SAE INTERNATIONAL

SURFACE VEHICLE INFORMATION REPORT

J2931/1 | DEC2014

Issued 2012-01
Revised 2014-12

Superseding J2931/1 JAN2014

(R) Digital Communications for Plug-in Electric Vehicles

RATIONALE

This SAE Technical Information Report is being updated to include information on the layers 3 to 6 of the ISO OSI 7-layer Communications stack to support DC Charging Application as specified in SAE J2847/2 over Broadband PLC defined in SAE J2931/4.

Several updates have been made to DIN SPEC 70121, and the ISO/IEC 15118 documents and this SAE document along with SAE J2847/2 and SAE J2931/4 are being updated to harmonize with this current level of completion.

TABLE OF CONTENTS

1. SCOPE

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

This is the third version of this document and completes the effort that specifies the digital communication protocol stack between Plug-in Electric Vehicles (PEV) and the Electric Vehicle Supply Equipment (EVSE). The purpose of the stack outlined in Figure 1 and defined by Layers 3 to 6 of the OSI Reference Model (Figure 1) is to use the functions of Layers 1 and 2 specified in SAE J2931/4 and export the functionalities to Layer 7 as specified in SAE J2847/2 (as of August 1, 2012, revision) and SAE J2847/1 (targeting revision at the end of 2012).

Communications between the EVSE and other than PEV entities such as AMI, ESI, HAN, Utility head-end, etc. as shown in Figure 2 are outside of the scope of this document. It is presumed that a bridging device will be required to carry PEV information beyond the EVSE and may be collocated with the latter.

The effort continues however, to additional comments and viewpoints, while the task force also continues additional testing and early implementation. Results of this effort will then be incorporated into updates of this document and lead to a republished versions as needed.

The SAE J2931 family of documents has been organized into several “slash” subsections:

This document, SAE J2931/1, defines architecture and general requirements including association, registration, security, and HAN requirements, as well as mapping to other SAE documents.

SAE J2931/2 is under development and is proposed to define a MAC & PHY layer implementation of digital communications using FSK and the SAE J1772™ Pilot wire.

SAE J2931/3 is under development and is proposed to define a MAC & PHY layer implementation of digital communications using NB OFDM and either the SAE J1772™ Pilot wire or mains.

SAE J2931/4 defines the MAC & PHY layer implementation of digital communications using BB OFDM and either the SAE J1772™ Pilot wire or mains.

Testing and validation of the aforementioned physical layer specifications is ongoing, and it is possible that the results of said testing may preclude one or more of the proposed solutions as unable to meet the technical requirements. Reduction of the available options to a single, worldwide standard remains the long-term goal.

The document mapping of the PEV communication standards are further defined in section 4.

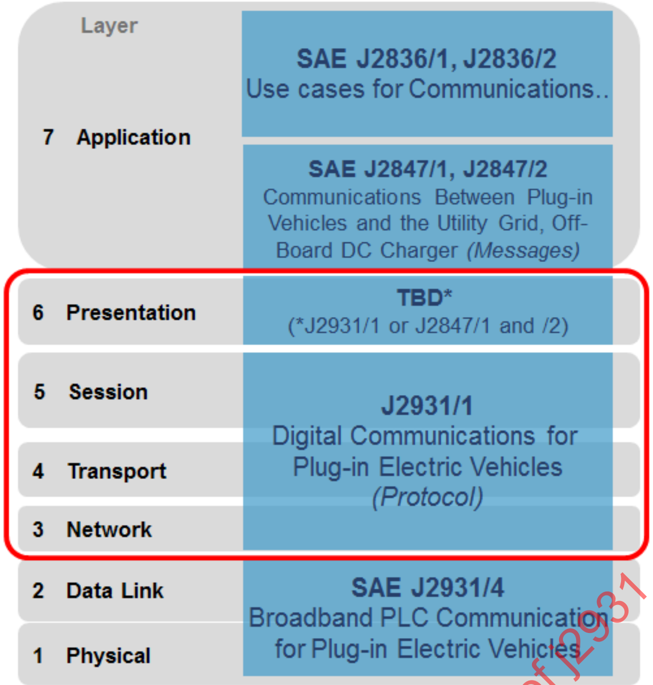


FIGURE 1 - DIGITAL COMMUNICATIONS PROTOCOL STACK.

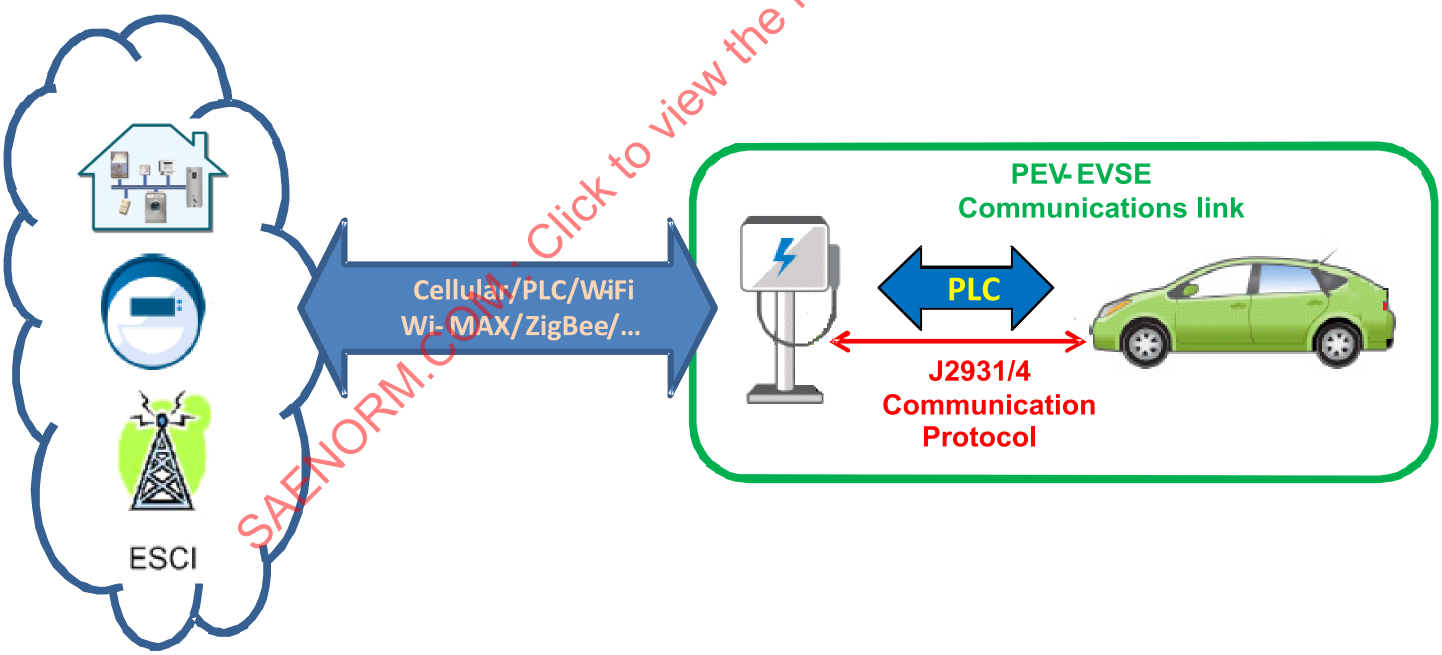


FIGURE 2 - SAE J2931/1 DOCUMENT SCOPE: PEV-EVSE COMMUNICATION PROTOCOL

1.1 Purpose

The purpose of SAE J2931 is to define the digital communications interface between the PEV and an off-board device to which it communicates. Such off-board devices may include one or more of an EVSE, DC charger, Home Area Network (HAN), AMI meter, etc.:

- To provide a safe electric energy transfer
- To interact with energy providers in a secure manner
- To communicate information to the customer on the transaction

In this regard, SAE J2931 serves to complement SAE J1772™, which describes the analog communication between the Electric Vehicle Supply Equipment (EVSE) and the PEV. The Use Cases for communications between a PEV and the utility or service provider are described in SAE J2836™ with the functional message details included in SAE J2847.

2. REFERENCES

2.1 Applicable Documents

The following referenced documents are required for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

SAE J2847/1 Communication between Plug-in Vehicles and the Utility Grid

SAE J2847/2 Communication between Plug-in Vehicles and Off-Board DC Chargers

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

SAE J2931/4 Broadband PLC Communication for Plug-in Electric Vehicles

DIN 70121 Electromobility Digital communication between a DC EV charging station and an electric vehicle for control of DC charging in the Combined Charging System

ISO/IEC 15118-1, 050 ISO IEC 15118-1 E 2011-03-30 Vehicle to grid communication interface - Part 1: General information and use-case definition

ISO/IEC 15118-2, 2011-04-04 ISO IEC 15118-2 E 2011-04-11 Vehicle to grid communication interface - Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements

ISO/IEC 15118-3 Vehicle to grid communication interface - Part 3: Physical layer requirements (working Draft)

ISO 10731 Information technology Open Systems Interconnection - Basic Reference Model - Conventions for the definition of OSI services

IETF RFC 768 User Datagram Protocol (August 1980)

IETF RFC 793 Transmission Control Protocol - DARPA Internet Program - Protocol Specification (September 1981)

IETF RFC 1323 TCP Extensions for High Performance (May 1992)

IETF RFC 1624 Computation of the Internet Checksum via Incremental Update (May 1994)

IETF RFC 1981 Path MTU Discovery for IP version 6 (August 1996)

IETF RFC 2018	TCP Selective Acknowledgment Options (October 1996)
IETF RFC 2460	Internet Protocol, Version 6 (IPv6) Specification (December 1998)
IETF RFC 2988	Computing TCP's Retransmission Timer (November 2000)
IETF RFC 3484	Default Address Selection for Internet Protocol version 6 (IPv6) (February 2003)
IETF RFC 3782	The NewReno Modification to TCP's Fast Recovery Algorithm (April 2004)
IETF RFC 4291	IP Version 6 Addressing Architecture (February 2006)
IETF RFC 4294	IPv6 Node Requirements (April 2006)
IETF RFC 4429	Optimistic Duplicate Address Detection (DAD) for IPv6
IETF RFC 4443	Internet Control Message Protocol (ICMP v6) for the Internet Protocol version 6 (IPv6) specification (March 2006)
IETF RFC 4861	Neighbor Discovery for IP version 6 (IPv6)
IETF RFC 4862	IPv6 Stateless Address Autoconfiguration (September 2007)
IETF RFC 4884	Extended ICMP to Support Multi-Part Messages (April 2007)
IETF RFC 5095	Deprecation of Type 0 Routing Headers in IPv6 (December 2007)
IETF RFC 5220	Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules (July 2008)
IETF RFC 5482	TCP User Timeout Option (March 2009)
IETF RFC 5681	TCP Congestion Control (September 2009)
IETF RFC 5722	Handling of Overlapping IPv6 Fragments (December 2009)
IETF RFC 5871	IANA Allocation Guidelines for the IPv6 Routing Header (May 2010)
IETF RFC 6298	Computing TCP's Retransmission Timer (June 2011)
IETF RFC 6335	Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transfer Protocol Port Number Registry (August 2011)
W3C EXI 1.0	Efficient XML Interchange (EXI) Format 1.0, W3C Recommendation (March 2011)

2.1.1 SAE Publications

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

2.2 Related Publications (Optional)

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

SAE J2836/1™ Use Cases for Communication between Plug-in Vehicles and the Utility Grid (Surface Vehicle Information Report).

SAE J2836/2™ Use Cases for Communication between Plug-in Vehicles and the Supply Equipment (EVSE) (Surface Vehicle Information Report).

SAE J2836/3™ Use Cases for Communication between Plug-in Vehicles and the Utility Grid for Reverse Power Flow (Surface Vehicle Information Report).

SAE J2836/4™ Use Cases for Diagnostic Communication for Plug-in Vehicles (Surface Vehicle Information Report).

SAE J2836/5™ Use Cases for Communication between Plug-in Vehicles and their customers (Surface Vehicle Information Report).

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

SAE J2847/4 Diagnostic Communication for Plug-in Vehicles (Surface Vehicle Recommended Practice).

SAE J2847/5 Communication between Plug-in Vehicles and their customers (Surface Vehicle Recommended Practice).

SAE J2847/6 Communication Between Wireless Charged Vehicles and Wireless EV Chargers

SAE J2894 Power Quality Requirements for Plug-In Electric Vehicle Chargers (Surface Vehicle Recommended Practice).

2.2.1 SAE Publications

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

2.2.2 Other Publications

Other publications may be found at:

OpenHAN Task Force of the UtilityAMI Working Group under the OpenSG Subcommittee of the UCA® International Users Group

http://www.utilityami.org/docs/UtilityAMI%20HAN%20SRS%20-%20v1.04%20-%20080819-1.pdf

ZigBee - Smart Energy

http://zigbee.org/Markets/ZigBeeSmartEnergy/ZigBeeSmartEnergyOverview/tabid/431/Default.aspx

2.2.3 Relation to other standards

2.2.3.1 Definition of OSI based services

This document is based on the conventions discussed in the OSI Service Conventions (refer to ISO 10731) as they apply for the individual layers specified in this document. This document describes requirements applicable to layer 3 - 6 according to the OSI layered architecture.

2.2.3.2 Usage of RFC references

When RFCs are referenced, all “must/ must not” requirements are mandatory. If a referenced RFC has been updated by one or several RFC, the update is fully applicable for this standard. If an update or part of an update applicable to an RFC referenced herein is not compatible with the original RFC or the implementation described by this standard the update shall not apply.

3. DEFINITIONS

3.1 INBAND COMMUNICATIONS

Refers to types of communications using a digital signal modulated over the SAE J1772™ Pilot wire.

3.2 POWER LINE CARRIER (PLC)

Refers broadly to the group of communications technologies in which a modulated carrier is transmitted over AC power circuits. The same communications technologies and designs may sometimes also be applied to circuits that do not carry AC current.

3.3 PEV (PLUG-IN ELECTRIC VEHICLE)

This is the generic term used to describe any vehicle that plugs in to receive electrical energy. 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.

3.4 EVSE (ELECTRIC VEHICLE SUPPLY EQUIPMENT)

This is the generic term used to describe the device that is physically connected and provides energy to the vehicle. EVSEs may take several physical forms, and their logical function may likewise differ substantially. Physical forms include a mobile cordset used for 120VAC charging, a fixed or wall-mounted 240VAC charger, or an off-board DC charger. In terms of logical function, any EVSE may or may not include one or more of the following: a “gateway” or physical layer bridge function to bridge PEV communications to the HAN/AMI, a device that communicates directly with the HAN/AMI itself, etc.

3.5 ESI (ENERGY SERVICES INTERFACE)

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 consumer premises. Each ESI creates an independent logical power distribution network within the premises, each with its own security, described further in J2931/7, section 5. 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.

3.6 EUMD (END-USE MEASUREMENT DEVICE)

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 submeter located in a branch circuit for PEV charging), or a logical function integrated into another physical device (for example, 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.

3.7 AN (HOME AREA NETWORK)

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.

3.8 EMS (ENERGY MANAGEMENT SYSTEM)

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.

It may be owned and operated by the home/premise owner, utility or service provider, or other party.

3.9 ASSOCIATION CONTROL

Entity, that provides the whole functionality for EV to EVSE association and initialization, via the Data Link Control SAP. This entity also controls the relationships between the basic signaling and the upper layers. The entity indicates link status and error information to higher layers. The control of PLC network management parameters is handled over the Control SAP.

3.10 CHARGING SESSION

Time between the beginning (connection of the cable) and the end (disconnection of the cable) of a charging process

NOTE During a charging session the EV may have none, one, or many periods of charging the battery, doing pre-conditioning or post-conditioning

3.11 SERVICE ACCESS POINT (SAP)

Port or logical connection point to one of the 7 layers of the Open System Interconnection (OSI) model

3.12 DATA LINK CONTROL SERVICE ACCESS POINT (SAP)

Port or logical connection point between data link and network layer

3.13 IP ADDRESS

IP-layer identifier for an interface or a set of interfaces

3.14 GLOBAL ADDRESS

IPv6 globally routable address

3.15 INITIALIZATION

Process of interaction between the EV, the EVSE and an external trigger, beginning from plug-in of the charging cable assembly until the decision for the charging mode to be applied

3.16 LINK LOCAL ADDRESS

IP address with link-only scope that can be used to reach neighboring nodes attached to the same link

3.17 MAC ADDRESS

Unique identifier assigned to network interfaces for communication on the data link layer

3.18 MESSAGE SET

Set of mandatory messages and parameters for a specific protocol

3.19 NODE

Device that is part of a communication network
EXAMPLE A device implementing IPv6 in an IP network.

3.20 PHY

An implementation of the Physical layer in the OSI architecture. Connects the data link layer and subsequent upper layers of the OSI model to a physical medium.

3.21 PROFILE

Group of mandatory and optional message sets

3.22 SDP CLIENT

V2G entity that uses the SDP server to retrieve configuration information about the SECCs.

3.23 SDP SERVER

V2G entity providing configuration information for accessing the SECC

3.24 TIMEOUT

Specific time a V2G entity monitors the communication system for a certain event to occur. If the specified time is exceeded, the respective V2G entity initiates the related error handling

3.25 TIMER

Device or piece of software used in an implementation for measuring time. Depending on the specific use case a timer is used to trigger certain system events as well

3.26 V2G COMMUNICATION SESSION

Association of two specific V2G entities for exchanging V2G messages.

3.27 V2G ENTITY

Primary or secondary actor participating in the V2G communication.

3.28 V2G MESSAGE

Message exchanged on application layer.

3.29 V2GTP ENTITY

V2G entity supporting the V2G transfer protocol

4. DOCUMENT MAPPING

4.1 Summary

SAE has published multiple documents relating to PEVs and vehicle-to-grid interfaces. The purpose of this section is to describe the content within and relationships between the various documents, and examples of how to apply them to various scenarios. Existing document series are listed below, with a brief explanation of each.

SAE J1772™ - Defines the physical interface and coupler requirements for PEVs.

SAE J2836™ - General Requirements and Use Cases. This document is divided into several sections. SAE J2836/1™ is for Utility/Smart Grid messaging, SAE J2836/2™ is for DC Charge Control, SAE J2836/3™ is for Reverse Energy Flow. SAE J2836/4™ is for Diagnostics. SAE J2836/5™ is for Consumer Requirements and the HAN.

SAE J2847 - Functional Messaging Requirements. This document defines the functional messages required for a given function. This document is divided into several sections that correspond to SAE J2836 above. SAE J2847/1 is for Utility/Smart Grid messaging, SAE J2847/2 is for DC Charge Control, SAE J2847/3 is for Reverse Energy Flow. SAE J2847/4 is for Diagnostics. SAE J2847/5 is for Consumer Requirements.

SAE J2931 - Digital Communications for PEVs. This series of documents defines the requirements to enable digital communications for PEVs. It is divided into several sections. SAE J2931/1 describes overall General requirements, while each subsequent document is proposed to define a different possible MAC/PHY layer spec. SAE J2931/2 is proposed to define an FSK-based MAC/PHY, J2931/3 proposed to define a G3-PLC based MAC/PHY, and SAE J2931/4 proposed to define a HomePlug GreenPHY based MAC/PHY. Testing and validation of the aforementioned physical layer specifications is ongoing, and it is possible that the results of said testing may preclude one or more of the proposed solutions as unable to meet the technical requirements. Reduction of the available options to a single, worldwide standard remains the long-term goal.

The examples in the next section are to provide a clear overview of which specifications are applicable to different architectural and functional scenarios. Note that the scenarios described below are not mutually exclusive, and may be combined. For example, it is possible to implement utility or service provider programs using Smart Energy Protocol 2.0 (SEP 2.0) together with DC Energy Transfer.

4.2 Example - Utility or service provider Programs Using SEP2.0

- SAE J2836/1 defines the Use Cases for utility or service provider programs (U1 through U5) and system architecture.
- SAE J2847/1 defines the functional messaging between the PEV and the Energy Management System (such as an AMI meter, premise-based charge controller, etc.) and communication protocol stack information.
- SAE J1772 defines the physical interface and connector requirements.
- Digital Communications interface:
    - SAE J2931/1 defines general communications requirements.
    - The MAC/PHY layer used for communication is defined by a subsequent section of SAE J2931, such as SAE J2931/2, /3 or /4. Harmonization and testing efforts with respect to these sections and technologies is ongoing.

4.3 Example - DC Energy Transfer

- SAE J2836/2 defines the architectural requirements for DC energy transfer.
- SAE J2847/2 defines the functional messaging between the PEV and the off-board DC charger, and communication protocol stack information.
- SAE J1772 defines the physical interface and connector requirements.

- Digital Communications interface:
  - SAE J2931/1 defines general communications requirements.
  - The MAC/PHY layer used for communication is defined by a subsequent section of SAE J2931, such as SAE J2931/2, /3 or /4. Harmonization and testing efforts with respect to these sections and technologies is ongoing.

4.4 Example - Reverse Power Flow

- SAE J2836/3 defines the architectural requirements for reverse power flow.
- SAE J2847/3 defines the functional messaging required for reverse power flow, and communication protocol stack information.
- SAE J1772 defines the physical interface and connector requirements.
- Digital Communications interface:
  - SAE J2931/1 defines general communications requirements.
  - The MAC/PHY layer used for communication is defined by a subsequent section of SAE J2931, such as SAE J2931/2, /3 or /4. Harmonization and testing efforts with respect to these sections and technologies is ongoing.

5. REQUIREMENTS

5.1 High-Level Requirements

The following is a set of high level requirements that shall be met:

- Use the existing charging Infrastructure i.e., SAE J1772™
- Enable both public and residential charging
- Accommodate both AC and DC charging methods
- Interact with Energy Providers to optimize energy transfer at the lowest energy cost
- Provide a single interoperable standard to assure compatible systems. Global Acceptance is desired
- Communicate with customer
- Minimal customer interaction
- Requirements should provide expansion capabilities and headroom
- The selected vehicle communications technology must provide reliable communications in typical residential and commercial environments. These environments may include multiple devices, operating using multiple communications technologies, sharing a medium and therefore drive the need to consider both compatibility of technologies as well as potential interoperability
- Security for the four basic areas including (1) Utility communication, (2) DC Charging/Discharging, (3) Telematics and (4) Wireless Charging are identified in J2931/7, section 5.

5.2 Assumptions

The following are assumed:

- Home Area Networks will use a variety of different physical communication interfaces and protocols.

- The communication interface for receiving energy information is known as the ESI. The ESI is defined in the OpenHAN SRS version 2.0. The ESI may host various PEV resources important in managing PEV interactions with energy information. The PEV may "register" with the ESI for a charging session and may request and receive charging session information. In a typical home setting, the ESI may be the premise's Smart Meter as well as other forms (e.g., EVSE, Internet gateway, PEV-hosted).

- An Energy Management System (EMS) if utilized may provide a gateway between the Utility or service provider HAN and the Consumer HAN and the Internet.

- A PEV can implement all of the anticipated functionality.

- If an intelligent PEV is connected to an Intelligent EVSE, the control can be taken over by the PEV.

- EVSE may control the charging of the PEV but may be limited in functionality. E.g., it has no knowledge of PEV's state of charge.

- A method is required to correctly measure energy consumption of an individual PEV (e.g., for tax credits, special tariffs). This requires that a physical and logical relationship be established between a PEV, the EUMD measuring its consumption, and the premise's electrical meter such that the PEV's consumption be calculated separately from the premise's consumption. This relationship is further defined in this document.

- The security requirements for human users and software applications are different from the purely technical security requirements found in many communication and device standards. For user security standards, more emphasis must be on “policy and procedures” and “roles and authorization” rather than “bits and bytes” cryptographic technologies that should be included in Information and Communications Technology (ICT). In addition, engineering practices and system configurations must be taken into account, since no cryptography can compensate for poor design. Figure 3 illustrates the relationships between security requirements, threats, and attacks.

    - Security is structured into four sections in J2931/7:

        - Section 1: Security requirements for standards and specifications which do not address specific cybersecurity technologies but where interactions between human users, software applications, and smart devices must be secured.

        - Section 2: Security requirements for standards and specifications that address information and communication technologies (ICT).

        - Section 3: Engineering design and configuration requirements that provide system reliability, defense in depth, and other security threat mitigations.

        - Section 4: Security requirements related to the OSI Reference Model

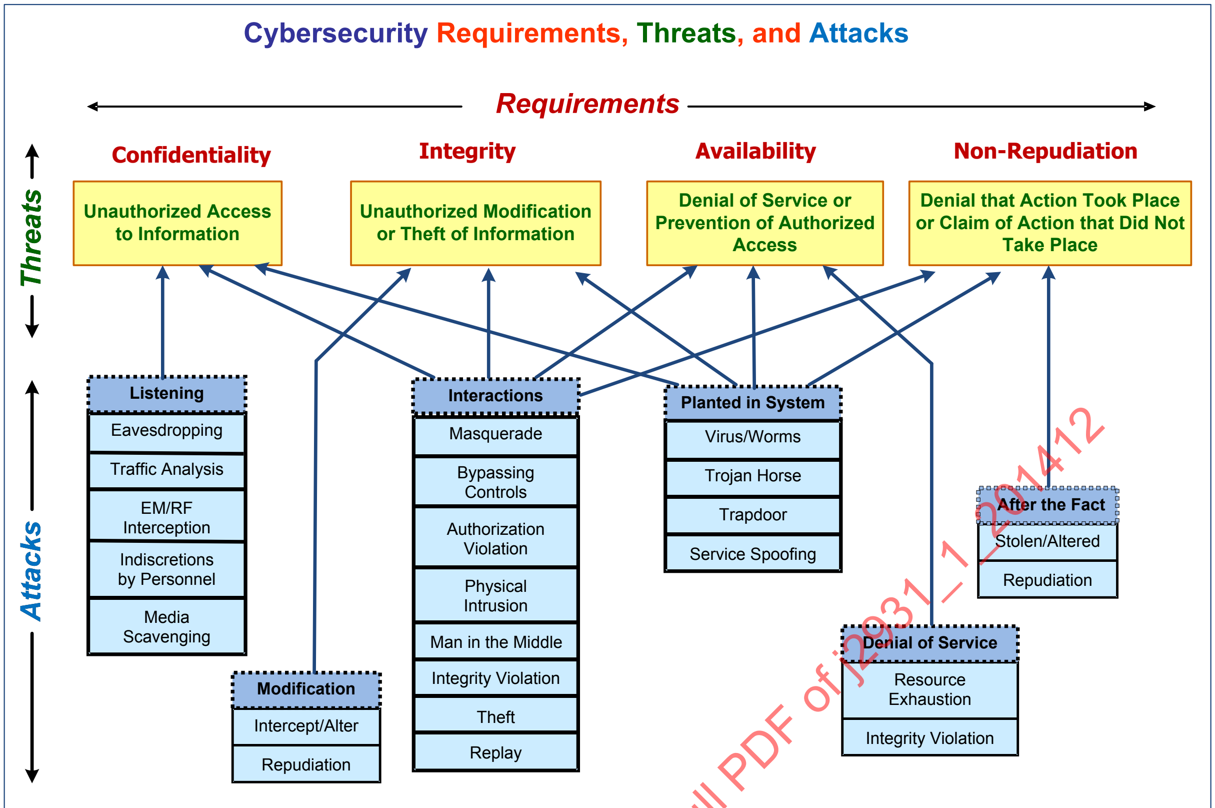


FIGURE 3 – SECURITY REQUIREMENTS, THREATS AND POSSIBLE ATTACKS

5.3 Existing Charging Infrastructure

The conductive charging Infrastructure is defined in SAE J1772™. The EVSE safely provides power to the PEV. SAE J1772™ covers vehicle charging with both AC and DC current and defines three different power/voltage levels for each.

- AC Level 1 uses 120V and the EVSE (typically a mobile cordset type) is normally part of the cable between the Electric Vehicle and a 15A outlet.
- AC Levels 2 & 3 and DC Levels 1, 2, & 3 have the EVSE permanently mounted at the charging location.

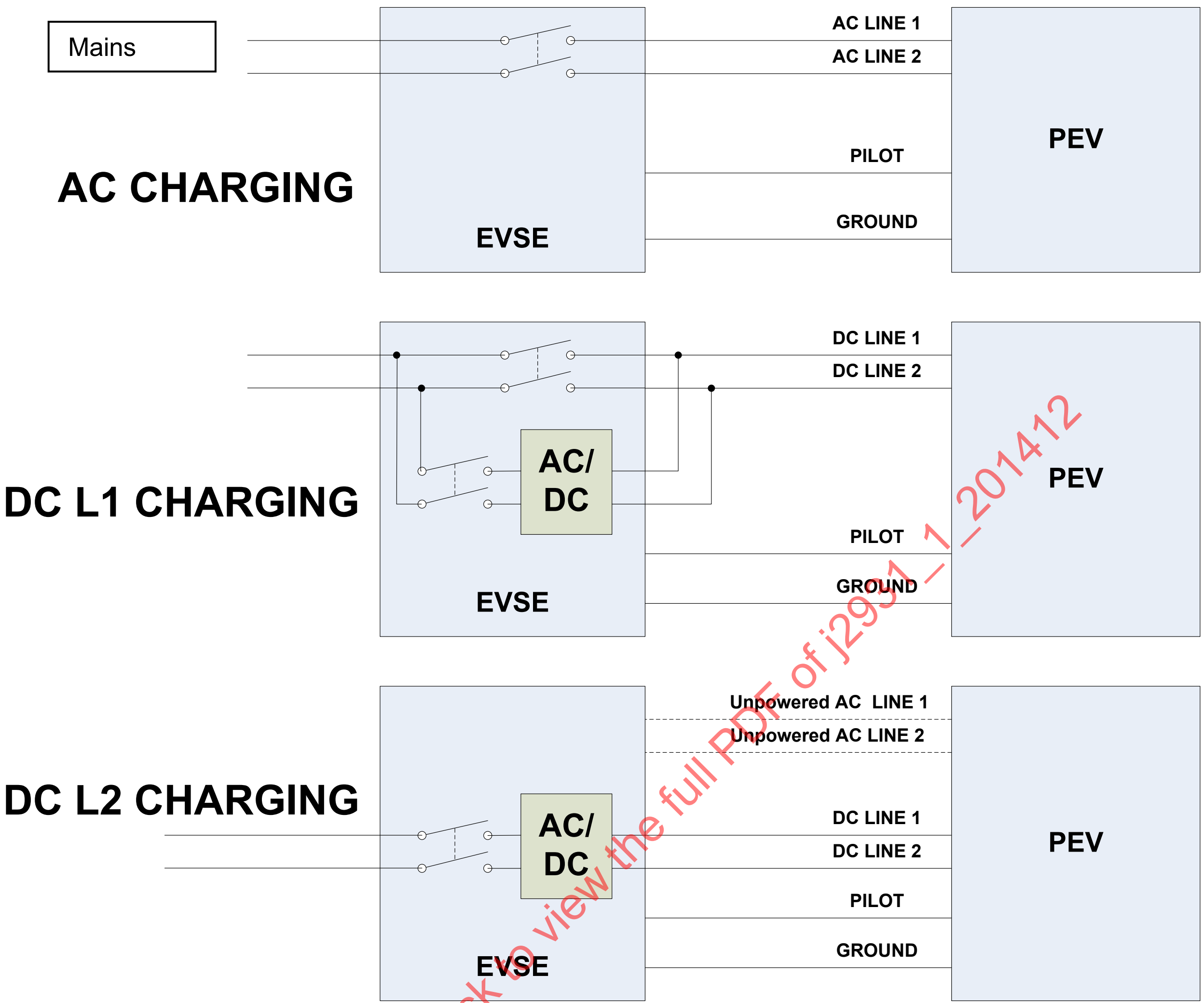


FIGURE 4 - CHARGING INFRASTRUCTURE

Notes for Figure 4:

- The Pilot shares the system ground return circuit.
- If the communications medium between the PEV and the EVSE (or HAN), is not wireless, there are two possible wired connections: the Mains (in case of AC or DC L1/L2) and the Pilot wire, which have a different set of characteristics, such as loads and interfering noise sources. The Pilot wire extends only between the PEV and the EVSE.
- There may exist other media that may play a role in the future but the primary focus of this requirement document is on PLC which is being pursued as a primary option for PEV communication

5.4 General Requirements

The Priority column as defined in HAN SRS 2.0 includes:

- B or Basic - Minimum compliance threshold (required attribute). These are requirements basic to the function or logical device. Logical devices must comply with all basic requirements to be considered Utility or service provider Basic-compliant.
- O or Optional - Suggested requirement; some utilities, service providers, or other users of the standard may require these. These are requirements that are suggested to be included for this logical device. Vendors are encouraged to include optional functionality in a logical device where appropriate or cost effective. It is possible that some Utilities may choose to include these as Basic or Enhanced requirements in their procurements.

- TBD or To Be Determined - The requirement cannot be defined at this time due to a lack of available data, pending development of future standards, requirements, etc.

Requirement ID	Requirement	Reference	Priority
	Application Requirements		
RD.App.1	Support basic Utility or service provider use cases	J2836/1	Basic
RD.App.2	Support basic Utility or service provider messages	J2847/1, SEP2.0, ISO15118	Basic
RD.App.3	If DC Charging is provided, then Support off board charger use cases	J2836/2	Basic
RD.App.4	If DC Charging is provided, then Support DC messages	J2847/2, ISO15118	Basic
RD.App.5	Support Reverse Energy Flow use cases	J2836/3	TBD
RD.App.6	Support Reverse Energy Flow messages	J2847/3	TBD
RD.App.7	Support Diagnostics use cases	J2836/4	TBD
RD.App.8	Support Diagnostic messages	J2847/4	TBD
RD.App.9	Support Customer and HAN use cases	J2836/5	Optional
RD.App.10	Support Customer and HAN messages	J2847/5	Optional
RD.App.11	Utility or service provider messages and DC will use as many common components/software layers as possible and still comply with basic requirements to minimize cost		Basic
RD.App.12	Interoperate with all EVSE and EV	J2953/1, J2953/2	Basic
RD.App.13	Communication solution must not interfere with operation of existing legacy devices compliant with the current (2010) release of J1772™.	J1772	Basic
RD.App.14	Support for Multiple EUMDs, EVSEs, and ESIs on the same physical network (transformer)		Basic
RD.App.15	Support public and residential charging		Basic
Requirement ID	**Requirement**	**Reference**	**Priority**
	Common Communication Requirements		
RD.Comm.1	The DC and Utility or service provider messages shall use the same channel or media between the EV and EVSE to minimize cost based on the different requirements		TBD
RD.Comm.2	Meet Industry EMC and Radiated RF Standards		Basic
RD.Comm.3	Full compliance with SAE licensing terms - RANZ preferred (ref is Patent Release Form-2003.pdf)		Basic
RD.Comm.4	Solution shall be automotive-qualified	AEC-Q100 for ICs and AEC-Q101 for discrete semis	Basic
RD.Comm.5	Solution shall demonstrate technological maturity proven in other general contexts.	Specific metrics TBD	TBD
RD.Comm.7	Global acceptance is desired		Optional
RD.Comm.8	Solution shall be available from multiple vendors		Basic
RD.Comm.9	Length of Cordset is defined as in SAE J1772™, with an assumed typical value of 25 feet		Basic
RD.Comm.10	Solution shall be an international standard i.e., IEEE		Basic
RD.Comm.11	Resulting standard shall select one medium and one PLC technology for communication over the cordset		Basic

5.5 Association Requirements

A HAN and neighborhood network may contain several ESIs, EUMDs and EVSEs. A PEV and cordset EVSE are not permanent members of a HAN.

An association process is used to physically and logically associate which ESI, EUMD and/or EVSE is connected to the PEV requesting a charge so that services (e.g., energy usage, billing, special EV tariffs, calculating tax or carbon credits) can be securely offered and managed per NISTIR_7628, requirement SG.AC-4 for Access Enforcement.

5.6 Authentication Requirements

Once the PEV is authenticated and authorized by the correct servers in the HAN per NISTIR_7628, requirement SG.IA-5 for Device Identification and Authentication", the PEV can discover the hosts of the Smart Energy Resources (e.g., Metering, Pricing, DRLC) it supports. Depending on the physical communications media used or HAN configuration, the EUMD may make the charging session information available to associated PEVs. The functionality of the system will be determined by the availability of Smart Energy Resource servers in the HAN.

Figure 5 and 6 shows the EUMD is electrically connected between the ESI and EVSE (it may be integrated). Figure 7 shows the EUMD integrated into the EV. Although this could eliminate the need to associate, as in the above, there could be substantial regulatory hurdles to redefine a EUMD in the PEV.

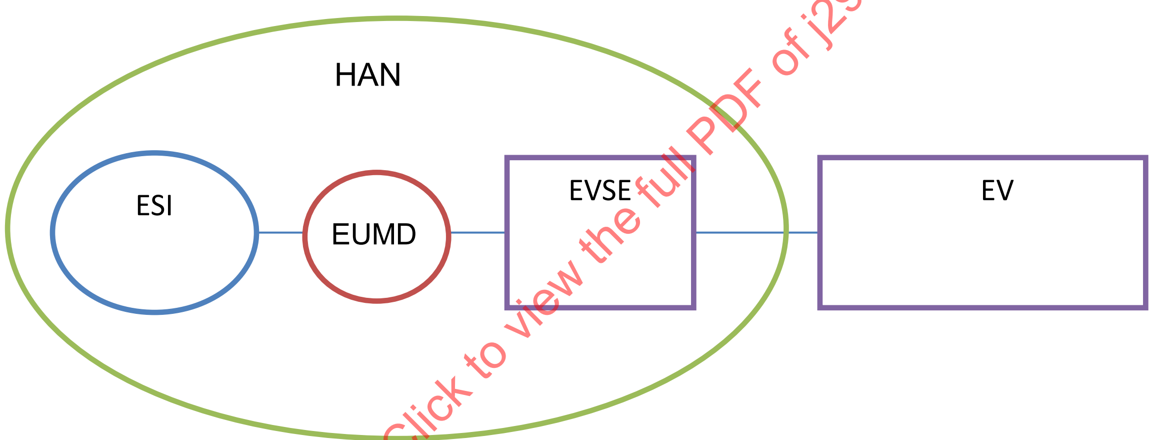


FIGURE 5 - ELECTRICAL NETWORK – HAN EUMD

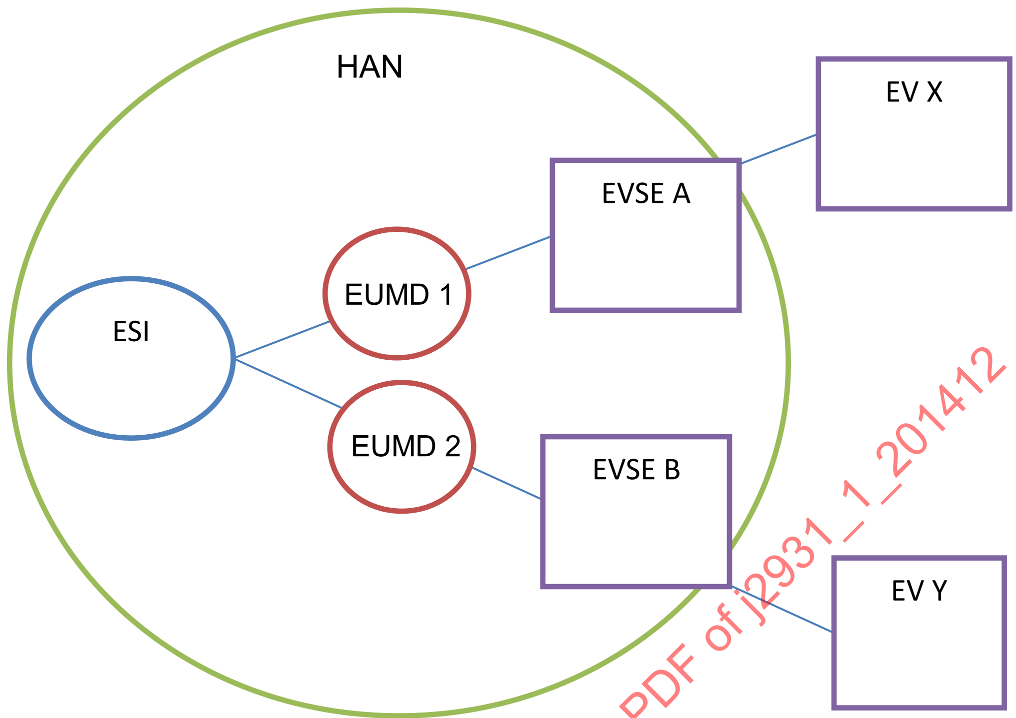


FIGURE 6 - ELECTRICAL NETWORK – MULTIPLE EVSE AND MULTIPLE EUMD

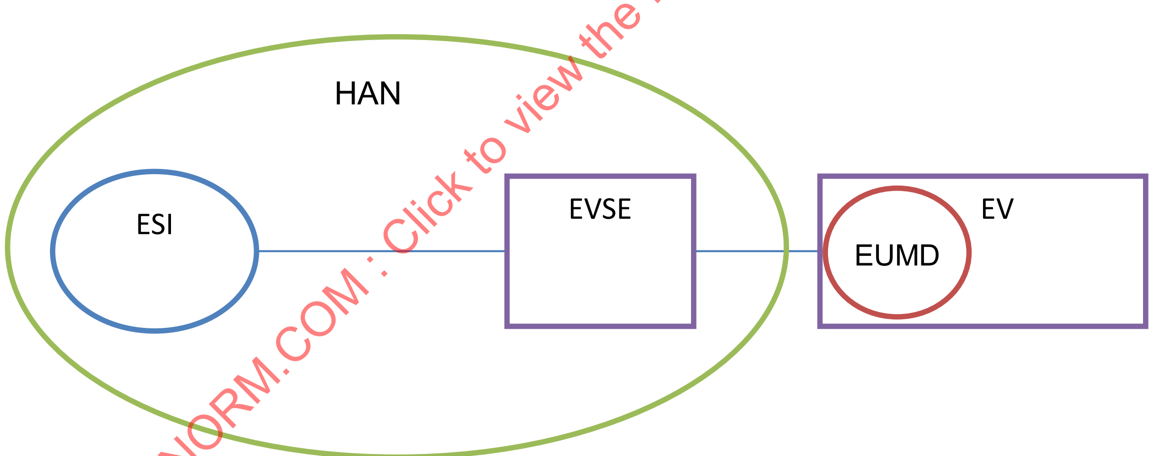


FIGURE 7 - ELECTRICAL NETWORK – PEV EUMD

RD.UtilComm.1	Provide correct association between the PEV and Smart Energy Resource servers (e.g., Metering, Pricing, DRLC) in the same physical electrical circuit		Basic
RD.UtilComm.2	False association shall not occur from two or more twisted EVSE cordsets		Basic

5.7 The HAN and Consumer Networks

In addition to Smart Energy applications, a variety of consumer applications like the Internet, audio, and video may also be served and consumed by a variety of devices. Figure 8 shows the general layout of such a network. In some cases, a dedicated device (e.g., an EMS) may provide network bridging and routing functions to facilitate the co-existence of multiple applications on multiple consumer devices. The different scenarios that were developed by the SE2 MRD working group can be found in the Smart Energy Profile Marketing Requirements Document (MRD) (2). It should be noted that each HAN scenario has to take into account multiple neighbors on the same transformer if PLC wired technology is used or nearby neighbors if wireless technology is used. SAE J2931/1 requires Smart Energy resource servers be present in order to enable PEV applications (e.g., Metering, Pricing) but does not specify requirements for other applications (e.g., Internet, audio, visual).

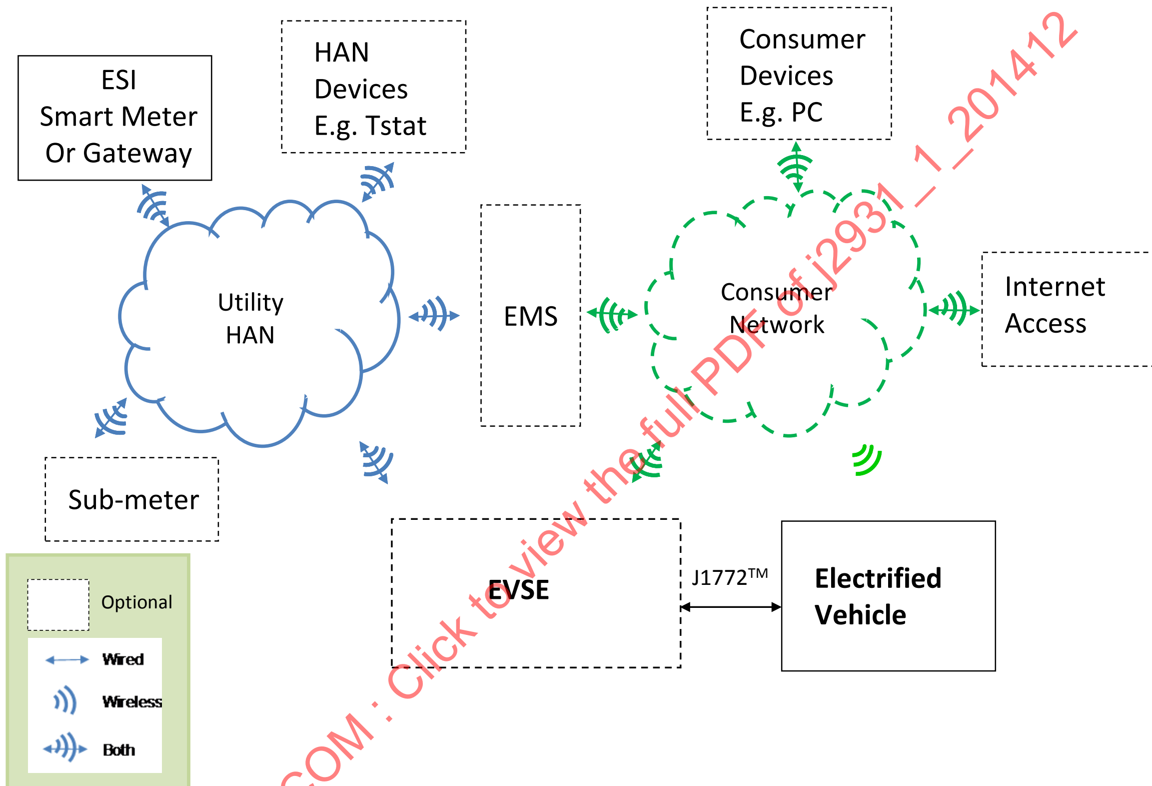


FIGURE 8 - UTILITY OR SERVICE PROVIDER/CONSUMER NETWORK

5.7.1 Communications Performance Requirements

RD.UtilComm.3	MAC/PHY throughput shall be 100kbps or greater		Basic
RD.UtilComm.4	The Utility or service provider message latency is 15 minutes max.		Basic

5.7.2 Protocol Requirements

RD.UtilComm.5	Use IPv6/HTTP1.1 and XML	SE2.0	Basic

5.7.3 Scenarios

RD.UtilComm.6	Minimum distance over which communication capability shall be maintained without intermediary devices independent of the communications medium • minimum distance for utility or service provider communications is 40 meters if using AC mains for communication • minimum distance for utility or service provider communication if using the J1772™ Pilot wire shall be based on the maximum cable length allowed by SAE J1772™	40 meters (AC mains) or As defined by SAE J1772™ (Pilot wire)	Basic
RD.UtilComm.7	Minimum number of devices that share a common communications technology, on a common network, that operate simultaneously and in proximity to the PEV that the PEV communications system must tolerate without causing the vehicle communications to fail to meet minimum bandwidth and latency requirements. Minimum device count, common network, for operation shall be 32 (typically 20)	32 (Typical 20)	TBD
RD.UtilComm.8	Minimum number of devices that share a common communications technology, on separate networks, that operate simultaneously and in proximity to the PEV that the PEV communications system must tolerate without causing the vehicle communications to fail to meet minimum bandwidth and latency requirements. Minimum device count, separate network, for operation shall be 200 (typically 120). Maximum has no definable limit	200 (Typical 120)	TBD
RD.UtilComm.9	Minimum number of devices using a different communications technology but share the communications medium and that operate simultaneously and in proximity to the PEV that the PEV communications system must tolerate without causing the vehicle communications to fail to meet minimum bandwidth and latency requirements. Minimum device count, separate network, for operation shall be 200 (typically 120). Maximum has no limit	200 (Typical 120)	TBD
RD.UtilComm.12	Where a particular scenario has unique attributes for association • association shall correctly identify the correct EV attached to the EVSE in the presence of multiple EVSE and EV within the same premise and neighborhood networks		Basic

5.8 DC Charging / Discharging Communications

When the AC/DC converter is off board in the EVSE, then communications is required between the PEV and the converter.

RD.DCComm.1	Application Data (payload) rate is 6 Kbps or greater concurrently (full-duplex)		Basic
RD.DCComm.2	Round trip message Latency is 25ms max		Basic
RD.DCComm.3	Minimum distance over which communication capability must be maintained without intermediary devices independent of the communications medium is defined by SAE J1772™	25 feet	Basic
RD.DCComm.4	Minimum number of devices that share a common communications technology, on separate networks, that operate simultaneously and in proximity to the PEV that the PEV communications system must tolerate without causing the vehicle communications to fail to meet minimum bandwidth and latency requirements. Minimum device count, separate network, for operation is 200 (typically 120) Maximum has no definable limit	200 (Typical 120)	TBD
RD.DCComm.5	Minimum number of devices using a different communications technology but share the communications medium and that operate simultaneously and in proximity to the PEV that the PEV communications system must tolerate without causing the vehicle communications to fail to meet minimum bandwidth and latency requirements. Minimum device count, separate network, for operation is 200 (typically 120) Maximum has no limit	200 (Typical 120)	TBD
RD.DCComm.6	If utility or service provider messages and DC charge control are combined, then a QoS mechanism must be capable of prioritizing packets and the latency requirements provided in RD.DCComm.2 and RD.UtilComm.2 must be met		Basic

5.9 Security

The PEV communication system must be secured against a number of potential threats. An attacker may attempt to:

- Avoid payment for electricity
- Gain unauthorized access to the utility or service provider's network
- Gain unauthorized access to private customer information, such as time and amount of energy use or vehicle usage logs.
- Cause physical damage to the PEV, EVSE, or electrical distribution system
- Cause denial of service – preventing the customer from being able to charge their PEV

The system must provide a level of security sufficient to prevent these threats, as well as implement a security framework with sufficient flexibility and extensibility to mitigate future threats.

RD.Sec.1	Utility or service provider messages will comply with NIST security requirements	SE2	Basic
RD.Sec.2	DC messages will comply with automotive security requirements		Basic
RD.Sec.3	DC messages will use same security as Utility or service provider Messages		TBD

5.10 Reliability

Communications reliability can be expressed as the probability that a message sent through the system will be delivered correctly to the recipient.

Reliability is one of the most important requirements for the PEV charging system. Communication reliability can be less than 100% for several reasons. On a shared medium, noise from various sources can cause the message to be lost or unreadable. Noise can come from physical processes, other equipment, or other communications systems that are sharing the medium. Physical limitations of signal propagation, transmitter power, and receiver sensitivity limit the usable communications range. When operating near range limit, reliability will be reduced. Reliability can also be affected by imperfect compatibility between systems. Verification of proper interoperability is essential for reliable operation of communication system, especially standards-based technologies from multiple vendors.

Reliability Requirements			
RD.RelComm.1	There shall be no excessive impairment or degradation to the consumer network e.g., Multimedia distribution. Initial requirement set to 10% reduction in bandwidth maximum between two nodes on the consumer network[1]		Basic
RD.RelComm.2	Communication shall not be susceptible to noise and transmissions caused by crosstalk (4-sigma value of 99.4%) from other conductors in the cordset, or from another twisted cordset		Basic
RD.RelComm.3	The technology chosen shall not cause interference to signals that may be on other conductors in the cordset, or another twisted cordset		Basic
RD.RelComm.4	Co-exist with all current physical network interfaces operating on the medium		Basic
RD.RelComm.5	Co-exist with future physical interfaces not present in the market or in development		TBD
RD.RelComm.6	Co-exist with neighbor networks on the same medium without substantial throughput degradation on consumer network or HAN		Basic
RD.RelComm.7	Shall provide connectivity to 99% of the nodes in homes		TBD

[1] The Task Force will collect additional data and refine at a later date

Reliability Requirements - continued			
RD.RelComm.8	The communication technology shall implement mitigation methods to deal with all common interferers found in home networks (Wired or Wireless), including hairdryers, holiday lights, high frequency switching power supplies, and microwave ovens.		Basic
RD.RelComm.10	Interoperability requirements as defined by SAE must interoperate with following technologies: TBD		TBD

5.11 Performance Requirements

RD.Perf.1	The time to indicate to the consumer that communications has successfully established shall be <10s		Basic
RD.Perf.2	Except in the case of DC charging, the PEV shall receive charge if no communications can be established. In the event no communications can be established, the PEV may not qualify for certain PEV rate programs.		Basic

5.12 Communication Stack

The communication stack is planned to address both the utility or service provider requirements for SEP2 messages and the out-of-band path to an off-board charger. The PHY & MAC layers implemented by the PEV and the ESI/HAN may differ, however the remaining layers are common to insure security and other aspects are according to the SEP2 criteria. Figure 9 identifies an example of how this may be accomplished. This example of a stack implementation illustrates just one of the possible architectures, and is thought to be the most common or likely architecture in a typical residential scenario. Other possible architectures may include lack of a SEP2.0-capable HAN, increased functionality in the EVSE, etc.

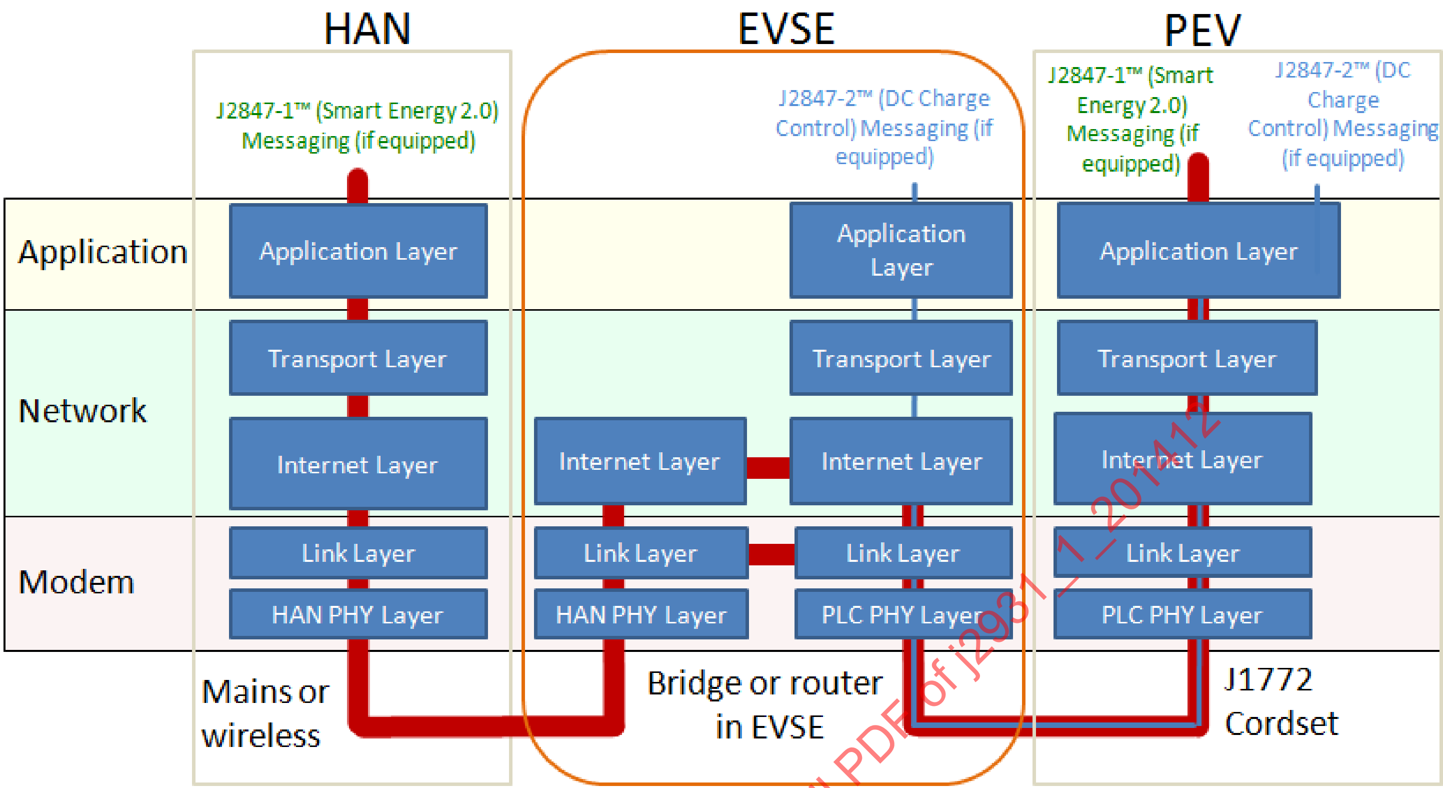


FIGURE 9 - PROPOSED COMMUNICATION STACK

6. SEP 2.0 SYSTEM ARCHITECTURE

6.1 Residential AC Charging System Architecture

Two typical Network configurations of the Residential AC Charging System are shown below. Both consist of at least one PEV, EVSE, EUMD and ESI. Device descriptions can be found in section 3, whereas logical functions are described below. In all scenarios it is assumed that if present, devices are authorized and authenticated to communicate on the network according to their function and role. Note that both the EV and the EVSE could control the Charging and respond to Demand Response (DR) and Pricing events. In the event of the conflict, the EV will take control. The EUMD (submeter) could reside in the HAN, the EV or both.

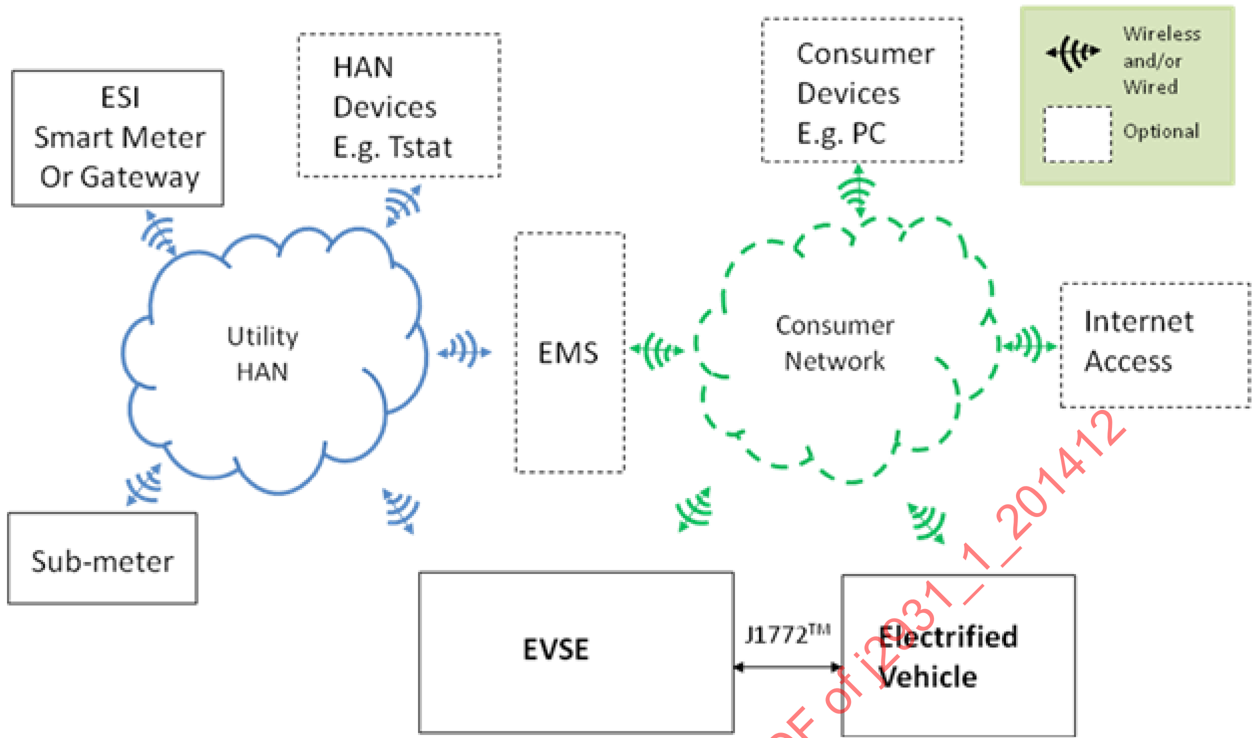


FIGURE 10 - OVERALL NETWORK SYSTEM ARCHITECTURE W/ ONE ESI, EVSE, PEV, EUMD (SUBMETER), CONSUMER NETWORK

Electrically, the Network is connected as shown in Figure 11. Note that this is different than the network configuration.

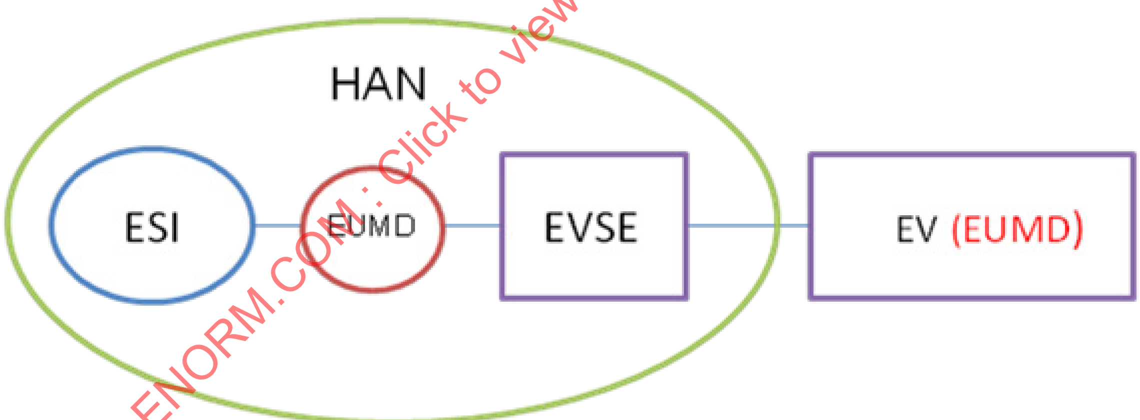


FIGURE 11 - OVERALL ELECTRICAL SYSTEM ARCHITECTURE

6.2 Device Functions and Roles

Within SEP 2.0, devices are described by the function sets and roles that they implement. A function set is a grouping of related data objects that enable a given service or desired capability and represents a network resource which facilitates a given type of transaction. The primary SEP 2.0 function sets of interest to PEVs are Metering, Pricing, Demand Response/Load Control (DRLC), and Distributed Energy Resources (DER) Control.

Roles relate to how a device interacts with other devices. Devices may be clients, servers, or both. Both function sets and roles are determined by device manufacturers, and their configuration in the HAN determines service provider program eligibility. Some devices will necessarily implement a determined function set (e.g., a submeter minimally implements the metering function), while some devices may implement more than one (e.g., a PEV may implement pricing, DRLC, and DER Control).

6.2.1 Metering

The metering function set provides information such as reading type and meter reading between HAN devices. The metering function set is necessary for some service provider programs that require separately metering the PEV energy consumption.

6.2.2 Pricing

The pricing function set provides service provider tariff structures. It is not intended to provide all the information necessary to represent a premises' bill but to help determine charging schedules and incentivize off-peak PEV charging. The pricing function set is designed to support a variety of tariff types:

- Flat-rate pricing
- Time-of-Use blocks
- Consumption blocks
- Hourly day-ahead pricing
- Real-time pricing
- Combinations of the above.

6.2.3 DRLC

This function set provides an interface for Demand Response and Load Control. Servers expose load control events called EndDeviceControls (EDC) to client devices. All EDC instances will expose attributes that allow devices to respond to events that are explicitly targeted at their device type. For example, an EDC may contain an Offset object indicating a degree offset to be applied by an EVSE. The EDC will also expose necessary attributes that load control client devices will need in order to process an event. These include Start Time and Duration, as well as an indication on the need for randomization at the start and/or end of the event.

6.2.4 DER Control

This function set provides an interface to control Distributed Energy Resources (whereby energy is provided to and managed by the grid). PEVs, as Distributed Energy Resources (DER), are devices which utilize a Reservation for bi-directional energy transfer when load, cost, and timing are such that a simple energy transfer does not suffice.

6.2.5 Roles

The rich variety of interactions on the HAN can make it difficult to define client and server implementations that are true for all deployments. Generically, the server is the device that hosts a resource, and the client is the device that obtains, extends, updates, or deletes representations of that resource. Devices may be both clients and servers.

In keeping with a RESTful paradigm, messages (generally) are not sent to clients. Clients poll servers to obtain representations of the current state of a resource, and take action based on that state. For example, a PEV might poll a meter to obtain a representation of the metering data resource or a DRLC server to obtain the current event list. In order to reduce polling, which can be an inefficient use of resources, devices may also subscribe to a resource. When a change to a resource is made (e.g., an addition to the DRLC event list, or an update to an event's attribute), the server (notifier) will contact each client (subscriber) that is subscribed to notifications for that resource.

6.3 Feature Descriptions

The following general features may be implemented in a PEV HAN. Support for these features is determined by the service provider programs being offered and the client-server implementations available at a particular charge point. Because of the variety of functions and roles able to be implemented on devices, the tables within each section below are informative and not meant to constrain the range of possible implementations.

6.3.1 PEV Tariffs

This is the ability for a service provider to provide Pricing information, potentially including special PEV tariffs. Depending on the jurisdiction and policy of the service provider, special PEV pricing information may require authentication of a PEV and presence of an EUMD to separately record the energy consumed or provided by the PEV. EVSEs may be able to proxy for the PEV to the service provider depending on its policy and the jurisdiction.

6.3.2 Demand Response

This is the ability for a PEV or EVSE to respond to service provider requests to reduce electricity demand in response to grid infrastructure constraints. The only way to know with certainty that a PEV has complied with a request is to have authentication/presence of an EUMD. A variety of service provider programs and incentives exist, but compliance with these requests is subject to EVSE and PEV owner preferences.

6.3.3 Charging Management

This is the ability to charge a vehicle based upon parameters determined by the service provider's electricity distribution infrastructure (e.g., dynamic balancing of PEV charging parameters within a circuit or on a neighborhood transformer). Without the knowledge of the PEV state of charge, a service provider may only perform basic demand response. With Distributed Energy Resource Control, the service provider may be able to more intelligently manage PEV charging parameters depending upon the PEV owner's preferences and the PEV state of charge.

6.3.4 Roaming

This is the ability to identify the PEV or its contract at the moment of charging and settle the transaction with the PEV's preferred service provider while crediting the charging spot's owner for the electricity consumed. This requires correlation of a specific PEV to a known actor in the premise able to record the charging energy (e.g., EUMD). An EVSE alone may not be sufficient to enable this capability without additional input from the PEV owner (e.g., credit card, service provider smart card, mobile phone).

6.4 Feature Enablement and Functionality Requirements

The chart below provides the implementation capabilities and SEP 2.0 function sets required to enable the features described above. This table is not device-centric, as a variety of charging system architecture implementations can satisfy these functional requirements.

Feature/Program	PEV-to-Premise Association	Server and Client Function Set Implementations Required				
		Metering	Pricing	DRLC	DER Control	Billing
PEV Tariffs	Y	Y	Y			
Demand Response	Y	Y		Y		
Charging Management	Y	Y			Y	
Roaming	Y	Y				Y

While some subset of features/programs may be possible with lesser implementations (e.g., without premise association), PEV manufacturers and service providers will want to comply in order to meet the highest common denominator found in their market. For example, a service provider could use demand response features in PEVs if they were not associated to the premise of their charging spot during the event, but the ability to provide incentives based on performance achieved during the event is not possible without correlation to the premise. Premises association is discussed in greater detail above.

6.5 Smart Charging Implementation Design

There are three sets of sequence diagrams of primary importance in understanding basic smart charging:

- EVSE and EUMD initial setup
- PEV registration and service discovery
- Normal and repeating operations

6.5.1 Each diagram describes the steps taken, as well as the device's role for the scenario. EVSE and EUMD Initial Setup[2].

This activity diagram represents the initial setup of the EVSE and EUMD as authenticated and authorized members of the HAN. It assumes the EUMD is located between the ESI and PEV, the PEV owner has provided EVSE and PEV security materials out-of-band to the service provider, and the service provider has populated the ESI with the PEV security materials[3]. The EUMD will follow the same initial setup as the EVSE and so is not shown.

[2] This material is subject to change

[3] Security materials will be a Globally Unique Identifier (GUID). Requirements SHOULD be in place to include a GUID on these devices

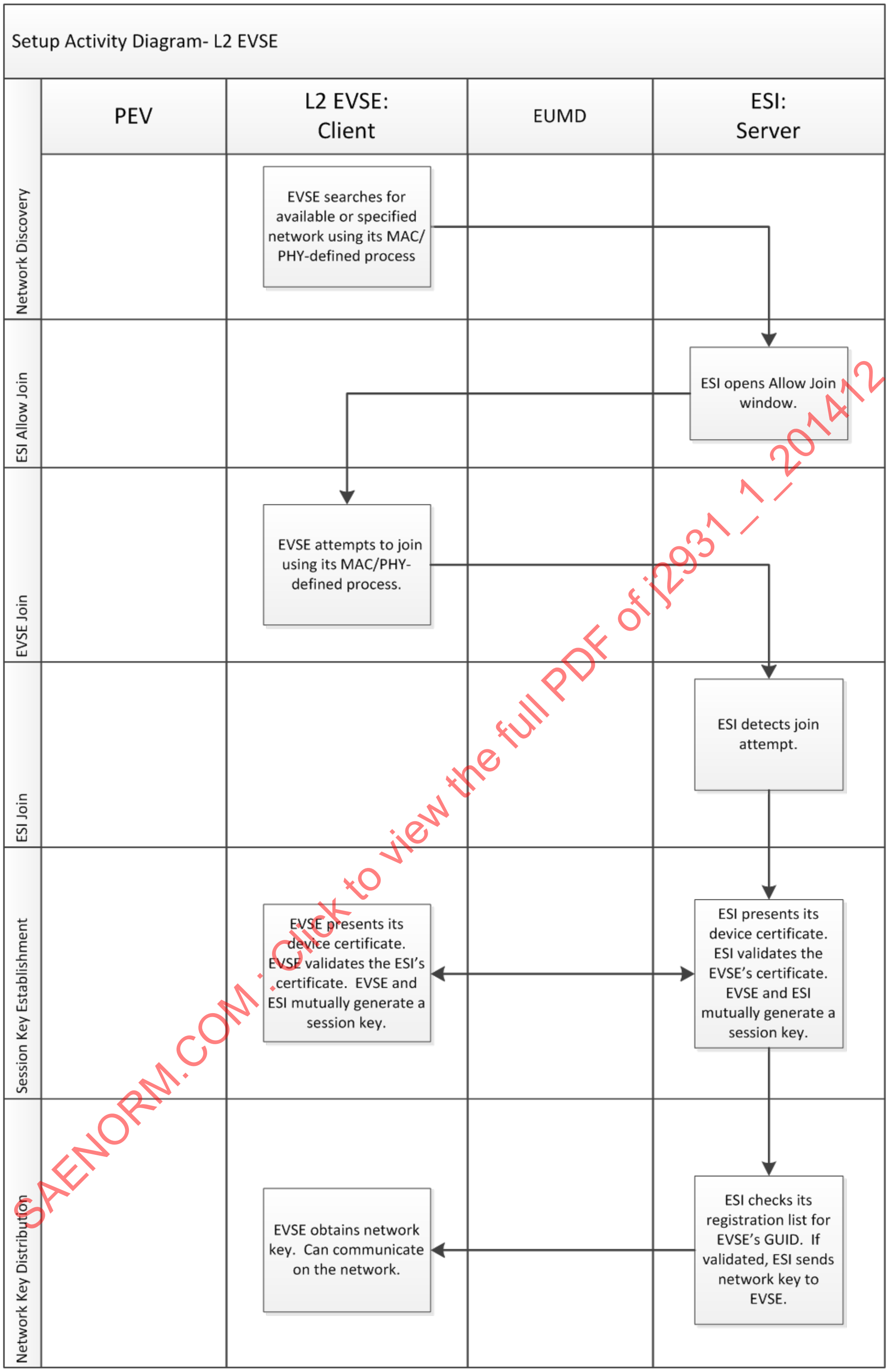


FIGURE 12 - SETUP ACTIVITY DIAGRAM - LEVEL 2 EVSE (W/ASSOCIATION)

6.5.2 Network Discovery

The Installer initiates the EVSE's network discovery functionality. The Network ID could be provided to the user by the service provider, the EVSE could scan for available ESIs allowing joining, or the EVSE could search for all available networks.

6.5.2.1 ESI Allow Join

The ESI operator configures the ESI to Allow Join (if not already done so). The ESI may be permanently configured in the Allow Join state.

6.5.2.2 EVSE Join

The EVSE attempts to proceed to the session key establishment step. There may be multiple ESIs allowing join visible to the EVSE. As such, the EVSE may require a steering mechanism (e.g., button push) or HMI (e.g., PIN input) in order ensure it joins the intended ESI.

6.5.2.3 ESI Join

ESI operator provides the PEV security materials communicated out-of-band by the Installer to the ESI's registration list. This process is out of scope for this document.

6.5.2.4 Session Key Establishment

EVSE initiates the PANA/EAP-TTLSv0 sequence with the ESI. The EVSE and ESI present their certificates to each other and validate them using the PKI to its embedded root CA certificate/public key. The ESI may also do a revocation check on EVSE's certificate (e.g., EVSE is known to the ESI operator as a bad actor and has been black listed by the ESI). The EVSE and ESI mutually negotiate a session key.

6.5.2.5 Network Key Distribution

The ESI checks the EVSE's GUID contained in its device certificate against its registration list. If there is a match, the ESI distributes the network key to the EVSE. The EVSE is now admitted to the network and can securely communicate within the network.

6.5.2.6 PEV Registration and Service Discovery

This activity diagram represents the initial and repeated setup of the PEV as an authenticated and authorized member of the HAN. It assumes the EVSE and EUMD have already joined the network, the EUMD is located anywhere between the ESI and PEV, the PEV owner has provided PEV security materials out-of-band to the service provider, and the service provider has populated the ESI with the security materials[4]. For the initial registration, the PEV will follow the same setup sequence as detailed the EVSE Setup Activity Diagram above.

[4] Security materials will be a Globally Unique Identifier (GUID). Requirements SHALL be in place to include a GUID on these devices

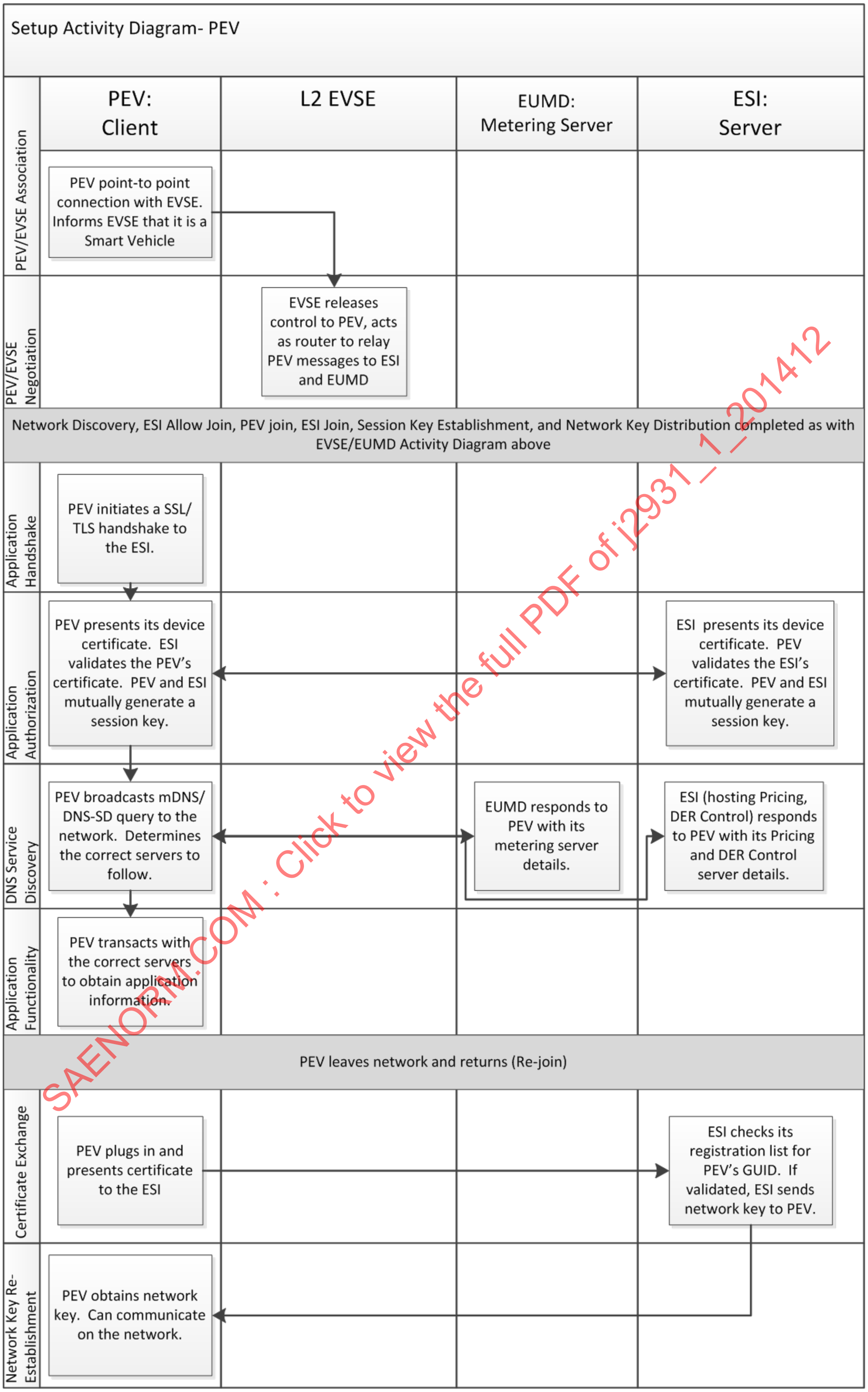


FIGURE 13 - SETUP ACTIVITY DIAGRAM - PEV (W/ASSOCIATION)

6.5.2.7 PEV/EVSE Association

The PEV and EVSE must be associated in order for the EVSE to retain or release control of the charging session to the PEV.

6.5.2.8 EVSE/PEV Negotiation

If the both the PEV and EVSE are capable of SEP2.0 communications, the EVSE shall relinquish control of the session to the PEV.

6.5.2.9 Application Handshake

PEV wishes to access a resource on the ESI. ESI is an http(s) server.

6.5.2.10 Application Authorization

The ESI may populate the resources' Access Control List based on the service provider's security policy rules if it has not already done so. The PEV is now authorized to access application resources on the ESI.

6.5.2.11 DNS Service Discovery

The PEV may broadcast a request to discover all the devices offering SEP 2.0 services or append a service sub-type to locate devices offering specific services of interest (e.g., Metering, Pricing, DRLC, DER Control, etc.). Responses provide the URI of the *DeviceCapability* resource (along with TCP ports used for HTTPS). The PEV can then perform an HTTP GET to retrieve the device capabilities and URI information required to access those services.

6.5.2.12 Application Functionality

The PEV accesses relevant application information from the resources discovered in the previous step. Refer to Section 11 of the SEP 2.0 Application Specification for more information.

6.5.2.13 Certificate Exchange

This scenario assumes the network key has been updated while the PEV was away from the network, and that the PEV and ESI have retained the session key previously created in the Session Key Establishment step. If the network key remains the same, the PEV should be able to communicate immediately. If the network key has been updated and PEV and ESI have not retained the shared network access session key, the PEV will have to redo the full join as above.

6.5.2.14 Network Key Re-Establishment

PEV can now communicate on the network.

6.5.3 Normal and Repeating Operations

This activity diagram in Figure 14 represents some of the likely activities a PEV would perform as described by the typical residential scenario. It assumes that the previous two activity diagrams have been completed and there is an associated EUMD, EVSE, and PEV. The PEV is enrolled in utility programs and authorized to communicate on the HAN and has completed service discovery. As a pre-requisite to this diagram, the user has entered his charging preferences into the PEV or other HMI (e.g., smartphone). This could include Time Start, Time End, Price, and Accept DR Events. Detailed messages can be found in SAE J2847/1 and SEP2.0 Application Specification.

In this scenario, as with the others shown here, the ESI is also the function set server for all of the application functionality the PEV would like to access.

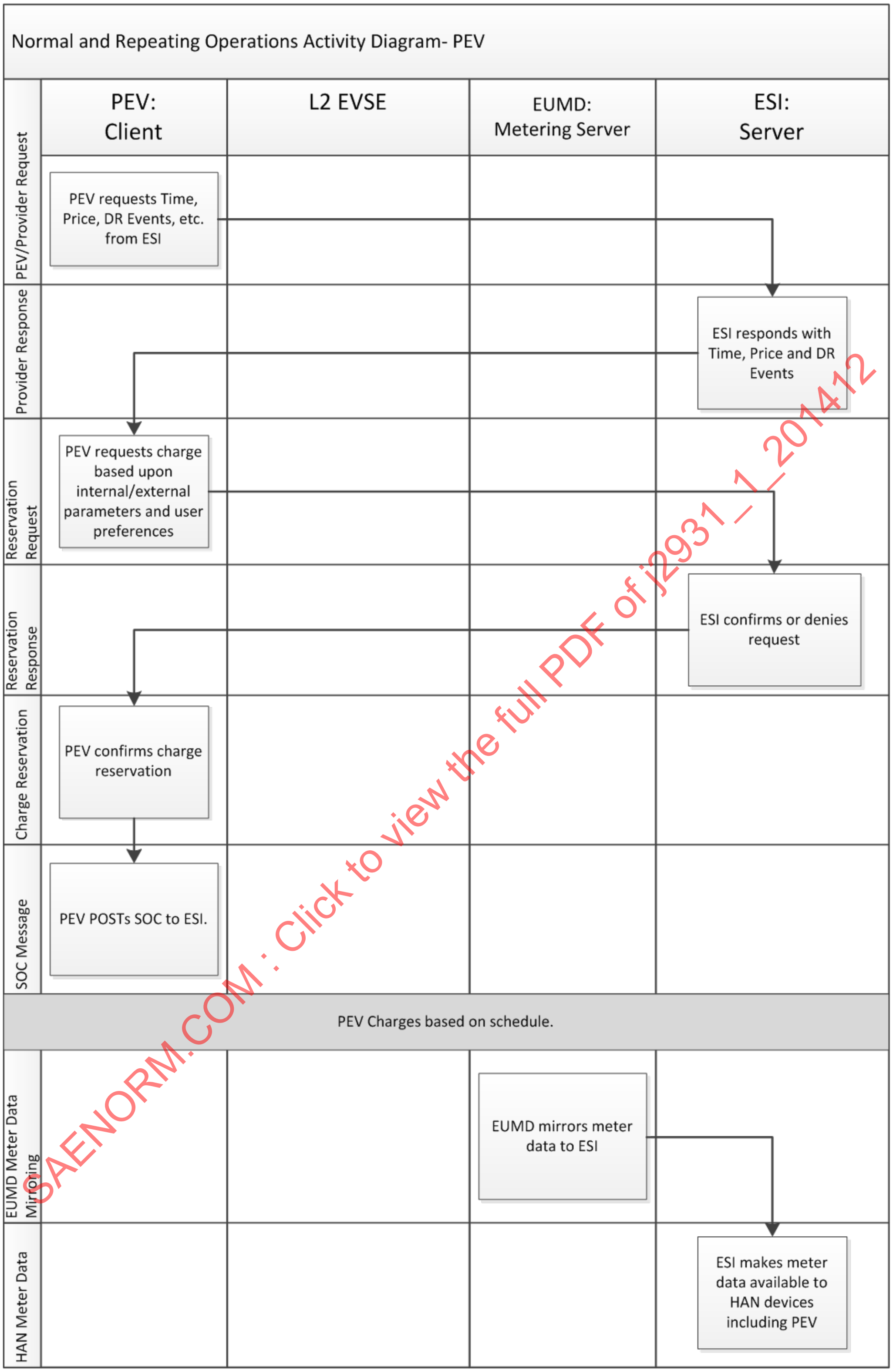


FIGURE 14 - PEV NORMAL AND REPEATING OPERATIONS

6.5.3.1 PEV/Provider Request

Pre-requisite for charging preferences entered into PEV. Preferences could include Time Start, Time End, Price, and Accept DR Events.

6.5.3.2 Provider Response

Price includes randomization.

6.5.3.3 Reservation Request

The PEV POSTs the relevant reservation request parameters to the DER Control server hosted by the ESI. The ESI could also be an energy management system (EMS) managing the load of the premise, which could be in a residence or business environment (e.g., fleet charging).

6.5.3.4 Charge Reservation

PEV determines whether the charging parameters provided in the Reservation Response meet its operator's criteria and takes action. PEV operator could override ESI request.

6.5.3.5 SOC Message

SOC is mirrored to ESI before, during (at a frequency TBD), and after charging for grid operator and user display purposes. Again, the "grid operator" in this case could be a facilities manager in charge of a PEV fleet.

6.5.3.6 EUMD Meter Data Mirroring

EUMD will know when connected PEV begins and ends charging and the amount of energy transferred. Data is mirrored to ESI.

6.5.3.7 HAN Meter Data

Mirrored meter data is now available for utility and customer use.

6.6 Public and Fleet Charging

6.6.1 Public Charging

The Public Charging scenario is similar to the Residential Charging from the systems point of view.

The major differences are:

- The Authentication and Authorization servers, if used could be provided by the facility manager server, i.e., not a Utility controlled ESI.

- Payment or identification methods may be used, instead of authenticating of the vehicle.

All other combinations of EVSE Types, EUMD and EV's may be found in Public AC/DC Charging.

6.6.2 Fleet Charging

The Fleet Charging scenario is similar to the Residential Charging from the Systems point of view.

The major differences are:

- The Authentication and Authorization servers, if used could be provided by the fleet owner. i.e., not in the Utility ESI
- There may be one EUMD for the whole Fleet, and therefore individual tracking of energy is not possible but the fleet may use the EUMD for total energy. i.e., the EUMD is not used by the EV.

All other combinations of EVSE types, EUMD and EV's may be found in Fleet Charging.

7. EV-EVSE COMMUNICATION

7.1 Basic requirements for V2G Communication

After establishing a physical connection, an IP based session has to be established. Within this session messages are transferred between EV and EVSE. Communication is needed for controlling a battery charging session and the interaction between EV and EVSE.

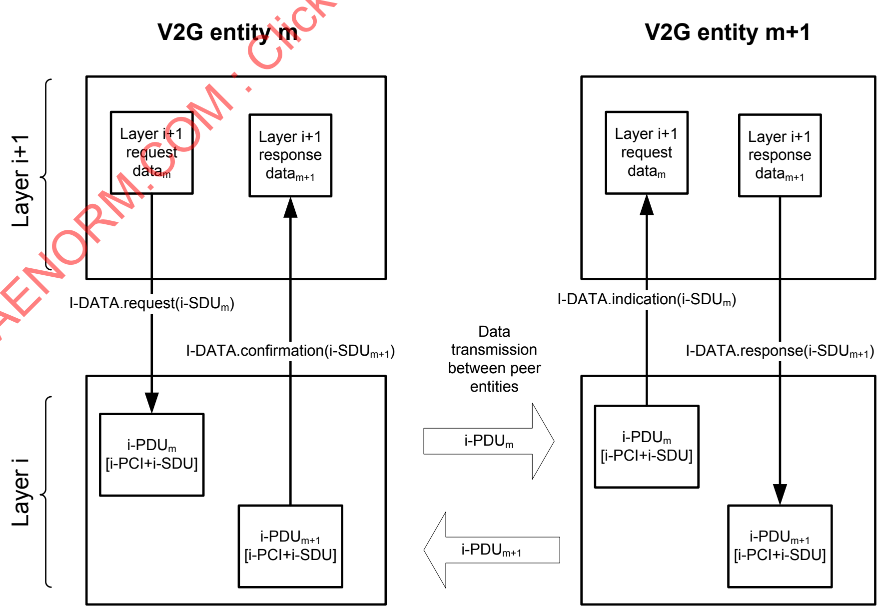
7.2 Communication Stack

The communication stack is defined in details in ISO/IEC 15118-2 and ISO/IEC 15118-3.

7.3 Service primitive concept of OSI layered architecture

7.3.1 Overview

This subsection explains how the OSI layered architecture is applied for the purpose of this document. It is intended to provide simple means for describing the interfaces between the individual communication protocol layers required by this document and furthermore allows for defining timing requirements more precisely. Services are specified by describing the service primitives and parameters that characterize a service. This is an abstract definition of services and does not force a particular implementation. Figure 15 depicts a simplified view of OSI layer interaction sufficient to understand the OSI layered architecture principles for the context of this document.



Key

PDUX: Protocol Data Unit of network entity x

PCI: Protocol Control Information

SDUX: Service Data Unit of network entity x

FIGURE 15 - OSI LAYERED ARCHITECTURE PRINCIPLES

When a layer i+1 instance of V2G entity m exchanges data with a layer i+1 instance of V2G entity m+1 each instance uses services of an instance of layer i. A service is defined as a set of service primitives.

7.3.2 Syntax of service primitives

Service primitives are described with the following syntax:

[Initial of layer]-[NAME].[primitive type](parameter list)

whereas [initial of layer] is one out of the following seven:
[Physical, Data Link, Network, Transport, Session, Presentation, Application]

whereas [NAME] is the name of the primitive

EXAMPLE: Typical examples for [Name] are CONNECT, DISCONNECT, DATA; other names are used in this document.

whereas [primitive type] is one out of the following four:
[request, indication, response, confirmation]

whereas (parameter list) includes a list of parameters separated by comma the user of the service is supposed to provide when using the respective service primitive; optional parameters are marked with brackets "[..]"

NOTE: In this document, the primitive type ".indication" always indicates an event asynchronously to the upper layer.

7.4 Physical and Data Link Layer Interfaces

7.4.1 Overview

As shown in Figure 16, the definition of the Data Link Layer provide two interfaces to higher layers,

- The Data Link Data SAP is the interface between the PLC technology and the layer 3 (e.g., IPv6)
- The Data Link Control SAP provides link status information, error information, control functionality and is located between the Connection Coordination and higher layers.

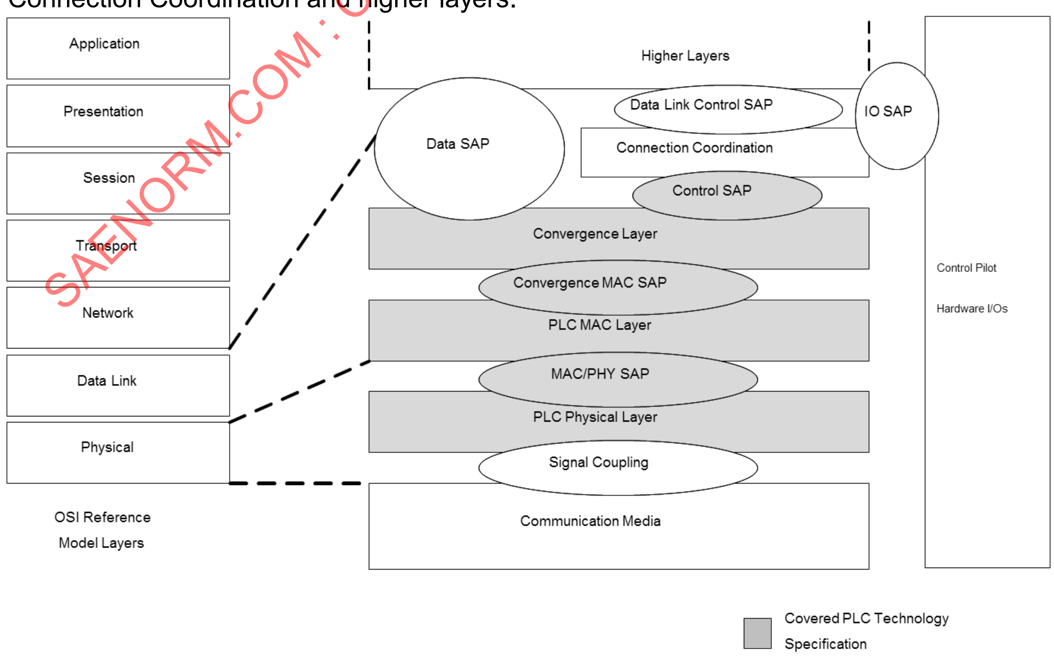


FIGURE 16 - DIN 70121 OSI LAYER 1-3 OVERVIEW

7.4.2 Hardware I/O Control

The hardware I/O Control Service Primitives provides methods for controlling, triggering and signaling interaction between the high-level digital communication and the connection coordination to the SAE J1772™ Basic Signaling. This interface is primarily accessed by higher layers and the connection coordination module to trigger on status changes and influence the status indicated via the Control Pilot. The IO-CPSTATE.indication notifies higher layers about a change in the current control pilot state. This indication shall be sent on any change of the control pilot status.

Primitive	**IO-CPSTATE.indication**
Entity to support	**EV,**
Parameter Name	**Description**
CPState	State of Control Pilot (A, B, C, D, E, F)

IO-GET_CPDUTYCYCLE.confirmation confirms the IO-SET_ CPDUTYCYCLE.request request by sending the current duty cycle within the parameter CPDUTYCYCLE.

Primitive	**IO-GET_ CPDUTYCYCLE.confirmation**
Entity to support	**EV, SE**
Parameter Name	**Description**
CPDUTYCYCLE	Duty cycle value of the control pilot (0-100%)

The IO-CPDTYCYCLE.indication notifies a change of the current control pilot duty cycle to higher layers. This indication shall only be sent, when the value change is greater than 2% within xyz ms. (TBD).

Primitive	**IO-GET_CPDUTYCYCLE.indication**
Entity to support	**SE**
Parameter Name	**Description**
CPDUTYCYCLE	Duty cycle value of the control pilot (0-100%)

7.5 V2G communication states

This subsection describes the basic states of the communication between EVCC and SECC. The timer and timeout values used in this subsection are described in subsection 5.11.

Figure 17 depicts the general communication states of the V2G communication from an EVCC perspective.

[V2G-DC-096] After the data link layer connection is established, the EVCC shall initiate the address assignment mechanism as defined in subsections 7.6.3.2 and 7.6.3.3.

NOTE: In this document this is described by D-LINK_READY.indication (DLINKSTATUS = Link established).

[V2G-DC-097] After the Application Layer requests the start of a Communication Session, the EVCC shall initiate the address assignment mechanism as defined in subsections 7.6.3.2 and 7.6.3.3.

[V2G-DC-098] The EVCC shall process the IP address assignment mechanism as defined in subsections 7.6.3.2 and 7.6.3.3.

The EVCC shall stop the IP address assignment mechanism as defined in subsections 7.6.3.2 and 7.6.3.3 when V2G_EVCC_CommunicationSessionSetup_Timer is equal or larger than V2G_EVCC_CommunicationSessionSetup_TimeOut.

[V2G-DC-100] After a link-local IP address is assigned, the EVCC shall perform the SECC discovery as defined in subsection 7.6.3.3. The EVCC should employ a link local multicast destination address when performing discovery for the SECC.

NOTE: In this document, this is described by N-IP_Address.indication (N_IP_STATUS = Link Local Address assigned).

[V2G-DC-101] The EVCC shall process the SDP according to subsection 7.6.3.3.

[V2G-DC-102] The EVCC shall stop the SDP when V2G_EVCC_CommunicationSessionSetup_Timer is equal or larger than V2G_EVCC_CommunicationSessionSetup_TimeOut.

[V2G-DC-103] After SECC IP address is discovered, the EVCC shall establish the TCP connection to the SECC as described in subsection 7.7.1.

NOTE: In this document, this is described by N-SECC_Address.indication(N_SECC_STATUS = SECC IP-address assigned).

The EVCC shall attempt establishing a TCP connection according to subsection 7.7.1.

[V2G-DC-105] The EVCC shall stop to attempt to establish a TCP connection when V2G_EVCC_CommunicationSessionSetup_Timer is equal or larger than V2G_EVCC_CommunicationSessionSetup_TimeOut.

[V2G-DC-106] Once the TCP connection is established, the EVCC shall initiate the V2G Communication Session as defined in section 7.10.

[V2G-DC-107] The EVCC shall stop the communication and terminate the TCP session after the application layer requests to stop the session.

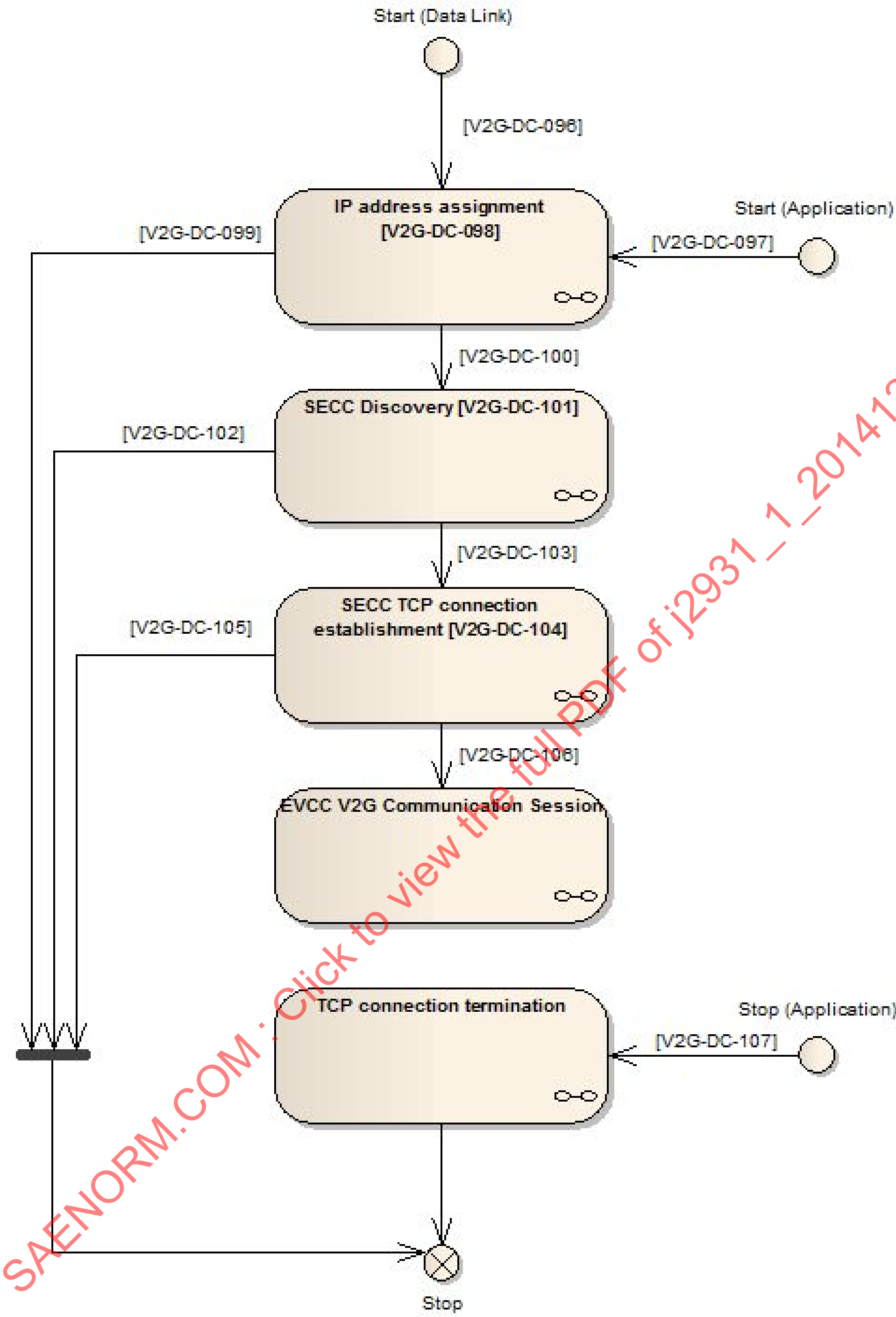


FIGURE 17 - OVERVIEW V2G COMMUNICATION STATES EVCC

Figure 18 depicts the general communication states of the V2G communication from an SECC perspective.

[V2G-DC-108] The SECC shall configure an IP address (static or dynamic) by any appropriate mechanism.

[V2G-DC-109] The SECC discovery service shall be running when the SECC enters CP State B.

[V2G-DC-110] The SECC discovery service shall be updated after an IP address for the SECC is changed.

NOTE: It is not required that the SECC discovery service is implemented in the SECC directly. It is also possible to have a separate unit providing the SECC discovery service.

The SECC shall stop the IP address assignment mechanism when V2G_SECC_CommunicationSessionSetup_Timer is equal or larger than V2G_SECC_CommunicationSessionSetup_TimeOut.

[V2G-DC-112] After the IP address is configured, the SECC shall wait for a TCP connection on the IP address that is distributed by the SECC discovery service.

NOTE: In this document, this is described by N-IP_Address.indication(N_IP_STATUS = Link Local Address assigned) or N-IP_Address.indication(N_IP_STATUS = Global Address assigned).

[V2G-DC-113] As long as a TCP connection is not yet established, the SECC shall wait for a TCP connection at least until the SECC enters CP State A.

[V2G-DC-115] After the TCP connection is established, the SECC shall wait for the initialization of the V2G Communication Session as defined in SAE J2847/2, Section 6.

[V2G-DC-116] The SECC shall stop the communication and terminate the TCP connection after the application layer requests to stop the TCP connection.

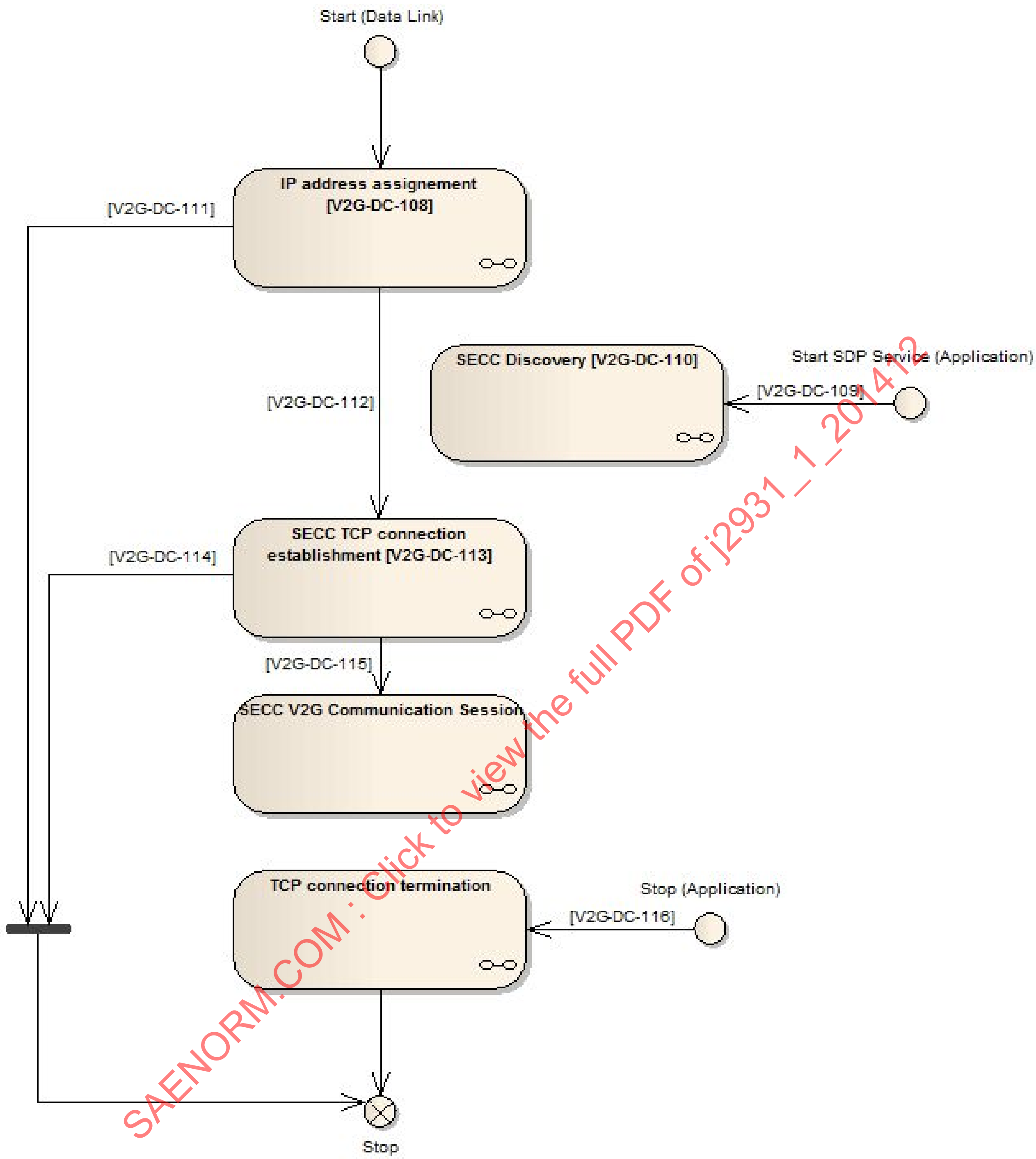


FIGURE 18 - OVERVIEW V2G COMMUNICATION SESSION STATES SECC

7.6 Network Layer

7.6.1 General

The protocol is based on the Internet Protocol standard IPv6. The Internet Protocol is datagram based; unreliable and located on the Network Layer according to the OSI layered architecture model. IP is the first transmission medium independent protocol.

The process of how a node will acquire an IP address is described in subsection 7.6.3.3.

7.6.2 Applicable RFCs and Limitations and Protocol Parameter Settings

[V2G-DC-117] All V2G entities shall implement the “must” requirements included in the following IETF RFCs if not explicitly excluded.

7.6.2.1 IPv6

[V2G-DC-118] All V2G entities shall implement IPv6 according to IETF RFC 2460.

NOTE: For EVCC side only node requirements and for SECC side host requirements are applicable. Router functionality is only an optional requirement for SECC side.

[V2G-DC-119] All V2G entities shall skip the following IPv6 Extension Headers: Hop-by-Hop Options Header, Routing Header (EVCC), and Destination Options Header.

[V2G-DC-120] All V2G entities shall fulfill the IPv6 node requirements specified in IETF RFC 4294.

[V2G-DC-121] All V2G entities shall not implement IPsec, required as must in IETF RFC 4294, chapter 8.

[V2G-DC-122] All V2G entities shall implement IETF RFC 5095, which updates IETF RFC 2460 and IETF RFC 4294.

NOTE: The IANA allocation guidelines for the routing type field in the IPv6 routing header are described in [1] IETF RFC 5871. It is recommended to adhere to these guidelines.

[V2G-DC-123] All V2G entities shall implement path MTU discovery according to IETF RFC 1981.

[V2G-DC-124] All V2G entities shall support handling of overlapping IP fragments according to IETF RFC 5722.

[V2G-DC-125] All V2G entities shall implement IETF RFC 5220, which extends IETF RFC 2460.

The following general requirements apply to the handling of IP packets addressed to a V2GTP entity:

[V2G-DC-126] Any packets with a multi- or broadcast address as source IP address shall be ignored.

7.6.2.2 Neighbor Discovery (ND)

Primary and secondary actors use IPv6 stateless address auto configuration for generating addresses for their interfaces. All interfaces have a link-local address. To ensure unique addresses and to support global addresses the neighbor broadcast protocol is used.

[V2G-DC-127] Each V2G entity shall implement ND as defined in IETF RFC 4861.

[V2G-DC-128] The EVCC and the SECC shall implement IETF RFC 4429 to allow assignment of IP address before ND has finished its work.

7.6.2.3 Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is part of the Internet protocol suite and is used to send error messages, e.g., to indicate that a requested service is not available or that a host could not be reached. Consequently ICMP is a mandatory part of an IP stack implementation and is located on the network layer according to the OSI layered architecture model.

[V2G-DC-129] Each V2G entity shall implement ICMPv6 as specified in IETF RFC 4443.

[V2G-DC-130] ICMP message types defined in IETF RFC 4443 shall only be implemented if included in Table 1.

All V2G entities shall implement extended ICMP to support Multi-Part-Messages according to IETF RFC 4884.

Each V2G entity shall implement the ICMP message set defined in Table 1.

[V2G-DC-133] Each V2G entity shall implement the IETF RFCs referred to in column "Reference" of Table 1 describing the implementation details for the respective ICMP message type.

TABLE 1 - MANDATORY ICMP MESSAGE SET

ICMP message ID	ICMP message name	Reference
1	Destination Unreachable	IETF RFC 4443
2	Packet Too Big	IETF RFC 4443
3	Time Exceeded	IETF RFC 4443
4	Parameter Problem	IETF RFC 4443
128	Echo Request	IETF RFC 4443
129	Echo Reply	IETF RFC 4443
133	Router Solicitation	IETF RFC 4861
134	Router Advertisement	IETF RFC 4861
135	Neighbour Solicitation	IETF RFC 4861
136	Neighbour Advertisement	IETF RFC 4861
137	Redirect Message	IETF RFC 4861
141	Inverse Neighbour Discovery Solicitation Message	IETF RFC 3122
142	Inverse Neighbour Discovery Advertisement Message	IETF RFC 3122
151	Multicast Router Advertisement	IETF RFC 4286
152	Multicast Router Solicitation	IETF RFC 4286
153	Multicast Router Termination	IETF RFC 4286

7.6.3 IP Addressing

7.6.3.1 General

This section specifies how an EV retrieves valid IP addresses to communicate over an IP-based network. Following addresses are considered for the purpose of this standard:

— EV's own IP address;

— IP address for connecting to the SECC.

NOTE: An IPv6 host usually has multiple IP addresses assigned to one physical network interface. (e.g., link-local, site-local and global address; if there are multiple routers connected to a local link the host has even several global addresses).

7.6.3.2 Stateless auto address configuration (SLAAC)

[V2G-DC-134] For IPv6 each V2G entity shall support the configuration of a link-local IPv6 unicast address as specified in IETF RFC 4291.

[V2G-DC-135] The interface ID of the Link-Local address of a V2G entity shall be generated from its IEEE 48 bit MAC identifier according to the definition in IETF RFC 4291.

[V2G-DC-136] If present in the network, an IPv6 address shall be derived from the router advertisement messages according to IETF RFC 4862.

7.6.3.3 Address selection

[V2G-DC-137] The IPv6 Default Address Selection shall be performed according to IETF RFC 3484.

7.6.4 Network Layer service primitive - N-IP_Address.indication

The N-IP_Address.indication notifies about the status of the IP address assignment. Table 2 describes the service primitive and its parameter(s).

TABLE 2 - N-IP_ADDRESS.INDICATION SERVICE PRIMITIVE

Primitive name	**N-IP_Address.indication**
Entity to support	EVCC, SECC
Parameter Name	Description
N_IP_STATUS	- Link local address assigned - Global address assigned - Error

N-IP_Address.indication (N_IP_STATUS = Link local address assigned) indicates the assignment of a local IP address.
N-IP_Address.indication (N_IP_STATUS= Global address assigned) indicates the assignment of a global IP address.
N-IP_Address.indication (N_IP_STATUS= Error) indicates any detected error during IP assignment.

7.6.5 SECC discovery

[V2G-DC-138] The EV shall support SECC discovery according to subsection 7.7.3.

7.7 Transport Layer

7.7.1 Transmission Control Protocol (TCP)

7.7.1.1 Overview

The Transmission Control Protocol (TCP) allows applications of V2G entities to establish a reliable data connection to other entities. It allows data exchange in a reliable way and allows orderly delivery of sender to recover data. Additionally TCP provides flow control and congestion control and also provides for various algorithms to handle congestion and influence flow control.

7.7.1.2 Applicable RFCs, Limitations and Protocol Parameter Settings

[V2G-DC-139] Each V2G entity shall implement TCP as specified in IETF RFC 793.

7.7.1.3 TCP Performance and Checksum Recommendations and Requirements

The following requirements define TCP implementation details relative to congestion control, retransmission, timing, initial window size and Selective Acknowledgement for the purpose of improving the overall performance of TCP.

It is recommended to use the following congestion control and re-transmission algorithms in addition to the standard TCP methods:

Each V2G entity should implement TCP congestion control according to IETF RFC 5681.

Each V2G entity should implement the NewReno Modification to TCP's Fast Recovery Algorithm according to IETF RFC 3782.

Each V2G entity should compute TCP's retransmission timer according to IETF RFC 6298.

In order to increase TCP's performance, each V2G entity should implement TCP extensions for High Performance according to IETF RFC 1323.

Each V2G entity should support TCP Selective Acknowledgment Options according to IETF RFC 2018.

Each V2G entity should implement the User Timeout Option according to IETF RFC 5482.

[V2G-DC-146] The urgent pointer for TCP shall not be used by any V2G entity.

It is recommended to use the following checksum algorithm:

The checksum fields required in TCP headers should be implemented according to IETF RFC 1624.

7.7.2 User Datagram Protocol (UDP)

7.7.2.1 Overview

The User Datagram Protocol (UDP) is a connectionless protocol. UDP does not provide the reliability and ordering guarantees that TCP does. Packets may arrive out of order or may be lost without notification of the sender or receiver. However, UDP is faster and more efficient for many lightweight or time-sensitive purposes. UDP is located on the Transport Layer of the OSI layered architecture model.

7.7.2.2 Applicable RFCs, limitations and protocol parameter settings

[V2G-DC-148] Each V2G entity shall implement User Datagram Protocol according to IETF RFC 768.

7.7.3 SECC Discovery Protocol

7.7.3.1 General Information

An EVCC uses the SECC Discover Protocol (SDP) to get the IP address and port number of the SECC. The SDP client sends out SECC Discovery Request messages to the local link (multicast) expecting any SDP server to answer its request with a SECC Discovery Response message containing this information.

After the EVCC received the IP address and the port number of the SECC, it can establish a TCP connection to the SECC (see subsection 7.8, V2G Transfer Protocol)

[V2G-DC-180] An SDP server shall be accessible in the local link.

NOTE: As common for internet technologies, an SDP server may be implemented on the same physical device as the SECC and may also interface to the same IP address. If this is not the case, optimistic DAD as specified in RFC 4429 won't lead to a benefit.

7.7.3.2 Supported ports

SDP is a UDP based protocol. The ports listed in Table 8 are used by SDP.

[V2G-DC-473] An SDP client shall support the port V2G_UDP_SDP_CLIENT as defined in Table 8 for sending and receiving SDP messages.

[V2G-DC-474] An SDP server shall support the port V2G_UDP_SDP_SERVER as defined in Table 8 for receiving and sending SDP messages.

NOTE: Depending on the implementation of the EVCC the dynamically assigned V2G_UDP_SDP_CLIENT port will be assigned once during or before the first transmission of a UDP packet to a SECC or can be dynamically re-assigned for each individual UDP request message and response. Also depending on whether messages are repeatedly sent, response messages may arrive asynchronously and may not be associated to the exact corresponding request anymore.

[V2G-DC-475] The SDP client shall be able to handle asynchronously arriving SECC Discovery Response messages.

7.7.3.3 Protocol Data Unit

7.7.3.3.1 Structure

An SDP message is based on the V2GTP message format as defined in subsection 7.8.3.1.

[V2G-DC-181] An SDP client shall support the definitions in subsection 7.8.3.1 as shown in Figure 21.

[V2G-DC-182] An SDP client shall use a separate UDP packet for each request message.

[V2G-DC-183] An SDP client shall locate the first byte of the request message header as defined in Figure 22 and Table 7 in the first byte of the UDP packet payload.

[V2G-DC-184] An SDP server shall support the definitions in subsection 7.8.3.1 as shown in Figure 21.

[V2G-DC-185] An SDP Server shall use a separate UDP packet for each response message.

[V2G-DC-186] An SDP server shall locate the first byte of the response message header as defined in Figure 22 and Table 7 in the first byte of the UDP packet payload.

Table 3 defines the generic SDP header structure, which is identical to the structure of the V2GTP header as defined in 7.8.3.1.

TABLE 3 - GENERIC SDP HEADER STRUCTURE

Item	Pos	Len	Description	Values
Generic V2GTP Header Synchronization Pattern				
Protocol Version	0	1	Identifies the protocol version of SDP packets.	0x00: reserved 0x01: SDP version 1 0x02…0xFF: reserved by document
Inverse Protocol Version	1	1	Contains the bit-wise inverse value of the protocol version which is used in conjunction with the SDP protocol version as a protocol verification pattern to ensure that a correctly formatted SDP message is received.	Equals the <Protocol_Version> XOR 0xFF (e.g., 0xFE for Protocol Version 0x01)
Generic SDP Header Payload type and Payload Length				
Payload type (GH_PT)	2	2	Contains information about how to interpret the data following the generic SDP header	Refer to Tabl4 8 for a complete list of currently specified payload type values.
Payload length (GH_PL)	4	4	Contains the length of the SDP message payload in bytes (i.e., excluding the generic SDP header bytes). Some payload types do not require any additional parameters (payload length is 0), some require a fixed SDP message length while others allow for dynamic length SDP messages.	0…4294967295 (= <d>)

7.7.3.3.2 Header Processing

An SDP header processing is based on the V2GTP message header processing as defined in subsection 7.8.3.1.

[V2G-DC-187] An SDP client shall apply to the header processing as defined in subsection 7.8.3.2 and shown in Figure 23.

[V2G-DC-188] An SDP server shall apply to the header processing as defined in subsection 7.8.3.2 and shown in Figure 23.

7.7.3.4 SECC Discovery Request Message

The SDP client uses the SECC Discovery request message to request the IP address and the port number of the SECC.

[V2G-DC-189] Only SDP client shall send SECC Discovery request messages.

[V2G-DC-190] An SDP client shall send SECC Discovery request messages with the source IP address on which it expects the SECC Discovery response message.

[V2G-DC-191] An SDP client shall send SDP request messages to destination port V2G_UDP_SDP_SERVER as defined in Table 6.

[V2G-DC-192] An SDP client shall send SDP request messages with source port V2G_UDP_SDP_CLIENT as defined in Table 6 on which it expects the SECC Discovery response message.

[V2G-DC-193] An SDP client shall send SECC Discovery request message to the destination local-link multicast address (FF02::1) as defined in IETF RFC 4291.

[V2G-DC-194] The SDP client shall send the SECC Discovery request message with payload type value 0x9000 as defined in Table 8.

[V2G-DC-196] The SDP client shall send the SECC Discovery request message with the payload length 2.

[V2G-DC-197] The SDP client shall send the SECC Discovery Request message with the payload as defined in Figure 19.

[V2G-DC-198] An SDP client shall send the payload in the order as shown in Figure 19. A byte with a lower number shall be sent before a byte with a higher number. The payload starts with byte 1 and ends with byte 2.

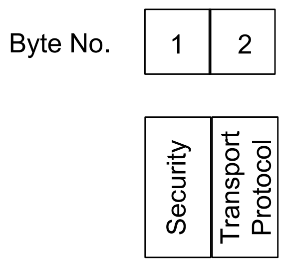


FIGURE 19 - SECC DISCOVERY REQUEST MESSAGE PAYLOAD

[V2G-DC-195] An SDP client shall use the encoding for the requested security option and the requested transport protocol as defined in Table 4.

TABLE 4 - PAYLOAD TYPE SECC DISCOVER REQUEST MESSAGE

	Security	*Transport Protocol*
Byte no. SDP request message	1	2
Byte no. SDP response message	19	20
Applicable values	0x00 = secured with TLS 0x01-0x0F = reserved 0x10 = No transport layer security 0x11-0xFF = reserved	0x00= TCP 0x01-0x0F = reserved 0x10 = reserved for UDP 0x11-0xFF = reserved

[V2G-DC-476] An SDP server shall use the encoding for the requested security option and the requested transport protocol as defined in Table 4 to define the supported transmission security and transport protocol for the port provided in the same payload as the security and transport protocol bytes.

[V2G-DC-546] For DC charging, Transport Protocol “TCP” and “No transport layer security” according to Table 4 shall be used.

7.7.3.5 SECC Discovery Response Message

The SDP server uses the SECC response message to response to an SECC Discovery request message and provides the IP-address and the port of the SECC to the client.

[V2G-DC-199] The SDP server shall be able to extract the source IP address and source port of a received UDP packet (client IP address and port number) and send a UDP packet to the identified IP address and port number.

[V2G-DC-200] An SDP server shall reply to any SECC Discovery request messages with an SECC Discovery response message.

NOTE: This requirement ensures that an SDP server serving multiple clients can be reached at any time. This supports charging of multiple EVs at an EVSE with a single SECC.

[V2G-DC-201] An SDP client shall not reply to any SECC Discovery Request message.

[V2G-DC-202] An SDP server shall only send response messages after an SECC Discovery Request message has been received.

An SDP server shall send an SECC Discovery Response messages as fast as possible after an SECC Discovery request message has been received.

[V2G-DC-204] If an SDP server has multiple IP addresses, the SDP server shall send an SECC Discovery response message with the source IP address on which the SDP server received the SECC request message.

[V2G-DC-205] An SDP server shall send an SDP response with source port V2G_UDP_SDP_SERVER as defined in Table 6.

[V2G-DC-206] An SDP server shall send an SECC Discovery Response message to the SDP client which sent the SECC Discovery request message.

[V2G-DC-207] An SDP server shall send an SECC Discovery Response message to the port of the SDP client which sent the SECC Discovery request message.

[V2G-DC-208] An SDP server shall send the SECC Discovery Response message with the payload type value 0x9001 as defined in Table 8.

[V2G-DC-477] An SDP server shall send the SECC Discovery Response message with payload length 20.

[V2G-DC-209] An SDP server shall send the SECC Discovery Response message with the payload as defined in Figure 20.

[V2G-DC-210] An SDP server shall send the payload in the order as shown in Figure 20. A byte with a lower number shall be sent before a byte with a higher number. The payload starts with byte 1 and ends with byte 20.

[V2G-DC-211] A SDP server shall send the fields “SECC IP Address” and “SECC Port” in big endian format: The most significant byte is sent first the least significant byte is sent last.

[V2G-DC-618] For DC charging, an SDP server shall send an SECC Discovery Response message with Transport Protocol equal to “TCP” and Security equal to “No transport layer security” according to Table 4.

NOTE: The mechanism used by the SDP server to determine its own IP address is out of the scope of DIN 70121.

NOTE: The source IP address and the source port of a received UDP packet is usually provided by the TCP/IP stack.

Byte No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	SECC IP Address																SECC Port		Security	Transport Protocol

FIGURE 20 - SECC DISCOVERY RESPONSE MESSAGE PAYLOAD

7.7.3.6 Timing and Error Handling

The process of SECC discovery is based on the application time out definitions. This subsection describes additional timing and error handling for the SECC Discovery Protocol.

[V2G-DC-212] The SDP client shall count the number of SECC Discovery request messages until a valid SECC Discovery response message has been received.

[V2G-DC-213] The SDP client shall reset the counter for sent SECC Discovery request messages after a valid SECC Discovery response message has been received.

[V2G-DC-214] After sending an SECC Discovery request message, the SDP client shall wait for an SECC Discovery response message for at least 250 ms.

[V2G-DC-215] After unsuccessfully waiting for an SECC Discovery response message the SDP client shall send a new SECC Discovery request message and increment the counter for sent SECC Discovery response messages.

[V2G-DC-216] If the SDP client has not received any SECC Discovery Response message after sending in maximum 5 consecutive SECC Discovery request messages it shall stop the SECC Discovery.

[V2G-DC-478] After stopping the SECC Discovery, the SDP client shall go to the same state as defined for an application (refer to Figure 17).

7.7.3.7 SECC Discovery service primitives

The N-SECC_Address.indication notifys about the status of the SECC IP address discovery. Table 5 describes the service primitive and its parameter(s).

TABLE 5 - N-SECC_ADDRESS.INDICATION SERVICE PRIMITIVE

Primitive name	**N-SECC_Address.indication**
Entity to support	EVCC
Parameter Name	**Description**
N_SECC_STATUS	- SECC IP -address discovered - Error

N-SECC_Address.indication (N_SECC_STATUS = SECC IP-address discovered) indicates that SDP returned a local or global IP-address for the SECC.

SECC_Address.indication (N_SECC_STATUS = Error) indicates any error during SDP as defined in subsection 7.7.3.

[V2G-DC-217] If SDP returns a global SECC IP-address, the EVCC shall not indicate the discovered SECC IP-address before the EVCC has configured a global IP address as defined in subsection 7.6.3.2 and 7.6.3.3.

[V2G-DC-218] If the SDP returns a global SECC IP-address, the EVCC shall indicate the discovered SECC IP-address after a global address assignment as defined in subsection 7.6.3.2 and 7.6.3.3 is indicated.

7.8 V2G Transfer Protocol

7.8.1 General Information

The V2G Transfer Protocol (V2GTP) is a compact communication protocol to transfer V2G messages between two V2GTP entities. It mainly consists of a header and payload definition that allows separating and processing V2G messages efficiently. V2GTP is the standard transfer protocol between the EVCC and SECC but may also be used for communication with other V2G Entities that support the V2GTP protocol.

7.8.2 Supported ports

V2GTP is based on TCP and UDP. In both transport protocols, a pair of IP addresses (source address and destination address) and a pair of port numbers (source port and destination port) are used to establish and identify a connection for bidirectional data exchange. The TCP connection is established from the source address and source port to the destination address and destination port. UDP is not connection-based; datagrams are exchanged between the source address and source port and the destination address and destination port. The ports listed in Table 6 are used by V2GTP entities.

TABLE 6 - SUPPORTED PORTS FOR V2GTP

Name	Protocol	Port number	Description
V2G_SRC_TCP_DATA	TCP(unicast)	Port number in the range of Dynmaic Ports (49152-65535) as defined in RFC6335.	V2GTP source port at a Primary Actor (e.g., EVCC) that implements the V2GTP protocol.
V2G_DST_TCP_DATA	TCP (unicast)	Port number at V2GTP entity providing a V2GTP destination port. For SECC it will be dynamically assigned by SDP mechanism	V2GTP destination port at a Primary Actor (e.g., SECC)
V2G_UDP_SDP_CLIENT	UDP (unicast)	Port number in the range of Dynamic Ports (49152-65535) as defined in RFC6335,	SDP client source port at the EVCC
V2G_UDP_SDP_SERVER	UDP (multicast)	15118	SDP server port which accepts UDP packets with a local-link IP multicast destination address.

For V2GTP entities implementing the V2GTP the following general requirements apply:

[V2G-DC-149] A V2GTP entity providing a destination port shall support at least one connection on the local port V2G_DST_TCP_DATA as defined in Table 6.

A V2GTP entity providing a destination port shall support multiple simultaneous connections on the local port V2G_DST_TCP_DATA as defined by Table 6.

A V2GTP entity using a source port shall support at least one connection on the local port V2G_SRC_TCP_DATA as defined in Table 6.

[V2G-DC-151] A V2GTP entity using a source port may support multiple connections on the local port V2G_SRC_TCP_DATA as defined in Table 6.

Especially, for an EVCC and an SECC the following applies:

[V2G-DC-153] The EVCC shall use a source port V2G_SRC_TCP_DATA as defined in Table 6.

[V2G-DC-154] The SECC shall provide a destination port V2G_DST_TCP_DATA as defined in Table 6.

[V2G-DC-155] The EVCC shall support at least one connection for a V2G Communication Session on port V2G_SRC_TCP_DATA.

[V2G-DC-156] The SECC shall support at least one connection for a V2G Communication Session on port V2G_DST_TCP_DATA.

[V2G-DC-157] The EVCC shall use the port V2G_DST_TCP_DATA returned in the last SECC Discovery response message (refer to SAE J2847/2) for connecting the SECC.

[V2G-DC-158] An SDP client shall support the port V2G_UDP_SDP_CLIENT as defined in Table 6 for sending and receiving SDP messages.

[V2G-DC-159] An SDP server shall support the port V2G_UDP_SDP_SERVER as defined in Table 6 for receiving and sending SDP messages.