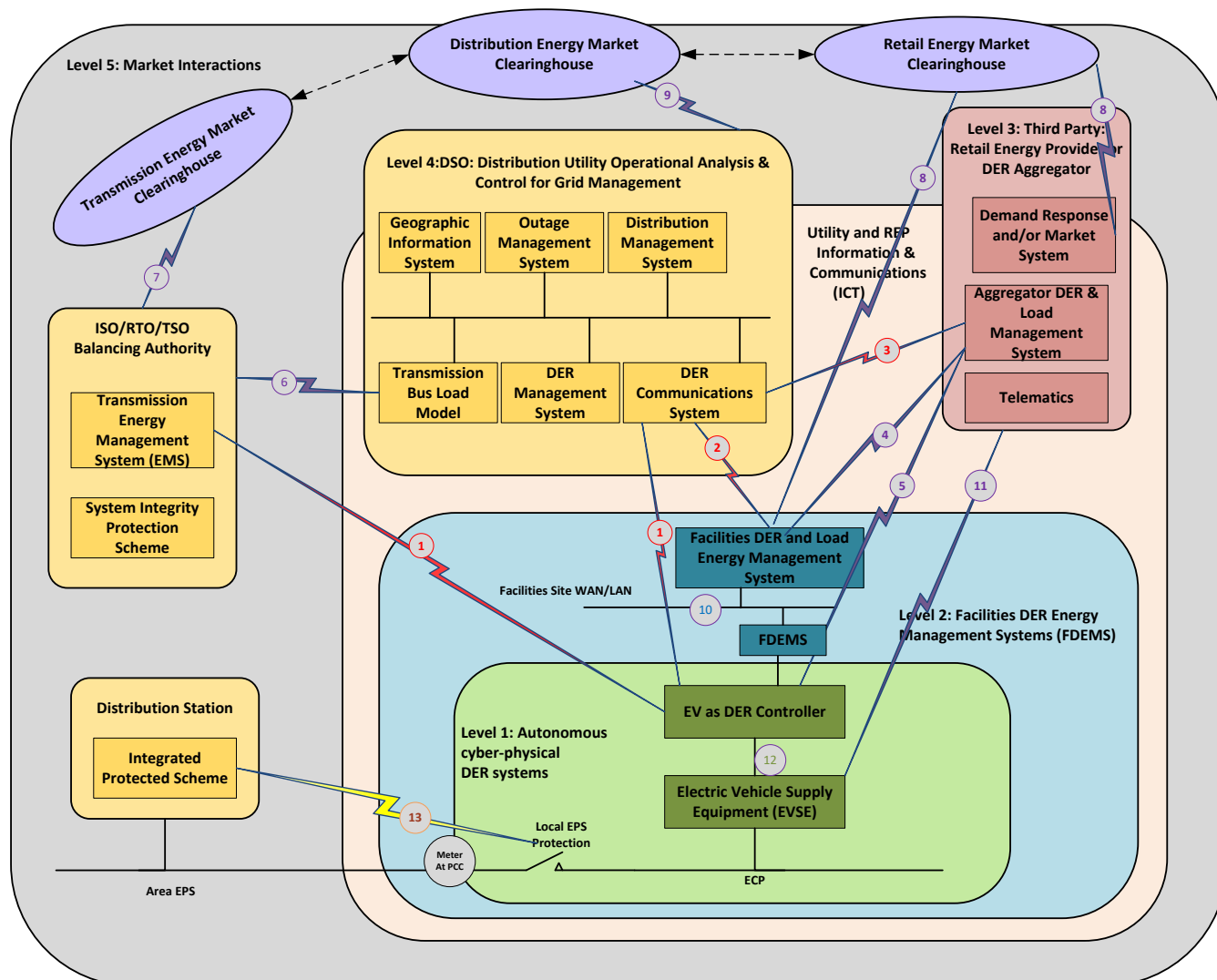


Figure 1 - Logical interfaces for an EVSE and PEV

Security Vulnerabilities likely to be present in the interfaces**Interface between control systems within the same organization (NIST Logical Interface Category 5-U7, 9, 11, 13, 27, 65, 67, 83, 87, 115, Ux2)**

Interfaces between control systems within the same organization or levels (Level 1, 2, 3, and 4) in Figure 1 for example:

- Between multiple energy management systems within FDEMS belonging to the same facility (commercial or industrial); and
- Between subsystems within DCS and ancillary control systems within a power plant.

Control systems with interfaces between them have the following characteristics and issues:

- Since control systems generally have high data accuracy and high availability requirements, the interfaces between them need to implement those security requirements even if they do not have the same requirements.
- The interfaces generally use communication channels (wide area networks [WANs] and/or local area networks [LANs]) that are designed for control systems.
- The control systems themselves are usually in secure environments, such as within a utility control center or within a power plant.

High Level Security Requirements

- User Identification and Authentication
- Authorization and Access Control
- Denial of Service Protection
- Resource Priority
- Boundary Protection
- Communication Integrity
- Software and Information Integrity

Interface between control systems in different organizations (NIST Logical Interface Category 6)

Interfaces between control systems in different organizations, for example:

- Between Autonomous cyber-physical DER systems and Facility DER and Load Management Systems (FDEMS) (Level 1 and 2)
- Between Facility DER and Load Management Systems (FDEMS) and Third-Party Retail Energy Provider or DER Aggregator systems (Level 2 and 3)
- Between Facility DER and Load Management Systems (FDEMS) and RTO/ISO/TSO Balancing Authority systems (Level 2 and 4)
- Between Third-Party Retail Energy Provider or DER Aggregator systems and Distribution System Operators (DSO) (Level 3 and 4)

Control systems with interfaces between them have the following characteristics and issues:

- Since control systems generally have high data accuracy and high availability requirements, the interfaces between them need to implement those security requirements even if they do not have the same requirements.
- The interfaces generally use communication channels (WANs and/or LANs) that are designed for control systems.
- The control systems are usually in secure environments, such as within a utility control center, facility control center or within a power plant.
- Since the control systems are in different organizations, the establishment and maintenance of the chain of trust is more important.

High Level Security Requirements

- User Identification and Authentication
- Authorization and Access Control
- Denial of Service Protection
- Resource Priority
- Boundary Protection
- Communication Integrity
- Software and Information Integrity

Interface with business to business (B2B) connections between systems usually involving financial or market transactions (NIST Logical Interface Category 9- U4, 9, 17, 20, 51, 52, 53, 55, 57,58, 63, 72, 90, 93, 97)

Interface with B2B connections between systems usually involving financial or market transactions, for example:

- Between a Retail Energy Provider (REP) or DER Aggregator and Energy Clearinghouse (Level 3 and 5)
- Distribution System Operators (DSO) and Energy Clearinghouse (Level 4 and 5)

These B2B interactions have the following characteristics and issues:

- Confidentiality needs to be considered since the interactions involve financial transactions with potentially large financial impacts and where confidential bids are vital to a legally operating market.
- Privacy, in terms of historical information on what energy and/or ancillary services were bid, is important to maintaining legal market operations and avoiding market manipulation or gaming.
- Timing latency (critical time availability) and integrity are also important, although in a different manner than for control systems. For financial transactions involving bidding into a market, timing can be crucial. Therefore, although average availability does not need to be high, time latency during critical bidding times is crucial to avoid either inadvertently missed opportunities or deliberate market manipulation or gaming of the system.
- By definition, market operations are across organizational boundaries, thus posing trust issues.
- Special communication networks are not expected to be needed for the market transactions and may include the public internet as well as other available wide area networks

High Level of Security Requirements

- User Identification and Authentication
- Authorization and Access Control
- Denial of Service Protection
- Resource Priority
- Boundary Protection
- Communication Integrity
- Communication Confidentiality
- Software and Information Integrity

Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs (NIST Logical Interface Category 15- U42, 43, 44, 45, 49, 62, 120, 124, 126, 127)

Interface between systems that use customer (residential, commercial, and industrial) site networks such as home area networks, building/business area networks, and neighborhood area networks (NANs), for example:

- Between customer EMS and customer DER equipment
- Between an energy service interface (ESI) and PEVs

The security-related issues for this intra-customer site environment HAN/BAN/NAN interface category include the following:

- Some information exchanged among different appliances and systems must be treated as confidential to ensure that an unauthorized third party does not gain access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential from other appliances whose vendors may want to capture this information for marketing purposes.
- Integrity of data is clearly important in general, but since so many different types of interactions are taking place, the integrity requirements will need to be specific to the particular application.

High Level of Security Requirements

- User Identification and Authentication
- Authorization and Access Control
- Denial of Service Protection
- Security function isolation
- Resource Priority
- Boundary Protection
- Communication Integrity

- Communication Confidentiality
- Confidentiality of Information at Rest
- Software and Information Integrity

Interface between metering equipment (NIST Logical Interface Category 18)

Interfaces between metering equipment, for example:

- Between submeter to meter
- Between End User Measurement Device (EUMD) and Energy Service provider (ESP)
- Between electric vehicles and EUMD

The issues for this metering interface category include

- Integrity of revenue grade metering data is vital, since it has a direct financial impact on all stakeholders of the loads and generation being metered.
- Availability of metering data is important but not critical, since alternate means for retrieving metering data can still be used.
- Meters are constrained in their computational capabilities, primarily to keep costs down, which may limit the types and layers of security that could be applied.
- Revenue-grade meters must be certified, so patches and upgrades require extensive testing and validation.
- Key Management issues.
- Multiple (authorized) stakeholders, including customers, utilities, and third parties, may need access to energy usage either directly from the meter or after it has been processed and validated for settlements and billing, thus adding cross-organizational security concerns.
- Utility-owned meters are in unsecured locations that are not under utility control, limiting physical security.

High Level of Security Requirements

- User Identification and Authentication
- Authorization and Access Control
- Denial of Service Protection
- Security function isolation
- Resource Priority
- Boundary Protection
- Communication Integrity
- Communication Confidentiality
- Software and Information Integrity

Interface between control systems and their vendors for standard maintenance and service (NIST Logical Interface Category 21)

Interfaces between control systems and their vendors for standard maintenance and service, for example:

- Between EVSE and its vendor
- Between PEV and its manufacturer

The main activities performed on this interface include:

- Updating firmware and/or software
- Retrieving maintenance information
- Retrieving event logs

High Level of Security Requirements

- User Identification and Authentication
- Authorization and Access Control
- Denial of Service Protection
- Resource Priority
- Boundary Protection
- Communication Integrity
- Communication Confidentiality
- Confidentiality of Information at rest
- Software and Information Integrity

5. REQUIREMENTS**5.1 General Considerations and Assumptions**

- It is assumed that the PEV, EVSE, and the utility have the communication capabilities.
- The utility offers PEV programs and services for its customers and should provide the necessary support processes for enrollment, communications, and billing, as well as energy and ancillary service tariffs.
- The vehicle manufactures provides the information to the customer about the fuel and/or emission gains of the vehicles offered.
- Each PEV, customer, premise and the utility should have their own unique ids.
- The utility maintains the information on all customers and the PEVs enrolled in different PEV programs, including demand side management programs, associated PEV ids, customer ids and the premise ids. It can determine customers/premises not enrolled in the PEV programs for that utility (although they may be enrolled in programs of different utilities).

- The utility has established message and data interface exchange mechanism with the clearing house for the verification of the roaming PEV.
- End User Measurement Device (EUMD), either fixed or mobile, is available for metering the energy provided to the PEV and applying any smart charging tariffs. If not available, charging will proceed, but with limitations on incentive rates.
- The Energy Service Communication Interface (ESI) exists at the customer/work/public premise and is capable of communicating to the utility and the PEV to facilitate the exchange of the charging session information.
- An un-enrolled PEV can be prohibited from binding to the utility devices or network (Energy Service Communication Interface or ESI), however the charging process will be allowed to proceed.

5.2 Basic Requirements

To meet the basic requirements for the safety and security of the charging process, it is necessary that the communications between the PEV and the EVSE fulfill the higher level of cyber security objectives for the requirements listed below.

- **Authentication** of the systems, devices, and applications that are sending and receiving data, is generally the most important security requirement.
- **Authorization** ensures that the requesting system has the right to view, receive, update, create, and/or delete the data. This is usually provided by Role-Based Access Control (RBAC).
- **Non-repudiation** ensures that some entity cannot deny having received or acted upon a message.
- **Accountability**, enhances non-repudiation by ensuring that all records of actions are traceable to their authors and are kept securely.
- **Data integrity** of all interactions and of information within the systems, is also critical. Data integrity of messages usually implies the need for authentication of the source of the data, and the ability to detect tampering since it is not possible to prevent messages from being destroyed or modified, but it is possible to detect these actions. For the EVSE, PEV, and ESI, integrity also includes
 - o Access of any users or devices is authenticated
 - o No data has been modified without proper authorization
 - o The source of data is properly authenticated according to the applied security policies
 - o Time stamp associated with the data is known, adequately accurate and precise, and authenticated
 - o Quality of the data is known and authenticated according to the applied security policies
 - o Data is valid (i.e., reasonable as well as authorized)
 - o Error management does not prevent charging
- **Confidentiality** is usually required for financial, market, corporate, or private data, but is not usually necessary for normal power system operational data exchanges.
- **Privacy** can also be considered as part of confidentiality, but is focused on *Personally Identifiable Information (PII)* that could potentially identify a specific individual and private data about that individual.

- **Availability** of the interactions can range from milliseconds to hours or days. Unlike the other cyber security requirements, availability generally relies on engineering design, configuration management, redundancy, functional analysis, communication network analysis, and engineering practices. For the EVSE, availability also includes:
 - o Time within which it should start communication setup, and
 - o Loss of non-critical communications does not prevent charging. Examples:
 1. Loss of non-critical communications: AC Charging can be accomplished with a 10 to 96% PWM on the J1772 control pilot. If High Level Communication (HLC) is lost while this PWM range is provided by the EVSE, basic charging would continue without the HLC features. (e.g., HLC for Payment and Authentication are in the Initialization stage that precedes the Energy transfer stage. If the Current Demand HLC message that includes EV Target Current, Voltage, and Power signals, were lost during the charging process, the vehicle would default to the Control Pilot PWM Available Line Current value, instead of stopping the charging process).
 2. Loss of critical communications: If the Control Pilot PWM were lost however, this is a critical analogue communication and charging would stop. Loss of the CP could also mean loss of the ground safety circuit or open circuit of the CP.

Table 2 summarizes the actors and their authorized actions.

Table 2 - Actors and their authorized actions summary

Roles Permissions	Vehicle Owner	Vehicle Operator	Vehicle Maintenance Personnel	Guest	Utility	ESI Owner	EMS Owner	EVSE Owner	EUMD Owner	Vehicle Manufacturer	Vehicle Security Engineer/Security Admin
View vehicle id	X			X							X
Modify vehicle id	X									X	
View Settings and Configurations including security configuration	X	X	X								X
Modify Settings and Configurations including security configuration	X									X	X
View vehicle owner account details	X										
View vehicle operators	X		X	X	X						
Add or delete vehicle operators	X										
View vehicle operators account details		X			X						
Modify vehicle operators account details		X									
View energy service provider id and settings	X				X	X					
View demand response program details	X	X			X	X	X	X	X		
Set the charging schedule	X	X								X	
View EVSE id, settings and configurations								X			
View EUMD id, settings and configurations									X		
View ESI id, settings and configurations						X					
View EMS id, settings and configurations							X				
View session (electric transmission) logs in EVSE								X			
View session (electric transmission) logs in EUMD									X		
View session (electric transmission) logs in ESI						X					
View session (electric transmission) logs in EMS							X				
View energy usage in EVSE								X			
View energy usage in EUMD									X		
View energy usage in EMS							X				
Patch or update EVSE software								X			
Patch or update EUMD software									X		
Patch or update ESI software						X					
Patch or update EMS software							X				
View vehicle maintenance logs	X		X							X	
View vehicle diagnostics	X		X							X	
View Security Certificates	X										X
Modify Security Certificates											X
Test Drive, Play Music, Infotainment, etc.		X		X							
Valet Parking		X		X							

5.3 Vehicle Owner Specific Requirements

5.3.1 Authentication

Identification and authentication of the vehicle, operator, and/or owner should be done to provide incentive rates and other utility information to the vehicle. The information that might be used for this purpose can be a combination of vehicle id, vehicle owner id, energy service provider id, contract id, EVSE id, etc. It is important that the confidentiality and integrity of this information is protected from both malicious and unintentional modification, and that it is handled only by the intended and authorized parties.

5.3.2 Authorization

Authorization of the vehicle owner be an additional control to make sure that authenticated user is not spoofing any other vehicle owner or performing actions that they are not authorized to perform. Implementation of role based access control can help implement authorization in a more granular manner. For example, an authenticated user, but who is not enrolled for incentive rates, cannot take advantage, if proper authorization controls are in place.

5.3.3 Non-Repudiation

There can be several users of a PEV and each of them are likely to be enrolled in the same or different PEV programs. Proper authentication and authorization is necessary to have non-repudiation in place. Further, having a capability of generating and storing logs of all user/system activities and transactions will make non-repudiation easy to implement.

5.3.4 Accountability

PEV users should be accountable for his/her charging activities, sessions, and transactions. Authentication, authorization, and logging are the key properties that will help achieve accountability for PEV owners.

5.3.5 Data Integrity

Any error that is related to the charging process and detected by any of the system control functions shall be logged in an audit log and reported to the user through suitable means.

5.3.6 Confidentiality

The information transmitted during the operations like authorization, authentication, charging, etc., should be protected against information disclosure. Malicious actors can steal this information while the data is in transit or in storage. Other information like energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential from other appliances whose vendors may want to capture this information for marketing purposes.

5.3.7 Privacy

Customer personal identifiable information (PII) shall only be readable by the intended and authorized parties.

5.3.8 Availability

When the cord-set is plugged into the EVSE, the user expects the communication to start between his PEV and the EVSE and consequently to recharge the batteries for the next trip. This charging has also to be completed as per the customer preferences within a predetermined point in time or other Smart Charging criteria, such as percent of charge or cost.

Once the connection is established, the PEV and the EVSE negotiate a charge schedule based on the user enrollment in one of the utility PEV programs, the vehicle operator's preferences, the utility's current capabilities and costs, the charging station programs, and other Smart Charging criteria. The user should be informed of this charge schedule and the time frame within which the vehicle is expected to be recharged.

In the absence or failure of this communication and connection setup, or for any other exceptional circumstances in which charging is able to proceed if the charge schedule cannot be met, the PEV charging will always proceed, however without the incentive rates of the charging program that the user is enrolled into. The error reporting procedure shall be triggered to inform the user about the error through suitable means, either through HMI or PEV dashboard.